```
################################################################

Hash_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                     20 21222324


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                     20 21222324


    personal_str is  <empty>
```

```
    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                    00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                      01 000001B8 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    Hash(counter||no_of_bits_to_return||input_string) is
                 D08FB441 F2F4CB37 CF6C2420 A82C7427 ACF7FCFD


    temp =
                 D08FB441 F2F4CB37 CF6C2420 A82C7427 ACF7FCFD


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                      02 000001B8 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    Hash(counter||no_of_bits_to_return||input_string) is
                 79901438 34A5C256 AB283936 6D96348C FE8C97AB


    temp =
                         D08FB441 F2F4CB37 CF6C2420 A82C7427
        ACF7FCFD 79901438 34A5C256 AB283936 6D96348C FE8C97AB
```

```
    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                        03 000001B8 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    Hash(counter||no_of_bits_to_return||input_string) is
                6767B05E 83A98040 6D94BEE3 3CBB8905 551B5451


    temp =
                                               D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


  V is
                                               D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    Hash(counter||no_of_bits_to_return||input_string) is
                54C5217B 5102D8DA 8BF1686E DBAB2BBC 0C11B0CC
```

```
    temp =
                54C5217B 5102D8DA 8BF1686E DBAB2BBC 0C11B0CC


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                               02 000001B8 00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    Hash(counter||no_of_bits_to_return||input_string) is
                B0F0AF23 4C24CF15 ECC8CB39 C233AACA 48FCCEEE


    temp =
                          54C5217B 5102D8DA 8BF1686E DBAB2BBC
        0C11B0CC B0F0AF23 4C24CF15 ECC8CB39 C233AACA 48FCCEEE


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                               03 000001B8 00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    Hash(counter||no_of_bits_to_return||input_string) is
                863DA881 FFCBB434 A6CCB7DA 2FB21018 3D9DB3CF


    temp =
                                              54C521 7B5102D8
        DA8BF168 6EDBAB2B BC0C11B0 CCB0F0AF 234C24CF 15ECC8CB
        39C233AA CA48FCCE EE863DA8 81FFCBB4 34A6CCB7 DA2FB210


  C is
                                              54C521 7B5102D8
        DA8BF168 6EDBAB2B BC0C11B0 CCB0F0AF 234C24CF 15ECC8CB
        39C233AA CA48FCCE EE863DA8 81FFCBB4 34A6CCB7 DA2FB210


----------------------------------------------------------------

First call to Generate
```

```
************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                              D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    w_i is
                 9F7CFF1E CA23E750 F6632696 9F11800F 12088BA6


    W is
                 9F7CFF1E CA23E750 F6632696 9F11800F 12088BA6


    ------------

    i = 2

    data is
                                              D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB8A


    w_i is
                 8E441D15 D888B3FE 12BF66FE 057494F4 546DE2F1


    W is
                         9F7CFF1E CA23E750 F6632696 9F11800F
        12088BA6 8E441D15 D888B3FE 12BF66FE 057494F4 546DE2F1
```

```
  returned_bits is
                          9F7CFF1E CA23E750 F6632696 9F11800F
        12088BA6 8E441D15 D888B3FE 12BF66FE 057494F4 546DE2F1


---------------------------

  Update V

    0x03||V is
                                             03D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    H is
                50888157 B42BE85F 4C53E8A1 B0AE46F9 91961027


  Updated values

  V is
                                               2554D5 BD43F7A4
        125B5D8C 8F83D79F E3B909AD CA2A80C3 5B80CA91 6C97F104
        702FC9DF A7D00ABE 4E198DB8 2CD75DD6 25C2A870 4F027DC1


  reseed_counter is
                                                 0000 00000002


rnd_val is
                          9F7CFF1E CA23E750 F6632696 9F11800F
        12088BA6 8E441D15 D888B3FE 12BF66FE 057494F4 546DE2F1


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

---------------------------

  Hashgen
```

```
    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                                2554D5 BD43F7A4
        125B5D8C 8F83D79F E3B909AD CA2A80C3 5B80CA91 6C97F104
        702FC9DF A7D00ABE 4E198DB8 2CD75DD6 25C2A870 4F027DC1


    w_i is
                 B77AA5C0 CD55BBCE ED7574AF 223AFD98 8C7EEC8E


    W is
                 B77AA5C0 CD55BBCE ED7574AF 223AFD98 8C7EEC8E


    ------------

    i = 2

    data is
                                                2554D5 BD43F7A4
        125B5D8C 8F83D79F E3B909AD CA2A80C3 5B80CA91 6C97F104
        702FC9DF A7D00ABE 4E198DB8 2CD75DD6 25C2A870 4F027DC2


    w_i is
                 FF4A94E5 E89D26A0 4F58FA79 F5E0D370 2D7A9A6A


    W is
                          B77AA5C0 CD55BBCE ED7574AF 223AFD98
        8C7EEC8E FF4A94E5 E89D26A0 4F58FA79 F5E0D370 2D7A9A6A


  returned_bits is
                          B77AA5C0 CD55BBCE ED7574AF 223AFD98
        8C7EEC8E FF4A94E5 E89D26A0 4F58FA79 F5E0D370 2D7A9A6A


---------------------------

  Update V

    0x03||V is
                                              032554D5 BD43F7A4
        125B5D8C 8F83D79F E3B909AD CA2A80C3 5B80CA91 6C97F104
        702FC9DF A7D00ABE 4E198DB8 2CD75DD6 25C2A870 4F027DC1
```

```
    H is
                4B2D04CB 62511A9A 13BDB8D9 BFBFB8A2 C42435B5


  Updated values

  V is
                                                7A19F7 3894FA7C
        ECE74EF4 FE5F82CB 9FC51B5E 96DB7172 7ECCEF60 8284B9CF
        A9F1FD8A BD460C58 9EF0E5FA C294E264 1A292DCA ED566588


  reseed_counter is
                                                 0000 00000003


rnd_val is
                          B77AA5C0 CD55BBCE ED7574AF 223AFD98
        8C7EEC8E FF4A94E5 E89D26A0 4F58FA79 F5E0D370 2D7A9A6A


###############################################################

Hash_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                               000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                               808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                               C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                 20 21222324
```

```
    PersonalizationString = <empty>

    AdditionalInput1 =
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##############################################################

**************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                    20 21222324


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                    00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    no_of_bits_to_return = 440

    ------------

    i = 1
```

```
counter||no_of_bits_to_return||input_string is
                  01 000001B8 00010203 04050607 08090A0B
    0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
    24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


Hash(counter||no_of_bits_to_return||input_string) is
             D08FB441 F2F4CB37 CF6C2420 A82C7427 ACF7FCFD


temp =
             D08FB441 F2F4CB37 CF6C2420 A82C7427 ACF7FCFD


------------

i = 2

counter||no_of_bits_to_return||input_string is
                  02 000001B8 00010203 04050607 08090A0B
    0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
    24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


Hash(counter||no_of_bits_to_return||input_string) is
             79901438 34A5C256 AB283936 6D96348C FE8C97AB


temp =
                     D08FB441 F2F4CB37 CF6C2420 A82C7427
    ACF7FCFD 79901438 34A5C256 AB283936 6D96348C FE8C97AB


------------

i = 3

counter||no_of_bits_to_return||input_string is
                  03 000001B8 00010203 04050607 08090A0B
    0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
    24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


Hash(counter||no_of_bits_to_return||input_string) is
             6767B05E 83A98040 6D94BEE3 3CBB8905 551B5451


temp =
                                          D08FB4 41F2F4CB
    37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
    366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89
```

```
  V is
                                                 D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    Hash(counter||no_of_bits_to_return||input_string) is
                54C5217B 5102D8DA 8BF1686E DBAB2BBC 0C11B0CC


    temp =
                54C5217B 5102D8DA 8BF1686E DBAB2BBC 0C11B0CC


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    Hash(counter||no_of_bits_to_return||input_string) is
                B0F0AF23 4C24CF15 ECC8CB39 C233AACA 48FCCEEE


    temp =
```

```
                        54C5217B 5102D8DA 8BF1686E DBAB2BBC
        0C11B0CC B0F0AF23 4C24CF15 ECC8CB39 C233AACA 48FCCEEE


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                               03 000001B8 00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    Hash(counter||no_of_bits_to_return||input_string) is
                863DA881 FFCBB434 A6CCB7DA 2FB21018 3D9DB3CF


    temp =
                                              54C521 7B5102D8
        DA8BF168 6EDBAB2B BC0C11B0 CCB0F0AF 234C24CF 15ECC8CB
        39C233AA CA48FCCE EE863DA8 81FFCBB4 34A6CCB7 DA2FB210


  C is
                                              54C521 7B5102D8
        DA8BF168 6EDBAB2B BC0C11B0 CCB0F0AF 234C24CF 15ECC8CB
        39C233AA CA48FCCE EE863DA8 81FFCBB4 34A6CCB7 DA2FB210


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input
                                              606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


--------------------------

  Process additional_input

    0x02||V||additional_input is
                           02D08F B441F2F4 CB37CF6C 2420A82C
```

```
        7427ACF7 FCFD7990 143834A5 C256AB28 39366D96 348CFE8C
        97AB6767 B05E83A9 80406D94 BEE33CBB 89606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    w=Hash(0x02||V||additional_input) is
                 9D19D4FF 31B805CA 44B1220A 8363DFCC F2F10DE2


    V is
                                              D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9635 2A186196 DD1F6D7A A334CB8A C3D1748B D62DC96B


---------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                              D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9635 2A186196 DD1F6D7A A334CB8A C3D1748B D62DC96B


    w_i is
                 E76B4EDD 5C865BC8 AFD809A5 9B69B429 AC7F4352


    W is
                 E76B4EDD 5C865BC8 AFD809A5 9B69B429 AC7F4352


    ------------

    i = 2

    data is
                                              D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9635 2A186196 DD1F6D7A A334CB8A C3D1748B D62DC96C


    w_i is
                 A579BCF3 F75E5624 9A3491F8 7C3CA684 8B0FAB25
```

```
    W is
                          E76B4EDD 5C865BC8 AFD809A5 9B69B429
        AC7F4352 A579BCF3 F75E5624 9A3491F8 7C3CA684 8B0FAB25


  returned_bits is
                          E76B4EDD 5C865BC8 AFD809A5 9B69B429
        AC7F4352 A579BCF3 F75E5624 9A3491F8 7C3CA684 8B0FAB25


---------------------------

  Update V

    0x03||V is
                                             03D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9635 2A186196 DD1F6D7A A334CB8A C3D1748B D62DC96B


    H is
                CA5C66D5 67C78BEF B7A32D13 387D5315 93268E18


  Updated values

  V is
                                               2554D5 BD43F7A4
        125B5D8C 8F83D79F E3B909AD CA2A80C3 5B80CA91 6C97F104
        702FC9E0 BEBDC53B 336D3712 DCD7C452 30F59459 43840994


  reseed_counter is
                                                0000 00000002


rnd_val is
                          E76B4EDD 5C865BC8 AFD809A5 9B69B429
        AC7F4352 A579BCF3 F75E5624 9A3491F8 7C3CA684 8B0FAB25


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320
```

```
  additional_input
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Process additional_input

    0x02||V||additional_input is
                            022554 D5BD43F7 A4125B5D 8C8F83D7
        9FE3B909 ADCA2A80 C35B80CA 916C97F1 04702FC9 E0BEBDC5
        3B336D37 12DCD7C4 5230F594 59438409 94A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    w=Hash(0x02||V||additional_input) is
                 FF5BDE25 5EE18D94 DB9ACE0C 1784FFD2 23E36123


    V is
                                                  2554D5 BD43F7A4
        125B5D8C 8F83D79F E3B909AD CA2A80C3 5B80CA91 6C97F104
        702FC9E1 BE19A360 924EC4A7 B872925E 487A942B 67676AB7


---------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                                  2554D5 BD43F7A4
        125B5D8C 8F83D79F E3B909AD CA2A80C3 5B80CA91 6C97F104
        702FC9E1 BE19A360 924EC4A7 B872925E 487A942B 67676AB7


    w_i is
                 6577B6B4 F87A9324 0B199FE5 1A3B3353 13683103


    W is
                 6577B6B4 F87A9324 0B199FE5 1A3B3353 13683103
```

```
    ------------

    i = 2

    data is
                                              2554D5 BD43F7A4
        125B5D8C 8F83D79F E3B909AD CA2A80C3 5B80CA91 6C97F104
        702FC9E1 BE19A360 924EC4A7 B872925E 487A942B 67676AB8


    w_i is
                DECE171E 3256FB7E 803586CA 4E45DD24 2EB01F70


    W is
                         6577B6B4 F87A9324 0B199FE5 1A3B3353
        13683103 DECE171E 3256FB7E 803586CA 4E45DD24 2EB01F70


  returned_bits is
                         6577B6B4 F87A9324 0B199FE5 1A3B3353
        13683103 DECE171E 3256FB7E 803586CA 4E45DD24 2EB01F70


---------------------------

  Update V

    0x03||V is
                                             032554D5 BD43F7A4
        125B5D8C 8F83D79F E3B909AD CA2A80C3 5B80CA91 6C97F104
        702FC9E1 BE19A360 924EC4A7 B872925E 487A942B 67676AB7


    H is
                DECE171E 3256FB7E 803586CA 4E45DD24 2EB01F70


  Updated values

  V is
                                               7A19F7 3894FA7C
        ECE74EF4 FE5F82CB 9FC51B5E 96DB7172 7ECCEF60 8284B9CF
        A9F1FD8D 1D51776A 1C4320BD C8F3C8D9 5A40D7CE 6D14D5FC


  reseed_counter is
                                                 0000 00000003


rnd_val is
```

```
                        6577B6B4 F87A9324 0B199FE5 1A3B3353
        13683103 DECE171E 3256FB7E 803586CA 4E45DD24 2EB01F70


###############################################################

Hash_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                              000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                              808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                              C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                 20 21222324


    PersonalizationString =
                                              404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

###############################################################

***************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                              000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
```

```
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                    20 21222324


    personal_str is
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                   000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
        01000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                 99B9537B 8427B8CE 23219A61 1CBE6106 44CF8503


    temp =
                 99B9537B 8427B8CE 23219A61 1CBE6106 44CF8503


    ------------

    i = 2
```

```
    counter||no_of_bits_to_return||input_string is
        02000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                 EEC5BA22 DE1AB212 C3D0858E 9E3B9026 D4E77D58


    temp =
                          99B9537B 8427B8CE 23219A61 1CBE6106
        44CF8503 EEC5BA22 DE1AB212 C3D0858E 9E3B9026 D4E77D58


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
        03000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                 E02E85A2 314CE3D7 4A93324B 27BDE85F 5498B7AC


    temp =
                                             99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


  V is
                                             99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                           0099B953 7B8427B8
```

```
    CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
    8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                            01 000001B8 0099B953 7B8427B8
    CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
    8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


Hash(counter||no_of_bits_to_return||input_string) is
             A70266F7 F91EC4D2 88731479 34CEAF2A 2CC35A0F


temp =
             A70266F7 F91EC4D2 88731479 34CEAF2A 2CC35A0F


------------

i = 2

counter||no_of_bits_to_return||input_string is
                            02 000001B8 0099B953 7B8427B8
    CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
    8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


Hash(counter||no_of_bits_to_return||input_string) is
             D5E00ABA E79DC660 5FABD6F5 F928E18C 63268E1A


temp =
                      A70266F7 F91EC4D2 88731479 34CEAF2A
    2CC35A0F D5E00ABA E79DC660 5FABD6F5 F928E18C 63268E1A


------------

i = 3

counter||no_of_bits_to_return||input_string is
                            03 000001B8 0099B953 7B8427B8
    CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
    8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                 F485DA6C BF0416DC DC5FB8BC 9C94B6BC 511E0813


    temp =
                                                A70266 F7F91EC4
         D2887314 7934CEAF 2A2CC35A 0FD5E00A BAE79DC6 605FABD6
         F5F928E1 8C63268E 1AF485DA 6CBF0416 DCDC5FB8 BC9C94B6


  C is
                                                A70266 F7F91EC4
         D2887314 7934CEAF 2A2CC35A 0FD5E00A BAE79DC6 605FABD6
         F5F928E1 8C63268E 1AF485DA 6CBF0416 DCDC5FB8 BC9C94B6


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                                99B953 7B8427B8
         CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
         8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


    w_i is
                 AB438BD3 B01A0AF8 5CFEE29F 7D7B7162 1C4908B9


    W is
                 AB438BD3 B01A0AF8 5CFEE29F 7D7B7162 1C4908B9
```

```
    ------------

    i = 2

    data is
                                                99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE9


    w_i is
                09124D43 0E7B406F B1086EA9 94C582E0 D656D989


    W is
                         AB438BD3 B01A0AF8 5CFEE29F 7D7B7162
        1C4908B9 09124D43 0E7B406F B1086EA9 94C582E0 D656D989


  returned_bits is
                         AB438BD3 B01A0AF8 5CFEE29F 7D7B7162
        1C4908B9 09124D43 0E7B406F B1086EA9 94C582E0 D656D989


---------------------------

  Update V

    0x03||V is
                                              0399B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


    H is
                5A78428C 33721011 3DA9EB00 17A5D327 B3372ACB


  Updated values

  V is
                                                40BBBA 737D467D
        A0AB94AE DA518D10 307192DF 13C4A5C4 DDC5B878 73237C5C
        84976472 0DB05097 A746C471 4C9A3BFA CBCCC612 BAFB7D6A


  reseed_counter is
                                                  0000 00000002


rnd_val is
```

```
                        AB438BD3 B01A0AF8 5CFEE29F 7D7B7162
        1C4908B9 09124D43 0E7B406F B1086EA9 94C582E0 D656D989


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                            40BBBA 737D467D
        A0AB94AE DA518D10 307192DF 13C4A5C4 DDC5B878 73237C5C
        84976472 0DB05097 A746C471 4C9A3BFA CBCCC612 BAFB7D6A


    w_i is
                29D9098F 987E7005 314A0F51 B3DD2B81 22F4AED7


    W is
                29D9098F 987E7005 314A0F51 B3DD2B81 22F4AED7


    ------------

    i = 2

    data is
                                            40BBBA 737D467D
        A0AB94AE DA518D10 307192DF 13C4A5C4 DDC5B878 73237C5C
        84976472 0DB05097 A746C471 4C9A3BFA CBCCC612 BAFB7D6B


    w_i is
                06735DE6 AD5DDBF2 23177C1E 5F3AEBC5 2FAB90B9
```

```
    W is
                          29D9098F 987E7005 314A0F51 B3DD2B81
        22F4AED7 06735DE6 AD5DDBF2 23177C1E 5F3AEBC5 2FAB90B9


  returned_bits is
                          29D9098F 987E7005 314A0F51 B3DD2B81
        22F4AED7 06735DE6 AD5DDBF2 23177C1E 5F3AEBC5 2FAB90B9


---------------------------

  Update V

    0x03||V is
                                            0340BBBA 737D467D
        A0AB94AE DA518D10 307192DF 13C4A5C4 DDC5B878 73237C5C
        84976472 0DB05097 A746C471 4C9A3BFA CBCCC612 BAFB7D6A


    H is
                800B98DD 1013A49B 0851E244 7961FB97 F3733076


  Updated values

  V is
                                              E7BE21 6B766542
        733407C3 53865BBF 5A9E5639 239A85CF 98AD563E D3832833
        7A908D54 1A1F1002 D24EEEE6 C1AB2256 220B2163 6B0B4298


  reseed_counter is
                                                0000 00000003


rnd_val is
                          29D9098F 987E7005 314A0F51 B3DD2B81
        22F4AED7 06735DE6 AD5DDBF2 23177C1E 5F3AEBC5 2FAB90B9


################################################################

Hash_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "NOT ENABLED"
```

```
    EntropyInput =
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                    20 21222324


    PersonalizationString =
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    nonce is
                                                    20 21222324


    personal_str is
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                   000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
        01000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                 99B9537B 8427B8CE 23219A61 1CBE6106 44CF8503


    temp =
                 99B9537B 8427B8CE 23219A61 1CBE6106 44CF8503


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
        02000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
```

```
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                 EEC5BA22 DE1AB212 C3D0858E 9E3B9026 D4E77D58


    temp =
                          99B9537B 8427B8CE 23219A61 1CBE6106
        44CF8503 EEC5BA22 DE1AB212 C3D0858E 9E3B9026 D4E77D58


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
        03000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                 E02E85A2 314CE3D7 4A93324B 27BDE85F 5498B7AC


    temp =
                                              99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


  V is
                                              99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            0099B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8
```

```
no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                            01 000001B8 0099B953 7B8427B8
    CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
    8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


Hash(counter||no_of_bits_to_return||input_string) is
             A70266F7 F91EC4D2 88731479 34CEAF2A 2CC35A0F


temp =
             A70266F7 F91EC4D2 88731479 34CEAF2A 2CC35A0F


------------

i = 2

counter||no_of_bits_to_return||input_string is
                            02 000001B8 0099B953 7B8427B8
    CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
    8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


Hash(counter||no_of_bits_to_return||input_string) is
             D5E00ABA E79DC660 5FABD6F5 F928E18C 63268E1A


temp =
                      A70266F7 F91EC4D2 88731479 34CEAF2A
    2CC35A0F D5E00ABA E79DC660 5FABD6F5 F928E18C 63268E1A


------------

i = 3

counter||no_of_bits_to_return||input_string is
                            03 000001B8 0099B953 7B8427B8
    CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
    8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


Hash(counter||no_of_bits_to_return||input_string) is
             F485DA6C BF0416DC DC5FB8BC 9C94B6BC 511E0813
```

```
    temp =
                                                A70266 F7F91EC4
        D2887314 7934CEAF 2A2CC35A 0FD5E00A BAE79DC6 605FABD6
        F5F928E1 8C63268E 1AF485DA 6CBF0416 DCDC5FB8 BC9C94B6


  C is
                                                A70266 F7F91EC4
        D2887314 7934CEAF 2A2CC35A 0FD5E00A BAE79DC6 605FABD6
        F5F928E1 8C63268E 1AF485DA 6CBF0416 DCDC5FB8 BC9C94B6


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


---------------------------

  Process additional_input

    0x02||V||additional_input is
                            0299B9 537B8427 B8CE2321 9A611CBE
        610644CF 8503EEC5 BA22DE1A B212C3D0 858E9E3B 9026D4E7
        7D58E02E 85A2314C E3D74A93 324B27BD E8606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    w=Hash(0x02||V||additional_input) is
                 AC253890 BEDFF91D BCBB8272 D02C21DA F03A34F0


    V is
                                                99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 D2FA200E 17C027A3 5EECCF56 A776B50D 3B61F2D8
```

```
---------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                                99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 D2FA200E 17C027A3 5EECCF56 A776B50D 3B61F2D8


    w_i is
                F1BC207E EB432886 094421F3 A63493FA 666DC2C4


    W is
                F1BC207E EB432886 094421F3 A63493FA 666DC2C4


    ------------

    i = 2

    data is
                                                99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 D2FA200E 17C027A3 5EECCF56 A776B50D 3B61F2D9


    w_i is
                2AC598CA 0986F692 9FE367F8 0311CA5A B9880D80


    W is
                         F1BC207E EB432886 094421F3 A63493FA
        666DC2C4 2AC598CA 0986F692 9FE367F8 0311CA5A B9880D80


  returned_bits is
                         F1BC207E EB432886 094421F3 A63493FA
        666DC2C4 2AC598CA 0986F692 9FE367F8 0311CA5A B9880D80


---------------------------

  Update V
```

```
    0x03||V is
                                                0399B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 D2FA200E 17C027A3 5EECCF56 A776B50D 3B61F2D8


    H is
                 FCC41757 C0FC70A2 8251F561 A52504F5 BD602531


  Updated values

  V is
                                                  40BBBA 737D467D
        A0AB94AE DA518D10 307192DF 13C4A5C4 DDC5B878 73237C5C
        84976473 5C215DF3 F3B11E20 4DFDC8CF 297819BB B55EACC0


  reseed_counter is
                                                    0000 00000002


rnd_val is
                          F1BC207E EB432886 094421F3 A63493FA
        666DC2C4 2AC598CA 0986F692 9FE367F8 0311CA5A B9880D80


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


--------------------------

  Process additional_input

    0x02||V||additional_input is
                            0240BB BA737D46 7DA0AB94 AEDA518D
        10307192 DF13C4A5 C4DDC5B8 7873237C 5C849764 735C215D
        F3F3B11E 204DFDC8 CF297819 BBB55EAC C0A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
```

```
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    w=Hash(0x02||V||additional_input) is
                 108B9D20 24618A08 D862EABD CACBFC4D 261DB816


    V is
                                                40BBBA 737D467D
        A0AB94AE DA518D10 307192DF 13C4A5C4 DDC5B878 73237C5C
        84976473 6CACFB14 1812A829 2660B38C F4441608 DB7C64D6


----------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                                40BBBA 737D467D
        A0AB94AE DA518D10 307192DF 13C4A5C4 DDC5B878 73237C5C
        84976473 6CACFB14 1812A829 2660B38C F4441608 DB7C64D6


    w_i is
                 CEF3D601 F2744E37 16A9D04F 9AA8481A 98D74518


    W is
                 CEF3D601 F2744E37 16A9D04F 9AA8481A 98D74518


    ------------

    i = 2

    data is
                                                40BBBA 737D467D
        A0AB94AE DA518D10 307192DF 13C4A5C4 DDC5B878 73237C5C
        84976473 6CACFB14 1812A829 2660B38C F4441608 DB7C64D7


    w_i is
                 D223014F EF8C8456 2708F833 A99817DD 62B7C90B


    W is
```

```
                        CEF3D601 F2744E37 16A9D04F 9AA8481A
        98D74518 D223014F EF8C8456 2708F833 A99817DD 62B7C90B


  returned_bits is
                        CEF3D601 F2744E37 16A9D04F 9AA8481A
        98D74518 D223014F EF8C8456 2708F833 A99817DD 62B7C90B


---------------------------

  Update V

    0x03||V is
                                            0340BBBA 737D467D
        A0AB94AE DA518D10 307192DF 13C4A5C4 DDC5B878 73237C5C
        84976473 6CACFB14 1812A829 2660B38C F4441608 DB7C64D6


    H is
                3018C221 DFEEDDF0 43315A7D A9F4DC3A 91A0E9F1


  Updated values

  V is
                                              E7BE21 6B766542
        733407C3 53865BBF 5A9E5639 239A85CF 98AD563E D3832833
        7A908D55 2928E3C4 12F60BF3 D6511221 7B1551FC 29B9E37F


  reseed_counter is
                                                0000 00000003


rnd_val is
                        CEF3D601 F2744E37 16A9D04F 9AA8481A
        98D74518 D223014F EF8C8456 2708F833 A99817DD 62B7C90B


##############################################################

Hash_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                              000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
```

```
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                    20 21222324


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                    20 21222324


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                    00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324
```

```
no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                  01 000001B8 00010203 04050607 08090A0B
    0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
    24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


Hash(counter||no_of_bits_to_return||input_string) is
             D08FB441 F2F4CB37 CF6C2420 A82C7427 ACF7FCFD


temp =
             D08FB441 F2F4CB37 CF6C2420 A82C7427 ACF7FCFD


------------

i = 2

counter||no_of_bits_to_return||input_string is
                  02 000001B8 00010203 04050607 08090A0B
    0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
    24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


Hash(counter||no_of_bits_to_return||input_string) is
             79901438 34A5C256 AB283936 6D96348C FE8C97AB


temp =
                     D08FB441 F2F4CB37 CF6C2420 A82C7427
    ACF7FCFD 79901438 34A5C256 AB283936 6D96348C FE8C97AB


------------

i = 3

counter||no_of_bits_to_return||input_string is
                  03 000001B8 00010203 04050607 08090A0B
    0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
    24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


Hash(counter||no_of_bits_to_return||input_string) is
             6767B05E 83A98040 6D94BEE3 3CBB8905 551B5451
```

```
    temp =
                                                D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


  V is
                                                D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


----------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                               00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    Hash(counter||no_of_bits_to_return||input_string) is
                 54C5217B 5102D8DA 8BF1686E DBAB2BBC 0C11B0CC


    temp =
                 54C5217B 5102D8DA 8BF1686E DBAB2BBC 0C11B0CC


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                               02 000001B8 00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                 B0F0AF23 4C24CF15 ECC8CB39 C233AACA 48FCCEEE


    temp =
                          54C5217B 5102D8DA 8BF1686E DBAB2BBC
        0C11B0CC B0F0AF23 4C24CF15 ECC8CB39 C233AACA 48FCCEEE


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                                03 000001B8 00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    Hash(counter||no_of_bits_to_return||input_string) is
                 863DA881 FFCBB434 A6CCB7DA 2FB21018 3D9DB3CF


    temp =
                                               54C521 7B5102D8
        DA8BF168 6EDBAB2B BC0C11B0 CCB0F0AF 234C24CF 15ECC8CB
        39C233AA CA48FCCE EE863DA8 81FFCBB4 34A6CCB7 DA2FB210


  C is
                                               54C521 7B5102D8
        DA8BF168 6EDBAB2B BC0C11B0 CCB0F0AF 234C24CF 15ECC8CB
        39C233AA CA48FCCE EE863DA8 81FFCBB4 34A6CCB7 DA2FB210


-----------------------------------------------------------------

First call to Generate

*****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

Generate FAILED: Reseed is required
-----------------------------------------------------------------
```

```
Hash_DRBG_Reseed_algorithm

  entropy_input
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  additional_input <empty>

----------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                           01D08F B441F2F4 CB37CF6C 2420A82C
        7427ACF7 FCFD7990 143834A5 C256AB28 39366D96 348CFE8C
        97AB6767 B05E83A9 80406D94 BEE33CBB 89808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                01000001 B801D08F B441F2F4 CB37CF6C 2420A82C
        7427ACF7 FCFD7990 143834A5 C256AB28 39366D96 348CFE8C
        97AB6767 B05E83A9 80406D94 BEE33CBB 89808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    Hash(counter||no_of_bits_to_return||input_string) is
                0A0441A5 2BEDF794 F5AA627B CBD81F93 E011D51F


    temp =
                0A0441A5 2BEDF794 F5AA627B CBD81F93 E011D51F


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                02000001 B801D08F B441F2F4 CB37CF6C 2420A82C
        7427ACF7 FCFD7990 143834A5 C256AB28 39366D96 348CFE8C
        97AB6767 B05E83A9 80406D94 BEE33CBB 89808182 83848586
```

```
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    Hash(counter||no_of_bits_to_return||input_string) is
                 3474802C 37507675 51B45B69 F3D35939 C932AE1C


    temp =
                          0A0441A5 2BEDF794 F5AA627B CBD81F93
        E011D51F 3474802C 37507675 51B45B69 F3D35939 C932AE1C


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                 03000001 B801D08F B441F2F4 CB37CF6C 2420A82C
        7427ACF7 FCFD7990 143834A5 C256AB28 39366D96 348CFE8C
        97AB6767 B05E83A9 80406D94 BEE33CBB 89808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    Hash(counter||no_of_bits_to_return||input_string) is
                 B7C9894F B88465E0 CFD1CC26 1E22C5CB 08918264


    temp =
                                              0A0441 A52BEDF7
        94F5AA62 7BCBD81F 93E011D5 1F347480 2C375076 7551B45B
        69F3D359 39C932AE 1CB7C989 4FB88465 E0CFD1CC 261E22C5


  V is
                                              0A0441 A52BEDF7
        94F5AA62 7BCBD81F 93E011D5 1F347480 2C375076 7551B45B
        69F3D359 39C932AE 1CB7C989 4FB88465 E0CFD1CC 261E22C5


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            000A0441 A52BEDF7
        94F5AA62 7BCBD81F 93E011D5 1F347480 2C375076 7551B45B
        69F3D359 39C932AE 1CB7C989 4FB88465 E0CFD1CC 261E22C5


    no_of_bits_to_return = 440
```

```
------------

i = 1

counter||no_of_bits_to_return||input_string is
                            01 000001B8 000A0441 A52BEDF7
    94F5AA62 7BCBD81F 93E011D5 1F347480 2C375076 7551B45B
    69F3D359 39C932AE 1CB7C989 4FB88465 E0CFD1CC 261E22C5


Hash(counter||no_of_bits_to_return||input_string) is
             0411C8B0 DBA756E8 842B3FB0 2D2FEB7C EEA56742


temp =
             0411C8B0 DBA756E8 842B3FB0 2D2FEB7C EEA56742


------------

i = 2

counter||no_of_bits_to_return||input_string is
                            02 000001B8 000A0441 A52BEDF7
    94F5AA62 7BCBD81F 93E011D5 1F347480 2C375076 7551B45B
    69F3D359 39C932AE 1CB7C989 4FB88465 E0CFD1CC 261E22C5


Hash(counter||no_of_bits_to_return||input_string) is
             EE9379C9 0E6D3B2F 1010D40F 4F4DCADA 61CFDFB4


temp =
                       0411C8B0 DBA756E8 842B3FB0 2D2FEB7C
    EEA56742 EE9379C9 0E6D3B2F 1010D40F 4F4DCADA 61CFDFB4


------------

i = 3

counter||no_of_bits_to_return||input_string is
                            03 000001B8 000A0441 A52BEDF7
    94F5AA62 7BCBD81F 93E011D5 1F347480 2C375076 7551B45B
    69F3D359 39C932AE 1CB7C989 4FB88465 E0CFD1CC 261E22C5


Hash(counter||no_of_bits_to_return||input_string) is
             8AF847CA CC4C92C6 144485C2 27CA05B7 A3796150
```

```
    temp =
                                                0411C8 B0DBA756
        E8842B3F B02D2FEB 7CEEA567 42EE9379 C90E6D3B 2F1010D4
        0F4F4DCA DA61CFDF B48AF847 CACC4C92 C6144485 C227CA05


  C is
                                                0411C8 B0DBA756
        E8842B3F B02D2FEB 7CEEA567 42EE9379 C90E6D3B 2F1010D4
        0F4F4DCA DA61CFDF B48AF847 CACC4C92 C6144485 C227CA05


************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                                0A0441 A52BEDF7
        94F5AA62 7BCBD81F 93E011D5 1F347480 2C375076 7551B45B
        69F3D359 39C932AE 1CB7C989 4FB88465 E0CFD1CC 261E22C5


    w_i is
                56EF4913 373994D5 539F4D7D 17AFE744 8CDF5E72


    W is
                56EF4913 373994D5 539F4D7D 17AFE744 8CDF5E72


    ------------

    i = 2

    data is
                                                0A0441 A52BEDF7
        94F5AA62 7BCBD81F 93E011D5 1F347480 2C375076 7551B45B
        69F3D359 39C932AE 1CB7C989 4FB88465 E0CFD1CC 261E22C6
```

```
    w_i is
                416CC6A7 1A340059 FA0D5AE5 26B23250 C46C0944


    W is
                         56EF4913 373994D5 539F4D7D 17AFE744
         8CDF5E72 416CC6A7 1A340059 FA0D5AE5 26B23250 C46C0944


  returned_bits is
                         56EF4913 373994D5 539F4D7D 17AFE744
         8CDF5E72 416CC6A7 1A340059 FA0D5AE5 26B23250 C46C0944


---------------------------

  Update V

    0x03||V is
                                            030A0441 A52BEDF7
         94F5AA62 7BCBD81F 93E011D5 1F347480 2C375076 7551B45B
         69F3D359 39C932AE 1CB7C989 4FB88465 E0CFD1CC 261E22C5


    H is
                2681DFB1 64FD2DE2 4340EDAF 404D2DC2 E732C72E


  Updated values

  V is
                                              0E160A 5607954E
         7D79D5A2 2BF9080B 10CEB73C 622307F9 F545BDB1 A461C52F
         79432124 3AACE23F 363FEFB3 5DC5BEA7 E7314414 CF78B3F9


  reseed_counter is
                                                0000 00000002


rnd_val is
                         56EF4913 373994D5 539F4D7D 17AFE744
         8CDF5E72 416CC6A7 1A340059 FA0D5AE5 26B23250 C46C0944


---------------------------------------------------------------

Second call to Generate

***************************************************************
```

```
Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                            010E16 0A560795 4E7D79D5 A22BF908
        0B10CEB7 3C622307 F9F545BD B1A461C5 2F794321 243AACE2
        3F363FEF B35DC5BE A7E73144 14CF78B3 F9C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                01000001 B8010E16 0A560795 4E7D79D5 A22BF908
        0B10CEB7 3C622307 F9F545BD B1A461C5 2F794321 243AACE2
        3F363FEF B35DC5BE A7E73144 14CF78B3 F9C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                DC24DF10 2FA9F96C C1CFF8C1 16C79D14 97D7C27B


    temp =
                DC24DF10 2FA9F96C C1CFF8C1 16C79D14 97D7C27B
```

```
    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                 02000001 B8010E16 0A560795 4E7D79D5 A22BF908
        0B10CEB7 3C622307 F9F545BD B1A461C5 2F794321 243AACE2
        3F363FEF B35DC5BE A7E73144 14CF78B3 F9C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                 BA5BA801 E1562193 353F31E3 22395784 69B80F2F


    temp =
                           DC24DF10 2FA9F96C C1CFF8C1 16C79D14
        97D7C27B BA5BA801 E1562193 353F31E3 22395784 69B80F2F


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                 03000001 B8010E16 0A560795 4E7D79D5 A22BF908
        0B10CEB7 3C622307 F9F545BD B1A461C5 2F794321 243AACE2
        3F363FEF B35DC5BE A7E73144 14CF78B3 F9C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                 51645437 28717F17 1FDB02B2 AD5795F2 3D794EBE


    temp =
                                              DC24DF 102FA9F9
        6CC1CFF8 C116C79D 1497D7C2 7BBA5BA8 01E15621 93353F31
        E3223957 8469B80F 2F516454 3728717F 171FDB02 B2AD5795


  V is
                                              DC24DF 102FA9F9
        6CC1CFF8 C116C79D 1497D7C2 7BBA5BA8 01E15621 93353F31
        E3223957 8469B80F 2F516454 3728717F 171FDB02 B2AD5795


---------------------------
```

```
Hash_df - Generate C - Step 4

  0x00||V is
                                          00DC24DF 102FA9F9
      6CC1CFF8 C116C79D 1497D7C2 7BBA5BA8 01E15621 93353F31
      E3223957 8469B80F 2F516454 3728717F 171FDB02 B2AD5795


  no_of_bits_to_return = 440

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                             01 000001B8 00DC24DF 102FA9F9
      6CC1CFF8 C116C79D 1497D7C2 7BBA5BA8 01E15621 93353F31
      E3223957 8469B80F 2F516454 3728717F 171FDB02 B2AD5795


  Hash(counter||no_of_bits_to_return||input_string) is
               FFAF4566 5B110CA1 335A3FCE 73A7981D 0FD5C8D9


  temp =
               FFAF4566 5B110CA1 335A3FCE 73A7981D 0FD5C8D9


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                             02 000001B8 00DC24DF 102FA9F9
      6CC1CFF8 C116C79D 1497D7C2 7BBA5BA8 01E15621 93353F31
      E3223957 8469B80F 2F516454 3728717F 171FDB02 B2AD5795


  Hash(counter||no_of_bits_to_return||input_string) is
               03F65FAA 46A3D597 BF34C4E0 CC167560 AB94EC10


  temp =
                       FFAF4566 5B110CA1 335A3FCE 73A7981D
      0FD5C8D9 03F65FAA 46A3D597 BF34C4E0 CC167560 AB94EC10


  ------------

  i = 3
```

```
    counter||no_of_bits_to_return||input_string is
                                03 000001B8 00DC24DF 102FA9F9
        6CC1CFF8 C116C79D 1497D7C2 7BBA5BA8 01E15621 93353F31
        E3223957 8469B80F 2F516454 3728717F 171FDB02 B2AD5795


    Hash(counter||no_of_bits_to_return||input_string) is
                 D6415F37 83B01567 891B5766 2ABB39CD 3B7734E9


    temp =
                                               FFAF45 665B110C
        A1335A3F CE73A798 1D0FD5C8 D903F65F AA46A3D5 97BF34C4
        E0CC1675 60AB94EC 10D6415F 3783B015 67891B57 662ABB39


  C is
                                               FFAF45 665B110C
        A1335A3F CE73A798 1D0FD5C8 D903F65F AA46A3D5 97BF34C4
        E0CC1675 60AB94EC 10D6415F 3783B015 67891B57 662ABB39


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                               DC24DF 102FA9F9
        6CC1CFF8 C116C79D 1497D7C2 7BBA5BA8 01E15621 93353F31
        E3223957 8469B80F 2F516454 3728717F 171FDB02 B2AD5795


    w_i is
                 575B37A2 739814F9 66C63B60 A2C4F149 CA9ACC84


    W is
                 575B37A2 739814F9 66C63B60 A2C4F149 CA9ACC84
```

```
    ------------

    i = 2

    data is
                                                DC24DF 102FA9F9
        6CC1CFF8 C116C79D 1497D7C2 7BBA5BA8 01E15621 93353F31
        E3223957 8469B80F 2F516454 3728717F 171FDB02 B2AD5796


    w_i is
                 FC4B2549 3289B085 C67B2E30 F5F0B99A 2C349E2A


    W is
                          575B37A2 739814F9 66C63B60 A2C4F149
        CA9ACC84 FC4B2549 3289B085 C67B2E30 F5F0B99A 2C349E2A


  returned_bits is
                          575B37A2 739814F9 66C63B60 A2C4F149
        CA9ACC84 FC4B2549 3289B085 C67B2E30 F5F0B99A 2C349E2A


---------------------------

  Update V

    0x03||V is
                                               03DC24DF 102FA9F9
        6CC1CFF8 C116C79D 1497D7C2 7BBA5BA8 01E15621 93353F31
        E3223957 8469B80F 2F516454 3728717F 171FDB02 B2AD5795


    H is
                 756401AD FDF039BC B59817FD 00828E2F 56BF8C85


  Updated values

  V is
                                                DBD424 768ABB06
        0DF52A38 8F8A6F35 31A7AD8B 54BE5207 AC27F9F7 2AF473F6
        C3EE4FCD 5A794EA9 3E17DF70 24443991 7F2B8489 6F979F54


  reseed_counter is
                                                  0000 00000002
```

```
rnd_val is
                        575B37A2 739814F9 66C63B60 A2C4F149
        CA9ACC84 FC4B2549 3289B085 C67B2E30 F5F0B99A 2C349E2A


##############################################################

Hash_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                              000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                              808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                              C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  20 21222324


    PersonalizationString = <empty>

    AdditionalInput1 =
                                              606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                              A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##############################################################
```

```
************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                    20 21222324


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                    00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                        01 000001B8 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    Hash(counter||no_of_bits_to_return||input_string) is
                 D08FB441 F2F4CB37 CF6C2420 A82C7427 ACF7FCFD


    temp =
                 D08FB441 F2F4CB37 CF6C2420 A82C7427 ACF7FCFD


    ------------

    i = 2
```

```
    counter||no_of_bits_to_return||input_string is
                        02 000001B8 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    Hash(counter||no_of_bits_to_return||input_string) is
                 79901438 34A5C256 AB283936 6D96348C FE8C97AB


    temp =
                           D08FB441 F2F4CB37 CF6C2420 A82C7427
        ACF7FCFD 79901438 34A5C256 AB283936 6D96348C FE8C97AB


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                        03 000001B8 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    Hash(counter||no_of_bits_to_return||input_string) is
                 6767B05E 83A98040 6D94BEE3 3CBB8905 551B5451


    temp =
                                              D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


  V is
                                              D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    no_of_bits_to_return = 440
```

```
------------

i = 1

counter||no_of_bits_to_return||input_string is
                            01 000001B8 00D08FB4 41F2F4CB
    37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
    366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


Hash(counter||no_of_bits_to_return||input_string) is
             54C5217B 5102D8DA 8BF1686E DBAB2BBC 0C11B0CC


temp =
             54C5217B 5102D8DA 8BF1686E DBAB2BBC 0C11B0CC


------------

i = 2

counter||no_of_bits_to_return||input_string is
                            02 000001B8 00D08FB4 41F2F4CB
    37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
    366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


Hash(counter||no_of_bits_to_return||input_string) is
             B0F0AF23 4C24CF15 ECC8CB39 C233AACA 48FCCEEE


temp =
                      54C5217B 5102D8DA 8BF1686E DBAB2BBC
    0C11B0CC B0F0AF23 4C24CF15 ECC8CB39 C233AACA 48FCCEEE


------------

i = 3

counter||no_of_bits_to_return||input_string is
                            03 000001B8 00D08FB4 41F2F4CB
    37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
    366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


Hash(counter||no_of_bits_to_return||input_string) is
             863DA881 FFCBB434 A6CCB7DA 2FB21018 3D9DB3CF
```

```
    temp =
                                                54C521 7B5102D8
        DA8BF168 6EDBAB2B BC0C11B0 CCB0F0AF 234C24CF 15ECC8CB
        39C233AA CA48FCCE EE863DA8 81FFCBB4 34A6CCB7 DA2FB210


  C is
                                                54C521 7B5102D8
        DA8BF168 6EDBAB2B BC0C11B0 CCB0F0AF 234C24CF 15ECC8CB
        39C233AA CA48FCCE EE863DA8 81FFCBB4 34A6CCB7 DA2FB210


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01D0 8FB441F2 F4CB37CF 6C2420A8 2C7427AC F7FCFD79
        90143834 A5C256AB 2839366D 96348CFE 8C97AB67 67B05E83
```

```
    A980406D 94BEE33C BB898081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                                      010000
    01B801D0 8FB441F2 F4CB37CF 6C2420A8 2C7427AC F7FCFD79
    90143834 A5C256AB 2839366D 96348CFE 8C97AB67 67B05E83
    A980406D 94BEE33C BB898081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Hash(counter||no_of_bits_to_return||input_string) is
             8FDEC9E6 189636F0 A5CE53E8 1C13AC93 84FAFBA0


temp =
             8FDEC9E6 189636F0 A5CE53E8 1C13AC93 84FAFBA0


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
    01B801D0 8FB441F2 F4CB37CF 6C2420A8 2C7427AC F7FCFD79
    90143834 A5C256AB 2839366D 96348CFE 8C97AB67 67B05E83
    A980406D 94BEE33C BB898081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Hash(counter||no_of_bits_to_return||input_string) is
             EE50C1E2 C8A099DE 41D8CC7A 31429E8C 8C8880E3


temp =
```

```
                        8FDEC9E6 189636F0 A5CE53E8 1C13AC93
        84FAFBA0 EE50C1E2 C8A099DE 41D8CC7A 31429E8C 8C8880E3


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                                                          030000
        01B801D0 8FB441F2 F4CB37CF 6C2420A8 2C7427AC F7FCFD79
        90143834 A5C256AB 2839366D 96348CFE 8C97AB67 67B05E83
        A980406D 94BEE33C BB898081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    Hash(counter||no_of_bits_to_return||input_string) is
                 B45D89DB 612CD9D2 8A55C0F0 D1F8F98B 1791FF77


    temp =
                                            8FDEC9 E6189636
        F0A5CE53 E81C13AC 9384FAFB A0EE50C1 E2C8A099 DE41D8CC
        7A31429E 8C8C8880 E3B45D89 DB612CD9 D28A55C0 F0D1F8F9


  V is
                                            8FDEC9 E6189636
        F0A5CE53 E81C13AC 9384FAFB A0EE50C1 E2C8A099 DE41D8CC
        7A31429E 8C8C8880 E3B45D89 DB612CD9 D28A55C0 F0D1F8F9


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                          008FDEC9 E6189636
        F0A5CE53 E81C13AC 9384FAFB A0EE50C1 E2C8A099 DE41D8CC
        7A31429E 8C8C8880 E3B45D89 DB612CD9 D28A55C0 F0D1F8F9


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
```

```
                           01 000001B8 008FDEC9 E6189636
    F0A5CE53 E81C13AC 9384FAFB A0EE50C1 E2C8A099 DE41D8CC
    7A31429E 8C8C8880 E3B45D89 DB612CD9 D28A55C0 F0D1F8F9


Hash(counter||no_of_bits_to_return||input_string) is
             97D07631 B22F7C95 7F19F844 F4DC2AFA 6FF97C35


temp =
             97D07631 B22F7C95 7F19F844 F4DC2AFA 6FF97C35


------------

i = 2

counter||no_of_bits_to_return||input_string is
                           02 000001B8 008FDEC9 E6189636
    F0A5CE53 E81C13AC 9384FAFB A0EE50C1 E2C8A099 DE41D8CC
    7A31429E 8C8C8880 E3B45D89 DB612CD9 D28A55C0 F0D1F8F9


Hash(counter||no_of_bits_to_return||input_string) is
             66189821 6991D15B DA75BBD0 5EDF8A0F A80CCAB9


temp =
                      97D07631 B22F7C95 7F19F844 F4DC2AFA
    6FF97C35 66189821 6991D15B DA75BBD0 5EDF8A0F A80CCAB9


------------

i = 3

counter||no_of_bits_to_return||input_string is
                           03 000001B8 008FDEC9 E6189636
    F0A5CE53 E81C13AC 9384FAFB A0EE50C1 E2C8A099 DE41D8CC
    7A31429E 8C8C8880 E3B45D89 DB612CD9 D28A55C0 F0D1F8F9


Hash(counter||no_of_bits_to_return||input_string) is
             5195F479 CD762022 35102EF6 27291945 8BCA75D5


temp =
                                          97D076 31B22F7C
    957F19F8 44F4DC2A FA6FF97C 35661898 216991D1 5BDA75BB
    D05EDF8A 0FA80CCA B95195F4 79CD7620 2235102E F6272919
```

```
  C is
                                                97D076 31B22F7C
        957F19F8 44F4DC2A FA6FF97C 35661898 216991D1 5BDA75BB
        D05EDF8A 0FA80CCA B95195F4 79CD7620 2235102E F6272919


****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                                8FDEC9 E6189636
        F0A5CE53 E81C13AC 9384FAFB A0EE50C1 E2C8A099 DE41D8CC
        7A31429E 8C8C8880 E3B45D89 DB612CD9 D28A55C0 F0D1F8F9


    w_i is
                183C242A 1430E46C 4ED70B4D BE1BF9AB 0AB8721C


    W is
                183C242A 1430E46C 4ED70B4D BE1BF9AB 0AB8721C


    ------------

    i = 2

    data is
                                                8FDEC9 E6189636
        F0A5CE53 E81C13AC 9384FAFB A0EE50C1 E2C8A099 DE41D8CC
        7A31429E 8C8C8880 E3B45D89 DB612CD9 D28A55C0 F0D1F8FA


    w_i is
                DCA2A2D1 820AD6F6 C9568585 43B2AA19 1D8D1287
```

```
    W is
                          183C242A 1430E46C 4ED70B4D BE1BF9AB
         0AB8721C DCA2A2D1 820AD6F6 C9568585 43B2AA19 1D8D1287


  returned_bits is
                          183C242A 1430E46C 4ED70B4D BE1BF9AB
         0AB8721C DCA2A2D1 820AD6F6 C9568585 43B2AA19 1D8D1287


---------------------------

  Update V

    0x03||V is
                                              038FDEC9 E6189636
         F0A5CE53 E81C13AC 9384FAFB A0EE50C1 E2C8A099 DE41D8CC
         7A31429E 8C8C8880 E3B45D89 DB612CD9 D28A55C0 F0D1F8F9


    H is
                 4C6A1544 99C73778 B037DE2C 2EB36123 8ADB312A


  Updated values

  V is
                                                27AF40 17CAC5B3
         8624E84C 2D10EFD7 8DF4F477 D654695A 0432326B 3A1C4E88
         4A902228 E89EAA90 36CD2AF7 05668126 2372C713 71D4533D


  reseed_counter is
                                                  0000 00000002


rnd_val is
                          183C242A 1430E46C 4ED70B4D BE1BF9AB
         0AB8721C DCA2A2D1 820AD6F6 C9568585 43B2AA19 1D8D1287


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input
```

```
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
-------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  additional_input
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0127 AF4017CA C5B38624 E84C2D10 EFD78DF4 F477D654
        695A0432 326B3A1C 4E884A90 2228E89E AA9036CD 2AF70566
        81262372 C71371D4 533DC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                          010000
        01B80127 AF4017CA C5B38624 E84C2D10 EFD78DF4 F477D654
        695A0432 326B3A1C 4E884A90 2228E89E AA9036CD 2AF70566
        81262372 C71371D4 533DC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
```

```
Hash(counter||no_of_bits_to_return||input_string) is
             2C9C0D80 03E34023 BE5B63FD B9D224B4 250CC815


temp =
             2C9C0D80 03E34023 BE5B63FD B9D224B4 250CC815


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
    01B80127 AF4017CA C5B38624 E84C2D10 EFD78DF4 F477D654
    695A0432 326B3A1C 4E884A90 2228E89E AA9036CD 2AF70566
    81262372 C71371D4 533DC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Hash(counter||no_of_bits_to_return||input_string) is
             5BD1EED8 E55D9106 2FDD2764 B8AEA9C8 2F847E09


temp =
                      2C9C0D80 03E34023 BE5B63FD B9D224B4
    250CC815 5BD1EED8 E55D9106 2FDD2764 B8AEA9C8 2F847E09


------------

i = 3

counter||no_of_bits_to_return||input_string is
                                                      030000
    01B80127 AF4017CA C5B38624 E84C2D10 EFD78DF4 F477D654
    695A0432 326B3A1C 4E884A90 2228E89E AA9036CD 2AF70566
    81262372 C71371D4 533DC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Hash(counter||no_of_bits_to_return||input_string) is
             A3FEA1C7 117D6F7D D2EF777D 7CF3EBAC 38E03050
```

```
    temp =
                                                2C9C0D 8003E340
        23BE5B63 FDB9D224 B4250CC8 155BD1EE D8E55D91 062FDD27
        64B8AEA9 C82F847E 09A3FEA1 C7117D6F 7DD2EF77 7D7CF3EB


  V is
                                                2C9C0D 8003E340
        23BE5B63 FDB9D224 B4250CC8 155BD1EE D8E55D91 062FDD27
        64B8AEA9 C82F847E 09A3FEA1 C7117D6F 7DD2EF77 7D7CF3EB


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                             002C9C0D 8003E340
        23BE5B63 FDB9D224 B4250CC8 155BD1EE D8E55D91 062FDD27
        64B8AEA9 C82F847E 09A3FEA1 C7117D6F 7DD2EF77 7D7CF3EB


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 002C9C0D 8003E340
        23BE5B63 FDB9D224 B4250CC8 155BD1EE D8E55D91 062FDD27
        64B8AEA9 C82F847E 09A3FEA1 C7117D6F 7DD2EF77 7D7CF3EB


    Hash(counter||no_of_bits_to_return||input_string) is
                 7E8AA493 4272F2A2 8BBFD7AF CC88CE1C 806A38EA


    temp =
                 7E8AA493 4272F2A2 8BBFD7AF CC88CE1C 806A38EA


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                               02 000001B8 002C9C0D 8003E340
        23BE5B63 FDB9D224 B4250CC8 155BD1EE D8E55D91 062FDD27
        64B8AEA9 C82F847E 09A3FEA1 C7117D6F 7DD2EF77 7D7CF3EB
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                 7B8945C8 D1B6F175 0378546A B1A29600 D644EC52


    temp =
                          7E8AA493 4272F2A2 8BBFD7AF CC88CE1C
        806A38EA 7B8945C8 D1B6F175 0378546A B1A29600 D644EC52


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                                03 000001B8 002C9C0D 8003E340
        23BE5B63 FDB9D224 B4250CC8 155BD1EE D8E55D91 062FDD27
        64B8AEA9 C82F847E 09A3FEA1 C7117D6F 7DD2EF77 7D7CF3EB


    Hash(counter||no_of_bits_to_return||input_string) is
                 0E8BFFF6 0CB77FA5 4BB11A83 31CB24BD 9A5B8B7F


    temp =
                                              7E8AA4 934272F2
        A28BBFD7 AFCC88CE 1C806A38 EA7B8945 C8D1B6F1 75037854
        6AB1A296 00D644EC 520E8BFF F60CB77F A54BB11A 8331CB24


  C is
                                              7E8AA4 934272F2
        A28BBFD7 AFCC88CE 1C806A38 EA7B8945 C8D1B6F1 75037854
        6AB1A296 00D644EC 520E8BFF F60CB77F A54BB11A 8331CB24


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1
```

```
    data is
                                                2C9C0D 8003E340
        23BE5B63 FDB9D224 B4250CC8 155BD1EE D8E55D91 062FDD27
        64B8AEA9 C82F847E 09A3FEA1 C7117D6F 7DD2EF77 7D7CF3EB


    w_i is
                 F196F9BD 021C745C BD5AC7BF CE48EAAF 0D0E7C09


    W is
                 F196F9BD 021C745C BD5AC7BF CE48EAAF 0D0E7C09


    ------------

    i = 2

    data is
                                                2C9C0D 8003E340
        23BE5B63 FDB9D224 B4250CC8 155BD1EE D8E55D91 062FDD27
        64B8AEA9 C82F847E 09A3FEA1 C7117D6F 7DD2EF77 7D7CF3EC


    w_i is
                 1FBF4369 40E63A19 8EE770D9 A4F07186 69AF2BC9


    W is
                          F196F9BD 021C745C BD5AC7BF CE48EAAF
        0D0E7C09 1FBF4369 40E63A19 8EE770D9 A4F07186 69AF2BC9


  returned_bits is
                          F196F9BD 021C745C BD5AC7BF CE48EAAF
        0D0E7C09 1FBF4369 40E63A19 8EE770D9 A4F07186 69AF2BC9


---------------------------

  Update V

    0x03||V is
                                             032C9C0D 8003E340
        23BE5B63 FDB9D224 B4250CC8 155BD1EE D8E55D91 062FDD27
        64B8AEA9 C82F847E 09A3FEA1 C7117D6F 7DD2EF77 7D7CF3EB


    H is
                 6B77061B ED13DFBC 0226822E F02EB752 A7561855
```

```
  Updated values

  V is
                                                AB26B2 13465632
        C64A1B3B AD865AF2 D0A57700 FFD75B34 A1B71482 7B33557B
        CF6A5140 347CCF86 48C66A5D BF44B71E 134D57E4 A804D765


  reseed_counter is
                                                  0000 00000002


rnd_val is
                          F196F9BD 021C745C BD5AC7BF CE48EAAF
        0D0E7C09 1FBF4369 40E63A19 8EE770D9 A4F07186 69AF2BC9


################################################################

Hash_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  20 21222324


    PersonalizationString =
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
```

```
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

############################################################

************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                              000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                20 21222324


    personal_str is
                                              404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                  000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
        01000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
```

```
    5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


Hash(counter||no_of_bits_to_return||input_string) is
             99B9537B 8427B8CE 23219A61 1CBE6106 44CF8503


temp =
             99B9537B 8427B8CE 23219A61 1CBE6106 44CF8503


------------

i = 2

counter||no_of_bits_to_return||input_string is
    02000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
    13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
    2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
    4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
    5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


Hash(counter||no_of_bits_to_return||input_string) is
             EEC5BA22 DE1AB212 C3D0858E 9E3B9026 D4E77D58


temp =
                      99B9537B 8427B8CE 23219A61 1CBE6106
    44CF8503 EEC5BA22 DE1AB212 C3D0858E 9E3B9026 D4E77D58


------------

i = 3

counter||no_of_bits_to_return||input_string is
    03000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
    13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
    2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
    4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
    5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


Hash(counter||no_of_bits_to_return||input_string) is
             E02E85A2 314CE3D7 4A93324B 27BDE85F 5498B7AC


temp =
                                          99B953 7B8427B8
    CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
    8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8
```

```
  V is
                                                99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              0099B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 0099B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


    Hash(counter||no_of_bits_to_return||input_string) is
                 A70266F7 F91EC4D2 88731479 34CEAF2A 2CC35A0F


    temp =
                 A70266F7 F91EC4D2 88731479 34CEAF2A 2CC35A0F


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                               02 000001B8 0099B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


    Hash(counter||no_of_bits_to_return||input_string) is
                 D5E00ABA E79DC660 5FABD6F5 F928E18C 63268E1A
```

```
    temp =
                         A70266F7 F91EC4D2 88731479 34CEAF2A
        2CC35A0F D5E00ABA E79DC660 5FABD6F5 F928E18C 63268E1A


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                                03 000001B8 0099B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


    Hash(counter||no_of_bits_to_return||input_string) is
                 F485DA6C BF0416DC DC5FB8BC 9C94B6BC 511E0813


    temp =
                                               A70266 F7F91EC4
        D2887314 7934CEAF 2A2CC35A 0FD5E00A BAE79DC6 605FABD6
        F5F928E1 8C63268E 1AF485DA 6CBF0416 DCDC5FB8 BC9C94B6


  C is
                                               A70266 F7F91EC4
        D2887314 7934CEAF 2A2CC35A 0FD5E00A BAE79DC6 605FABD6
        F5F928E1 8C63268E 1AF485DA 6CBF0416 DCDC5FB8 BC9C94B6


-------------------------------------------------------------

First call to Generate

*************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

Generate FAILED: Reseed is required
-------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                               808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

```
  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                            0199B9 537B8427 B8CE2321 9A611CBE
        610644CF 8503EEC5 BA22DE1A B212C3D0 858E9E3B 9026D4E7
        7D58E02E 85A2314C E3D74A93 324B27BD E8808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                01000001 B80199B9 537B8427 B8CE2321 9A611CBE
        610644CF 8503EEC5 BA22DE1A B212C3D0 858E9E3B 9026D4E7
        7D58E02E 85A2314C E3D74A93 324B27BD E8808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    Hash(counter||no_of_bits_to_return||input_string) is
                E5043D1B 954B34BA 60D248E8 83EF498C 5C5236B8


    temp =
                E5043D1B 954B34BA 60D248E8 83EF498C 5C5236B8


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                02000001 B80199B9 537B8427 B8CE2321 9A611CBE
        610644CF 8503EEC5 BA22DE1A B212C3D0 858E9E3B 9026D4E7
        7D58E02E 85A2314C E3D74A93 324B27BD E8808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    Hash(counter||no_of_bits_to_return||input_string) is
                260E238E 02C8D4FC 5FFE90FA 40134470 75BB543E
```

```
    temp =
                          E5043D1B 954B34BA 60D248E8 83EF498C
        5C5236B8 260E238E 02C8D4FC 5FFE90FA 40134470 75BB543E


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                03000001 B80199B9 537B8427 B8CE2321 9A611CBE
        610644CF 8503EEC5 BA22DE1A B212C3D0 858E9E3B 9026D4E7
        7D58E02E 85A2314C E3D74A93 324B27BD E8808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    Hash(counter||no_of_bits_to_return||input_string) is
                F00C3BDA 596B1088 61F06BF9 1B45D683 A8FCA873


    temp =
                                               E5043D 1B954B34
        BA60D248 E883EF49 8C5C5236 B8260E23 8E02C8D4 FC5FFE90
        FA401344 7075BB54 3EF00C3B DA596B10 8861F06B F91B45D6


  V is
                                               E5043D 1B954B34
        BA60D248 E883EF49 8C5C5236 B8260E23 8E02C8D4 FC5FFE90
        FA401344 7075BB54 3EF00C3B DA596B10 8861F06B F91B45D6


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                             00E5043D 1B954B34
        BA60D248 E883EF49 8C5C5236 B8260E23 8E02C8D4 FC5FFE90
        FA401344 7075BB54 3EF00C3B DA596B10 8861F06B F91B45D6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
```

```
                           01 000001B8 00E5043D 1B954B34
    BA60D248 E883EF49 8C5C5236 B8260E23 8E02C8D4 FC5FFE90
    FA401344 7075BB54 3EF00C3B DA596B10 8861F06B F91B45D6


Hash(counter||no_of_bits_to_return||input_string) is
             1F3F6310 ED10FC9F 938C4322 61AF42E9 E9175F08


temp =
             1F3F6310 ED10FC9F 938C4322 61AF42E9 E9175F08


------------

i = 2

counter||no_of_bits_to_return||input_string is
                           02 000001B8 00E5043D 1B954B34
    BA60D248 E883EF49 8C5C5236 B8260E23 8E02C8D4 FC5FFE90
    FA401344 7075BB54 3EF00C3B DA596B10 8861F06B F91B45D6


Hash(counter||no_of_bits_to_return||input_string) is
             0F3222DC 118BA7CF 888CDC3F 360DD28F 5ECB7C80


temp =
                      1F3F6310 ED10FC9F 938C4322 61AF42E9
    E9175F08 0F3222DC 118BA7CF 888CDC3F 360DD28F 5ECB7C80


------------

i = 3

counter||no_of_bits_to_return||input_string is
                           03 000001B8 00E5043D 1B954B34
    BA60D248 E883EF49 8C5C5236 B8260E23 8E02C8D4 FC5FFE90
    FA401344 7075BB54 3EF00C3B DA596B10 8861F06B F91B45D6


Hash(counter||no_of_bits_to_return||input_string) is
             A6BCFCFC 0F51FE2F 77C1C99D F0A2099F 44A616E7


temp =
                                          1F3F63 10ED10FC
    9F938C43 2261AF42 E9E9175F 080F3222 DC118BA7 CF888CDC
    3F360DD2 8F5ECB7C 80A6BCFC FC0F51FE 2F77C1C9 9DF0A209
```

```
  C is
                                                1F3F63 10ED10FC
        9F938C43 2261AF42 E9E9175F 080F3222 DC118BA7 CF888CDC
        3F360DD2 8F5ECB7C 80A6BCFC FC0F51FE 2F77C1C9 9DF0A209


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                                E5043D 1B954B34
        BA60D248 E883EF49 8C5C5236 B8260E23 8E02C8D4 FC5FFE90
        FA401344 7075BB54 3EF00C3B DA596B10 8861F06B F91B45D6


    w_i is
                 532CA116 5DCFF21C 55592687 639884AF 4BC4B057


    W is
                 532CA116 5DCFF21C 55592687 639884AF 4BC4B057


    ------------

    i = 2

    data is
                                                E5043D 1B954B34
        BA60D248 E883EF49 8C5C5236 B8260E23 8E02C8D4 FC5FFE90
        FA401344 7075BB54 3EF00C3B DA596B10 8861F06B F91B45D7


    w_i is
                 DF8F41DE 653AB44E 2ADEC7C9 303E75AB E277EDBF
```

```
    W is
                          532CA116 5DCFF21C 55592687 639884AF
         4BC4B057 DF8F41DE 653AB44E 2ADEC7C9 303E75AB E277EDBF


  returned_bits is
                          532CA116 5DCFF21C 55592687 639884AF
         4BC4B057 DF8F41DE 653AB44E 2ADEC7C9 303E75AB E277EDBF


---------------------------

  Update V

    0x03||V is
                                             03E5043D 1B954B34
         BA60D248 E883EF49 8C5C5236 B8260E23 8E02C8D4 FC5FFE90
         FA401344 7075BB54 3EF00C3B DA596B10 8861F06B F91B45D6


    H is
                 32AFEC24 6BED8E21 D97FCE1E 66769CEC 55424955


  Updated values

  V is
                                               0443A0 2C825C31
         59F45E8C 0AE59E8C 76456995 C0354046 6A14547C CBE88B6D
         39762117 328472F5 2B84575A AFE88B2D 1E504F21 EC4E3135


  reseed_counter is
                                                 0000 00000002


rnd_val is
                          532CA116 5DCFF21C 55592687 639884AF
         4BC4B057 DF8F41DE 653AB44E 2ADEC7C9 303E75AB E277EDBF


-------------------------------------------------------------

Second call to Generate

*************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>
```

```
Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                            010443 A02C825C 3159F45E 8C0AE59E
        8C764569 95C03540 466A1454 7CCBE88B 6D397621 17328472
        F52B8457 5AAFE88B 2D1E504F 21EC4E31 35C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                01000001 B8010443 A02C825C 3159F45E 8C0AE59E
        8C764569 95C03540 466A1454 7CCBE88B 6D397621 17328472
        F52B8457 5AAFE88B 2D1E504F 21EC4E31 35C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                9DC35208 EE2B8C58 1EA30BAA CB5D7431 7A879454


    temp =
                9DC35208 EE2B8C58 1EA30BAA CB5D7431 7A879454


    ------------

    i = 2
```

```
    counter||no_of_bits_to_return||input_string is
                02000001 B8010443 A02C825C 3159F45E 8C0AE59E
        8C764569 95C03540 466A1454 7CCBE88B 6D397621 17328472
        F52B8457 5AAFE88B 2D1E504F 21EC4E31 35C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                10717E58 D3705FBD C760BE0C C90ED1CC BB897D47


    temp =
                          9DC35208 EE2B8C58 1EA30BAA CB5D7431
        7A879454 10717E58 D3705FBD C760BE0C C90ED1CC BB897D47


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                03000001 B8010443 A02C825C 3159F45E 8C0AE59E
        8C764569 95C03540 466A1454 7CCBE88B 6D397621 17328472
        F52B8457 5AAFE88B 2D1E504F 21EC4E31 35C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                D27E2B2E 422B32B9 7F050D1B D2B49080 823932BF


    temp =
                                              9DC352 08EE2B8C
        581EA30B AACB5D74 317A8794 5410717E 58D3705F BDC760BE
        0CC90ED1 CCBB897D 47D27E2B 2E422B32 B97F050D 1BD2B490


  V is
                                              9DC352 08EE2B8C
        581EA30B AACB5D74 317A8794 5410717E 58D3705F BDC760BE
        0CC90ED1 CCBB897D 47D27E2B 2E422B32 B97F050D 1BD2B490


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            009DC352 08EE2B8C
        581EA30B AACB5D74 317A8794 5410717E 58D3705F BDC760BE
```

```
    0CC90ED1 CCBB897D 47D27E2B 2E422B32 B97F050D 1BD2B490


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                            01 000001B8 009DC352 08EE2B8C
    581EA30B AACB5D74 317A8794 5410717E 58D3705F BDC760BE
    0CC90ED1 CCBB897D 47D27E2B 2E422B32 B97F050D 1BD2B490


Hash(counter||no_of_bits_to_return||input_string) is
             1A5AD6CE A3D15DA5 FB474213 1309F0ED 88CF4C90


temp =
             1A5AD6CE A3D15DA5 FB474213 1309F0ED 88CF4C90


------------

i = 2

counter||no_of_bits_to_return||input_string is
                            02 000001B8 009DC352 08EE2B8C
    581EA30B AACB5D74 317A8794 5410717E 58D3705F BDC760BE
    0CC90ED1 CCBB897D 47D27E2B 2E422B32 B97F050D 1BD2B490


Hash(counter||no_of_bits_to_return||input_string) is
             A6C1CCEE 35A876EB FCCC8267 29B6639F 811965B0


temp =
                      1A5AD6CE A3D15DA5 FB474213 1309F0ED
    88CF4C90 A6C1CCEE 35A876EB FCCC8267 29B6639F 811965B0


------------

i = 3

counter||no_of_bits_to_return||input_string is
                            03 000001B8 009DC352 08EE2B8C
    581EA30B AACB5D74 317A8794 5410717E 58D3705F BDC760BE
    0CC90ED1 CCBB897D 47D27E2B 2E422B32 B97F050D 1BD2B490
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                EF8576E7 5CB3CFE8 220768B2 6CE77ACE CD58370F


    temp =
                                              1A5AD6 CEA3D15D
        A5FB4742 131309F0 ED88CF4C 90A6C1CC EE35A876 EBFCCC82
        6729B663 9F811965 B0EF8576 E75CB3CF E8220768 B26CE77A


  C is
                                              1A5AD6 CEA3D15D
        A5FB4742 131309F0 ED88CF4C 90A6C1CC EE35A876 EBFCCC82
        6729B663 9F811965 B0EF8576 E75CB3CF E8220768 B26CE77A


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                              9DC352 08EE2B8C
        581EA30B AACB5D74 317A8794 5410717E 58D3705F BDC760BE
        0CC90ED1 CCBB897D 47D27E2B 2E422B32 B97F050D 1BD2B490


    w_i is
                73C2C67C 696D686D 0C4DBCEB 5C2AF7DD F6F020B6


    W is
                73C2C67C 696D686D 0C4DBCEB 5C2AF7DD F6F020B6


    ------------

    i = 2
```

```
    data is
                                                9DC352 08EE2B8C
        581EA30B AACB5D74 317A8794 5410717E 58D3705F BDC760BE
        0CC90ED1 CCBB897D 47D27E2B 2E422B32 B97F050D 1BD2B491


    w_i is
                874FAE43 90F10211 7ECAAFF5 4418529A 367005A0


    W is
                         73C2C67C 696D686D 0C4DBCEB 5C2AF7DD
        F6F020B6 874FAE43 90F10211 7ECAAFF5 4418529A 367005A0


  returned_bits is
                         73C2C67C 696D686D 0C4DBCEB 5C2AF7DD
        F6F020B6 874FAE43 90F10211 7ECAAFF5 4418529A 367005A0


---------------------------

  Update V

    0x03||V is
                                              039DC352 08EE2B8C
        581EA30B AACB5D74 317A8794 5410717E 58D3705F BDC760BE
        0CC90ED1 CCBB897D 47D27E2B 2E422B32 B97F050D 1BD2B490


    H is
                03287CD5 69C9D511 E2E69645 0A15C4BA DAA6BB53


  Updated values

  V is
                                                B81E28 D791FCE9
        FE19EA4D BDDE6765 1F0356E0 E4B7334B 470918D6 A9C42D40
        73F2C535 6F651FB8 628BD8B3 F8857547 ABB6D130 A8E6575E


  reseed_counter is
                                                  0000 00000002


rnd_val is
                         73C2C67C 696D686D 0C4DBCEB 5C2AF7DD
        F6F020B6 874FAE43 90F10211 7ECAAFF5 4418529A 367005A0


################################################################
```

```
Hash_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                 C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                     20 21222324


    PersonalizationString =
                                                 404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                 606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************
```

```
Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                    20 21222324


    personal_str is
                                                 404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                   000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
        01000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                 99B9537B 8427B8CE 23219A61 1CBE6106 44CF8503


    temp =
                 99B9537B 8427B8CE 23219A61 1CBE6106 44CF8503
```

```
    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
        02000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                 EEC5BA22 DE1AB212 C3D0858E 9E3B9026 D4E77D58


    temp =
                          99B9537B 8427B8CE 23219A61 1CBE6106
        44CF8503 EEC5BA22 DE1AB212 C3D0858E 9E3B9026 D4E77D58


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
        03000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                 E02E85A2 314CE3D7 4A93324B 27BDE85F 5498B7AC


    temp =
                                              99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


  V is
                                              99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


---------------------------
```

```
Hash_df - Generate C - Step 4

  0x00||V is
                                          0099B953 7B8427B8
      CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
      8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


  no_of_bits_to_return = 440

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                             01 000001B8 0099B953 7B8427B8
      CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
      8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


  Hash(counter||no_of_bits_to_return||input_string) is
               A70266F7 F91EC4D2 88731479 34CEAF2A 2CC35A0F


  temp =
               A70266F7 F91EC4D2 88731479 34CEAF2A 2CC35A0F


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                             02 000001B8 0099B953 7B8427B8
      CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
      8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


  Hash(counter||no_of_bits_to_return||input_string) is
               D5E00ABA E79DC660 5FABD6F5 F928E18C 63268E1A


  temp =
                        A70266F7 F91EC4D2 88731479 34CEAF2A
      2CC35A0F D5E00ABA E79DC660 5FABD6F5 F928E18C 63268E1A


  ------------

  i = 3
```

```
    counter||no_of_bits_to_return||input_string is
                                03 000001B8 0099B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


    Hash(counter||no_of_bits_to_return||input_string) is
                 F485DA6C BF0416DC DC5FB8BC 9C94B6BC 511E0813


    temp =
                                               A70266 F7F91EC4
        D2887314 7934CEAF 2A2CC35A 0FD5E00A BAE79DC6 605FABD6
        F5F928E1 8C63268E 1AF485DA 6CBF0416 DCDC5FB8 BC9C94B6


  C is
                                               A70266 F7F91EC4
        D2887314 7934CEAF 2A2CC35A 0FD5E00A BAE79DC6 605FABD6
        F5F928E1 8C63268E 1AF485DA 6CBF0416 DCDC5FB8 BC9C94B6


----------------------------------------------------------------

First call to Generate

****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input
                                               606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
----------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                               808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  additional_input
                                               606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
```

```
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0199 B9537B84 27B8CE23 219A611C BE610644 CF8503EE
        C5BA22DE 1AB212C3 D0858E9E 3B9026D4 E77D58E0 2E85A231
        4CE3D74A 93324B27 BDE88081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                        010000
        01B80199 B9537B84 27B8CE23 219A611C BE610644 CF8503EE
        C5BA22DE 1AB212C3 D0858E9E 3B9026D4 E77D58E0 2E85A231
        4CE3D74A 93324B27 BDE88081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    Hash(counter||no_of_bits_to_return||input_string) is
                563A5D20 7D37707B F5F24D0B D4935DC3 8DBE0436


    temp =
                563A5D20 7D37707B F5F24D0B D4935DC3 8DBE0436


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                        020000
        01B80199 B9537B84 27B8CE23 219A611C BE610644 CF8503EE
        C5BA22DE 1AB212C3 D0858E9E 3B9026D4 E77D58E0 2E85A231
        4CE3D74A 93324B27 BDE88081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
```

```
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    Hash(counter||no_of_bits_to_return||input_string) is
                 37B3FF8A B68CFCE2 F290D169 95205524 190FD291


    temp =
                         563A5D20 7D37707B F5F24D0B D4935DC3
        8DBE0436 37B3FF8A B68CFCE2 F290D169 95205524 190FD291


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                                                        030000
        01B80199 B9537B84 27B8CE23 219A611C BE610644 CF8503EE
        C5BA22DE 1AB212C3 D0858E9E 3B9026D4 E77D58E0 2E85A231
        4CE3D74A 93324B27 BDE88081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    Hash(counter||no_of_bits_to_return||input_string) is
                 AA8A6E6B 8E6D56A4 31333B40 8E6FA812 0AE2B77C


    temp =
                                              563A5D 207D3770
        7BF5F24D 0BD4935D C38DBE04 3637B3FF 8AB68CFC E2F290D1
        69952055 24190FD2 91AA8A6E 6B8E6D56 A431333B 408E6FA8


  V is
                                              563A5D 207D3770
        7BF5F24D 0BD4935D C38DBE04 3637B3FF 8AB68CFC E2F290D1
        69952055 24190FD2 91AA8A6E 6B8E6D56 A431333B 408E6FA8


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            00563A5D 207D3770
        7BF5F24D 0BD4935D C38DBE04 3637B3FF 8AB68CFC E2F290D1
```

```
    69952055 24190FD2 91AA8A6E 6B8E6D56 A431333B 408E6FA8


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                            01 000001B8 00563A5D 207D3770
    7BF5F24D 0BD4935D C38DBE04 3637B3FF 8AB68CFC E2F290D1
    69952055 24190FD2 91AA8A6E 6B8E6D56 A431333B 408E6FA8


Hash(counter||no_of_bits_to_return||input_string) is
             C5D3E955 1E00E4EE 32B2116F AF4DEFF4 D4CFAD2B


temp =
             C5D3E955 1E00E4EE 32B2116F AF4DEFF4 D4CFAD2B


------------

i = 2

counter||no_of_bits_to_return||input_string is
                            02 000001B8 00563A5D 207D3770
    7BF5F24D 0BD4935D C38DBE04 3637B3FF 8AB68CFC E2F290D1
    69952055 24190FD2 91AA8A6E 6B8E6D56 A431333B 408E6FA8


Hash(counter||no_of_bits_to_return||input_string) is
             DC2DBAA2 E0E7F9DD B9D81EED 45E0A50D A5AFD5C1


temp =
                      C5D3E955 1E00E4EE 32B2116F AF4DEFF4
    D4CFAD2B DC2DBAA2 E0E7F9DD B9D81EED 45E0A50D A5AFD5C1


------------

i = 3

counter||no_of_bits_to_return||input_string is
                            03 000001B8 00563A5D 207D3770
    7BF5F24D 0BD4935D C38DBE04 3637B3FF 8AB68CFC E2F290D1
    69952055 24190FD2 91AA8A6E 6B8E6D56 A431333B 408E6FA8
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                F6BCDAF8 1D289CF4 BD3C91B7 005C1833 EBD4CAAB


    temp =
                                              C5D3E9 551E00E4
        EE32B211 6FAF4DEF F4D4CFAD 2BDC2DBA A2E0E7F9 DDB9D81E
        ED45E0A5 0DA5AFD5 C1F6BCDA F81D289C F4BD3C91 B7005C18


  C is
                                              C5D3E9 551E00E4
        EE32B211 6FAF4DEF F4D4CFAD 2BDC2DBA A2E0E7F9 DDB9D81E
        ED45E0A5 0DA5AFD5 C1F6BCDA F81D289C F4BD3C91 B7005C18


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                              563A5D 207D3770
        7BF5F24D 0BD4935D C38DBE04 3637B3FF 8AB68CFC E2F290D1
        69952055 24190FD2 91AA8A6E 6B8E6D56 A431333B 408E6FA8


    w_i is
                F2F76CE3D 13BE866F EB390DB5 7591CD12 09E4FE0F


    W is
                F2F76CE3D 13BE866F EB390DB5 7591CD12 09E4FE0F


    ------------

    i = 2
```

```
    data is
                                                563A5D 207D3770
        7BF5F24D 0BD4935D C38DBE04 3637B3FF 8AB68CFC E2F290D1
        69952055 24190FD2 91AA8A6E 6B8E6D56 A431333B 408E6FA9


    w_i is
                90794C97 218A6482 5D8E4097 CB15D30E D958BC18


    W is
                         2F76CE3D 13BE866F EB390DB5 7591CD12
        09E4FE0F 90794C97 218A6482 5D8E4097 CB15D30E D958BC18


  returned_bits is
                         2F76CE3D 13BE866F EB390DB5 7591CD12
        09E4FE0F 90794C97 218A6482 5D8E4097 CB15D30E D958BC18


---------------------------

  Update V

    0x03||V is
                                               03563A5D 207D3770
        7BF5F24D 0BD4935D C38DBE04 3637B3FF 8AB68CFC E2F290D1
        69952055 24190FD2 91AA8A6E 6B8E6D56 A431333B 408E6FA8


    H is
                E1229C4C 8AF4096D CF7297C9 CD5DCAEA 7F595990


  Updated values

  V is
                                                 1C0E46 759B3855
        6A28A45E 7B83E14D B8628DB1 6213E1BA 2D9774F6 C0AC68F0
        56DB00FB 12E15BF4 DE9550B7 331E2DBD 664C3AB7 76E82551


  reseed_counter is
                                                   0000 00000002


rnd_val is
                         2F76CE3D 13BE866F EB390DB5 7591CD12
        09E4FE0F 90794C97 218A6482 5D8E4097 CB15D30E D958BC18


---------------------------------------------------------------
```

```
Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input
                                              A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                              C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  additional_input
                                              A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            011C 0E46759B 38556A28 A45E7B83 E14DB862 8DB16213
        E1BA2D97 74F6C0AC 68F056DB 00FB12E1 5BF4DE95 50B7331E
        2DBD664C 3AB776E8 2551C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    no_of_bits_to_return = 440

    ------------

    i = 1
```

```
counter||no_of_bits_to_return||input_string is
                                                        010000
    01B8011C 0E46759B 38556A28 A45E7B83 E14DB862 8DB16213
    E1BA2D97 74F6C0AC 68F056DB 00FB12E1 5BF4DE95 50B7331E
    2DBD664C 3AB776E8 2551C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Hash(counter||no_of_bits_to_return||input_string) is
             600193C8 F6031A2D 49372A8B 0F60F68C 1DFDACD4


temp =
             600193C8 F6031A2D 49372A8B 0F60F68C 1DFDACD4


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                        020000
    01B8011C 0E46759B 38556A28 A45E7B83 E14DB862 8DB16213
    E1BA2D97 74F6C0AC 68F056DB 00FB12E1 5BF4DE95 50B7331E
    2DBD664C 3AB776E8 2551C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Hash(counter||no_of_bits_to_return||input_string) is
             F8EA0137 47D71482 333DF525 2E95B822 57391BF1


temp =
                      600193C8 F6031A2D 49372A8B 0F60F68C
    1DFDACD4 F8EA0137 47D71482 333DF525 2E95B822 57391BF1


------------

i = 3

counter||no_of_bits_to_return||input_string is
                                                        030000
    01B8011C 0E46759B 38556A28 A45E7B83 E14DB862 8DB16213
    E1BA2D97 74F6C0AC 68F056DB 00FB12E1 5BF4DE95 50B7331E
    2DBD664C 3AB776E8 2551C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
```

```
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    Hash(counter||no_of_bits_to_return||input_string) is
                 0AB07D12 08B6BD66 5B300AA4 DB9C3EF0 70322C9B


    temp =
                                              600193 C8F6031A
        2D49372A 8B0F60F6 8C1DFDAC D4F8EA01 3747D714 82333DF5
        252E95B8 2257391B F10AB07D 1208B6BD 665B300A A4DB9C3E


  V is
                                              600193 C8F6031A
        2D49372A 8B0F60F6 8C1DFDAC D4F8EA01 3747D714 82333DF5
        252E95B8 2257391B F10AB07D 1208B6BD 665B300A A4DB9C3E


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            00600193 C8F6031A
        2D49372A 8B0F60F6 8C1DFDAC D4F8EA01 3747D714 82333DF5
        252E95B8 2257391B F10AB07D 1208B6BD 665B300A A4DB9C3E


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 00600193 C8F6031A
        2D49372A 8B0F60F6 8C1DFDAC D4F8EA01 3747D714 82333DF5
        252E95B8 2257391B F10AB07D 1208B6BD 665B300A A4DB9C3E


    Hash(counter||no_of_bits_to_return||input_string) is
                 6B71823B 18200771 CAAE5D12 55C1403E DFE38B4D


    temp =
                 6B71823B 18200771 CAAE5D12 55C1403E DFE38B4D
```

```
    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00600193 C8F6031A
        2D49372A 8B0F60F6 8C1DFDAC D4F8EA01 3747D714 82333DF5
        252E95B8 2257391B F10AB07D 1208B6BD 665B300A A4DB9C3E


    Hash(counter||no_of_bits_to_return||input_string) is
                18C787BB 44CD1718 6152EFEA D6FDC4B8 94F92002


    temp =
                          6B71823B 18200771 CAAE5D12 55C1403E
        DFE38B4D 18C787BB 44CD1718 6152EFEA D6FDC4B8 94F92002


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                                03 000001B8 00600193 C8F6031A
        2D49372A 8B0F60F6 8C1DFDAC D4F8EA01 3747D714 82333DF5
        252E95B8 2257391B F10AB07D 1208B6BD 665B300A A4DB9C3E


    Hash(counter||no_of_bits_to_return||input_string) is
                C0720955 5D7E3554 F9D12FC5 597F22F4 44AAC5B9


    temp =
                                              6B7182 3B182007
        71CAAE5D 1255C140 3EDFE38B 4D18C787 BB44CD17 186152EF
        EAD6FDC4 B894F920 02C07209 555D7E35 54F9D12F C5597F22


  C is
                                              6B7182 3B182007
        71CAAE5D 1255C140 3EDFE38B 4D18C787 BB44CD17 186152EF
        EAD6FDC4 B894F920 02C07209 555D7E35 54F9D12F C5597F22


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>
```

```
---------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                                600193 C8F6031A
        2D49372A 8B0F60F6 8C1DFDAC D4F8EA01 3747D714 82333DF5
        252E95B8 2257391B F10AB07D 1208B6BD 665B300A A4DB9C3E


    w_i is
                79CE5A7D 09EBB2FF 600EDB53 1C8A212F F3EA267C


    W is
                79CE5A7D 09EBB2FF 600EDB53 1C8A212F F3EA267C


    ------------

    i = 2

    data is
                                                600193 C8F6031A
        2D49372A 8B0F60F6 8C1DFDAC D4F8EA01 3747D714 82333DF5
        252E95B8 2257391B F10AB07D 1208B6BD 665B300A A4DB9C3F


    w_i is
                1C5487E5 83592A0A BFEAFC4E 13045EA9 3666DB85


    W is
                         79CE5A7D 09EBB2FF 600EDB53 1C8A212F
        F3EA267C 1C5487E5 83592A0A BFEAFC4E 13045EA9 3666DB85


  returned_bits is
                         79CE5A7D 09EBB2FF 600EDB53 1C8A212F
        F3EA267C 1C5487E5 83592A0A BFEAFC4E 13045EA9 3666DB85


---------------------------

  Update V
```

```
    0x03||V is
                                                03600193 C8F6031A
        2D49372A 8B0F60F6 8C1DFDAC D4F8EA01 3747D714 82333DF5
        252E95B8 2257391B F10AB07D 1208B6BD 665B300A A4DB9C3E


    H is
                 EB7068BD AD62FFEA 6E358C7A 1FC2427D DC635B99


  Updated values

  V is
                                                  CB7316 040E2321
        9F13E587 9D652236 CAFDE138 2211B188 F28CA42B 9A9490E5
        1005937D C65C9AF9 A12E2270 D59BC16C DB1743B8 469876FA


  reseed_counter is
                                                    0000 00000002


rnd_val is
                          79CE5A7D 09EBB2FF 600EDB53 1C8A212F
        F3EA267C 1C5487E5 83592A0A BFEAFC4E 13045EA9 3666DB85
```

```
################################################################

Hash_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    nonce is
                                                202122 23242526


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                               0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                   010000 01B80001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        0BB6E53D
        916573A7 AC796702 CA6DD2E3 0D13B8A3 ACFD7E23 905D6F8A


    temp =
                                                        0BB6E53D
        916573A7 AC796702 CA6DD2E3 0D13B8A3 ACFD7E23 905D6F8A


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
```

020000 01B80001 02030405 06070809 0A0B0C0D
0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526

Hash(counter||no_of_bits_to_return||input_string) is
33D18070
2841C3D3 7CA40F35 645ECB1A A6548550 7F577CA9 8F418A0E

temp =
0BB6E5 3D916573
A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A

V is
0BB6E5 3D916573
A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A

Hash_df - Generate C - Step 4

0x00||V is
000BB6E5 3D916573
A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A

no_of_bits_to_return = 440

---

i = 1

counter||no_of_bits_to_return||input_string is
01 000001B8 000BB6E5 3D916573
A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A

Hash(counter||no_of_bits_to_return||input_string) is
E5B7AE6C

```
        8607715A F6CCCF35 2696C291 F43D10D1 E48E9FD0 717320C0


    temp =
                                                        E5B7AE6C
        8607715A F6CCCF35 2696C291 F43D10D1 E48E9FD0 717320C0


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 000BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        11F35DAE
        12883480 7F41DD3A A952DE09 0AB3C78C C4D38F67 F13F7896


    temp =
                                                  E5B7AE 6C860771
        5AF6CCCF 352696C2 91F43D10 D1E48E9F D0717320 C011F35D
        AE128834 807F41DD 3AA952DE 090AB3C7 8CC4D38F 67F13F78


  C is
                                                  E5B7AE 6C860771
        5AF6CCCF 352696C2 91F43D10 D1E48E9F D0717320 C011F35D
        AE128834 807F41DD 3AA952DE 090AB3C7 8CC4D38F 67F13F78


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>
```

```
---------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------

    i = 1

    data is
                                                0BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


    w_i is
                                                        5E68BDE0
        9AAA08BC 11B32790 2C82F011 4CBA0F9C CCA6203B A3940091


    W is
                                                        5E68BDE0
        9AAA08BC 11B32790 2C82F011 4CBA0F9C CCA6203B A3940091


    ------------

    i = 2

    data is
                                                0BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418B


    w_i is
                                                        3ECD3671
        A5B60EF9 22999D90 FCEEEC5C 227E5D25 C56921EE 572ED472


    W is
                                               5E68BDE0 9AAA08BC
        11B32790 2C82F011 4CBA0F9C CCA6203B A3940091 3ECD3671
        A5B60EF9 22999D90 FCEEEC5C 227E5D25 C56921EE 572ED472
```

```
  returned_bits is
                                                5E68BDE0 9AAA08BC
        11B32790 2C82F011 4CBA0F9C CCA6203B A3940091 3ECD3671
        A5B60EF9 22999D90 FCEEEC5C 227E5D25 C56921EE 572ED472


---------------------------

  Update V

    0x03||V is
                                                030BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


    H is
                                                        F4F9E387
        8DAC8089 5CE1C1DD E67CBEAD 36B59C8F 3767955D 3623164F


  Updated values

  V is
                                                  F16E93 AA176CE5
        02A34636 37F10495 750150C9 75918C1D F401D091 3F3FA865
        ABE74A81 B0DDA7CA 568A7056 5A66A4DC 14ABC069 47A39752


  reseed_counter is
                                                    0000 00000002


rnd_val is
                                                5E68BDE0 9AAA08BC
        11B32790 2C82F011 4CBA0F9C CCA6203B A3940091 3ECD3671
        A5B60EF9 22999D90 FCEEEC5C 227E5D25 C56921EE 572ED472


-------------------------------------------------------------

Second call to Generate

*************************************************************
```

```
Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------

    i = 1

    data is
                                                F16E93 AA176CE5
        02A34636 37F10495 750150C9 75918C1D F401D091 3F3FA865
        ABE74A81 B0DDA7CA 568A7056 5A66A4DC 14ABC069 47A39752


    w_i is
                                                        DC056FCB
        35FF51D7 D9FB72FD 4FD1B1D2 46451DB5 6CD4F889 E432E327


    W is
                                                        DC056FCB
        35FF51D7 D9FB72FD 4FD1B1D2 46451DB5 6CD4F889 E432E327


    ------------

    i = 2

    data is
                                                F16E93 AA176CE5
        02A34636 37F10495 750150C9 75918C1D F401D091 3F3FA865
        ABE74A81 B0DDA7CA 568A7056 5A66A4DC 14ABC069 47A39753


    w_i is
                                                        3F9ED82D
        E3EF7CD2 8B6A9C0F 4D78E5C8 451D3634 0A2BD7E6 9FAB32EB
```

```
    W is
                                                DC056FCB 35FF51D7
        D9FB72FD 4FD1B1D2 46451DB5 6CD4F889 E432E327 3F9ED82D
        E3EF7CD2 8B6A9C0F 4D78E5C8 451D3634 0A2BD7E6 9FAB32EB


  returned_bits is
                                                DC056FCB 35FF51D7
        D9FB72FD 4FD1B1D2 46451DB5 6CD4F889 E432E327 3F9ED82D
        E3EF7CD2 8B6A9C0F 4D78E5C8 451D3634 0A2BD7E6 9FAB32EB


---------------------------

  Update V

    0x03||V is
                                                03F16E93 AA176CE5
        02A34636 37F10495 750150C9 75918C1D F401D091 3F3FA865
        ABE74A81 B0DDA7CA 568A7056 5A66A4DC 14ABC069 47A39752


    H is
                                                        06BFA186
        BFC4A213 5AA645D7 D2E29A3B E15BA781 7EEC5A90 E0536E52


  Updated values

  V is
                                                  D72642 169D7456
        5D9A1305 6D179B58 06F58DDA 47761ABD C47343B2 06113D4A
        19BE74C9 8C032F7F 64165D70 44CD0025 205CEE89 8FE8451E


  reseed_counter is
                                                    0000 00000003


rnd_val is
                                                DC056FCB 35FF51D7
        D9FB72FD 4FD1B1D2 46451DB5 6CD4F889 E432E327 3F9ED82D
        E3EF7CD2 8B6A9C0F 4D78E5C8 451D3634 0A2BD7E6 9FAB32EB
```

```
################################################################

Hash_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
```

```
################################################################

****************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                  202122 23242526


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                               0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                    010000 01B80001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        0BB6E53D
        916573A7 AC796702 CA6DD2E3 0D13B8A3 ACFD7E23 905D6F8A
```

```
    temp =
                                                          0BB6E53D
        916573A7 AC796702 CA6DD2E3 0D13B8A3 ACFD7E23 905D6F8A


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                  020000 01B80001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    Hash(counter||no_of_bits_to_return||input_string) is
                                                          33D18070
        2841C3D3 7CA40F35 645ECB1A A6548550 7F577CA9 8F418A0E


    temp =
                                                 0BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


  V is
                                                 0BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                               000BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


    no_of_bits_to_return = 440

    ------------
```

```
  i = 1

  counter||no_of_bits_to_return||input_string is
                              01 000001B8 000BB6E5 3D916573
      A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
      702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


  Hash(counter||no_of_bits_to_return||input_string) is
                                                    E5B7AE6C
      8607715A F6CCCF35 2696C291 F43D10D1 E48E9FD0 717320C0


  temp =
                                                    E5B7AE6C
      8607715A F6CCCF35 2696C291 F43D10D1 E48E9FD0 717320C0


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                              02 000001B8 000BB6E5 3D916573
      A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
      702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


  Hash(counter||no_of_bits_to_return||input_string) is
                                                    11F35DAE
      12883480 7F41DD3A A952DE09 0AB3C78C C4D38F67 F13F7896


  temp =
                                                E5B7AE 6C860771
      5AF6CCCF 352696C2 91F43D10 D1E48E9F D0717320 C011F35D
      AE128834 807F41DD 3AA952DE 090AB3C7 8CC4D38F 67F13F78


C is
                                                E5B7AE 6C860771
      5AF6CCCF 352696C2 91F43D10 D1E48E9F D0717320 C011F35D
      AE128834 807F41DD 3AA952DE 090AB3C7 8CC4D38F 67F13F78
```

```
---------------------------------------------------------------

First call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


---------------------------

  Process additional_input

    0x02||V||additional_input is
                           020BB6 E53D9165 73A7AC79 6702CA6D
        D2E30D13 B8A3ACFD 7E23905D 6F8A33D1 80702841 C3D37CA4
        0F35645E CB1AA654 85507F57 7CA98F41 8A606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    w=Hash(0x02||V||additional_input) is
                                                        4287889E
        AD10CE0F D67794A8 CCE65303 02F18AEC 557970F0 CA5195D5


    V is
                                                0BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F CCBB5A1F
        1D390FD3 A9F438B8 024AB1CE 1D97DF71 A5F8C86D 73E0D75F


---------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------
```

```
  i = 1

  data is
                                                0BB6E5 3D916573
      A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F CCBB5A1F
      1D390FD3 A9F438B8 024AB1CE 1D97DF71 A5F8C86D 73E0D75F


  w_i is
                                                      B15DEC1B
      266433D9 7E587C87 1D15717A E15CA7B7 E616CFE1 0120523A


  W is
                                                      B15DEC1B
      266433D9 7E587C87 1D15717A E15CA7B7 E616CFE1 0120523A


  ------------

  i = 2

  data is
                                                0BB6E5 3D916573
      A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F CCBB5A1F
      1D390FD3 A9F438B8 024AB1CE 1D97DF71 A5F8C86D 73E0D760


  w_i is
                                                      E9504D80
      4E102D1C AFAFD3FF 677BEBBD 0C435952 505F8723 1D9EA679


  W is
                                              B15DEC1B 266433D9
      7E587C87 1D15717A E15CA7B7 E616CFE1 0120523A E9504D80
      4E102D1C AFAFD3FF 677BEBBD 0C435952 505F8723 1D9EA679


returned_bits is
                                              B15DEC1B 266433D9
      7E587C87 1D15717A E15CA7B7 E616CFE1 0120523A E9504D80
      4E102D1C AFAFD3FF 677BEBBD 0C435952 505F8723 1D9EA679
```

```
--------------------------

  Update V

    0x03||V is
                                              030BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F CCBB5A1F
        1D390FD3 A9F438B8 024AB1CE 1D97DF71 A5F8C86D 73E0D75F


    H is
                                                      9C1A49BE
        0F0F864F B744F3E4 59836BE7 F8D4F8EE 59534561 7F265D00


  Updated values

  V is
                                                F16E93 AA176CE5
        02A34636 37F10495 750150C9 75918C1D F401D091 28E7973A
        DA5B1E57 E1B86E79 96777094 1F778C27 8C10E15E 5AF873D8


  reseed_counter is
                                                   0000 00000002


rnd_val is
                                              B15DEC1B 266433D9
        7E587C87 1D15717A E15CA7B7 E616CFE1 0120523A E9504D80
        4E102D1C AFAFD3FF 677BEBBD 0C435952 505F8723 1D9EA679


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
```

```
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Process additional_input

    0x02||V||additional_input is
                           02F16E 93AA176C E502A346 3637F104
        95750150 C975918C 1DF401D0 9128E797 3ADA5B1E 57E1B86E
        79967770 941F778C 278C10E1 5E5AF873 D8A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    w=Hash(0x02||V||additional_input) is
                                                    6B2A78EE
        40118B02 0EBD27A2 812B5A04 4490BA01 A292FEC7 6FB262E6


    V is
                                              F16E93 AA176CE5
        02A34636 37F10495 750150C9 75918C1D F401D091 94121029
        1A6CA959 F075961C 17A2CA98 64084629 2EA3E025 CAAAD6BE


---------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------

    i = 1

    data is
                                              F16E93 AA176CE5
        02A34636 37F10495 750150C9 75918C1D F401D091 94121029
        1A6CA959 F075961C 17A2CA98 64084629 2EA3E025 CAAAD6BE


    w_i is
                                                    8E428812
        257FB69B 1A8C6712 88F702B0 A82574AF D2BA8868 F4124A7D
```

```
    W is
                                                        8E428812
        257FB69B 1A8C6712 88F702B0 A82574AF D2BA8868 F4124A7D


    ------------

    i = 2

    data is
                                              F16E93 AA176CE5
        02A34636 37F10495 750150C9 75918C1D F401D091 94121029
        1A6CA959 F075961C 17A2CA98 64084629 2EA3E025 CAAAD6BF


    w_i is
                                                        5A8EA256
        43141DA9 4042D1C7 170CB6B5 412F9178 84C5CA8D 6CD275F3


    W is
                                              8E428812 257FB69B
        1A8C6712 88F702B0 A82574AF D2BA8868 F4124A7D 5A8EA256
        43141DA9 4042D1C7 170CB6B5 412F9178 84C5CA8D 6CD275F3


  returned_bits is
                                              8E428812 257FB69B
        1A8C6712 88F702B0 A82574AF D2BA8868 F4124A7D 5A8EA256
        43141DA9 4042D1C7 170CB6B5 412F9178 84C5CA8D 6CD275F3


--------------------------

  Update V

    0x03||V is
                                              03F16E93 AA176CE5
        02A34636 37F10495 750150C9 75918C1D F401D091 94121029
        1A6CA959 F075961C 17A2CA98 64084629 2EA3E025 CAAAD6BE


    H is
                                                        41408548
        633CC968 D38560B6 AE43BB48 B6C6D1D9 A0E13F94 42BF565D
```

```
  Updated values

  V is
                                                 D72642 169D7456
        5D9A1305 6D179B58 06F58DDA 47761ABD C47343B2 956488CF
        2BBBFAF7 447A38B0 008FD8BF 23D9CBCA 5C49F349 755B6C95


  reseed_counter is
                                                   0000 00000003


rnd_val is
                                               8E428812 257FB69B
        1A8C6712 88F702B0 A82574AF D2BA8868 F4124A7D 5A8EA256
        43141DA9 4042D1C7 170CB6B5 412F9178 84C5CA8D 6CD275F3


################################################################

Hash_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                 C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
```

```
    Nonce =
                                                202122 23242526


    PersonalizationString =
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

###############################################################

***************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                202122 23242526


    personal_str is
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
```

```
    5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                                        0100
    0001B800 01020304 05060708 090A0B0C 0D0E0F10 11121314
    15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
    2D2E2F30 31323334 35362021 22232425 26404142 43444546
    4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
    5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


Hash(counter||no_of_bits_to_return||input_string) is
                                                    E2524D0E
    2D695606 3403E137 3C2A0310 5C27C33E FD4BE0E0 CB7462D9


temp =
                                                    E2524D0E
    2D695606 3403E137 3C2A0310 5C27C33E FD4BE0E0 CB7462D9


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                        0200
    0001B800 01020304 05060708 090A0B0C 0D0E0F10 11121314
    15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
    2D2E2F30 31323334 35362021 22232425 26404142 43444546
    4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
    5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


Hash(counter||no_of_bits_to_return||input_string) is
                                                    5FEA7A53
    F4A6C635 DC5FED69 1F36A168 A07266E7 75A7FB60 7BE9D680
```

```
    temp =
                                                E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


  V is
                                                E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              00E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 00E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                    FADECBC8
        A4B733F9 A903EFB7 F8C95434 54D37B2D 4C76B882 8A9A5463


    temp =
                                                    FADECBC8
        A4B733F9 A903EFB7 F8C95434 54D37B2D 4C76B882 8A9A5463


    ------------
```

```
    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        90A2F07A
        9E31D50D 5B7DE500 5AD7C1E8 9A3E1AFE D62C331D 6A561403


    temp =
                                              FADECB C8A4B733
        F9A903EF B7F8C954 3454D37B 2D4C76B8 828A9A54 6390A2F0
        7A9E31D5 0D5B7DE5 005AD7C1 E89A3E1A FED62C33 1D6A5614


  C is
                                              FADECB C8A4B733
        F9A903EF B7F8C954 3454D37B 2D4C76B8 828A9A54 6390A2F0
        7A9E31D5 0D5B7DE5 005AD7C1 E89A3E1A FED62C33 1D6A5614


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------

    i = 1
```

```
    data is
                                                E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


    w_i is
                                                        A13548D9
        029814B7 F142E991 5742B984 4EC5C386 E648CDA9 4BCDCE22


    W is
                                                        A13548D9
        029814B7 F142E991 5742B984 4EC5C386 E648CDA9 4BCDCE22


    ------------

    i = 2

    data is
                                                E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D7


    w_i is
                                                        60E79C86
        C06B5597 81E8DFEB BB978C76 0D04DAB9 56E79E7E D0065638


    W is
                                            A13548D9 029814B7
        F142E991 5742B984 4EC5C386 E648CDA9 4BCDCE22 60E79C86
        C06B5597 81E8DFEB BB978C76 0D04DAB9 56E79E7E D0065638


  returned_bits is
                                            A13548D9 029814B7
        F142E991 5742B984 4EC5C386 E648CDA9 4BCDCE22 60E79C86
        C06B5597 81E8DFEB BB978C76 0D04DAB9 56E79E7E D0065638


---------------------------
```

```
  Update V

    0x03||V is
                                                03E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


    H is
                                                            DAFAC71D
        EAFCE300 C98C6196 BB1AF5C8 F7FA2169 81211536 599E3665


  Updated values

  V is
                                                  DD3118 D6D22089
        FFDD07D0 EF34F357 44B0FB3E 6C49C299 63560EB8 17EB5488
        B98FBB9C 0CC43F69 2495042C 4934D1EB 676CE964 D7847650


  reseed_counter is
                                                     0000 00000002


rnd_val is
                                                A13548D9 029814B7
        F142E991 5742B984 4EC5C386 E648CDA9 4BCDCE22 60E79C86
        C06B5597 81E8DFEB BB978C76 0D04DAB9 56E79E7E D0065638


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

---------------------------

  Hashgen
```

```
  requested_no_of_bits  = 448

  ------------

  i = 1

  data is
                                                DD3118 D6D22089
      FFDD07D0 EF34F357 44B0FB3E 6C49C299 63560EB8 17EB5488
      B98FBB9C 0CC43F69 2495042C 4934D1EB 676CE964 D7847650


  w_i is
                                                        A2B1DC82
      42469DEC 61E738D1 2B3685FA D4D640B4 1C0D4343 03E6A185


  W is
                                                        A2B1DC82
      42469DEC 61E738D1 2B3685FA D4D640B4 1C0D4343 03E6A185


  ------------

  i = 2

  data is
                                                DD3118 D6D22089
      FFDD07D0 EF34F357 44B0FB3E 6C49C299 63560EB8 17EB5488
      B98FBB9C 0CC43F69 2495042C 4934D1EB 676CE964 D7847651


  w_i is
                                                        17CFF39A
      3C1FBF1B CBEF2B69 EB2C9A9D A76F5F49 D1BF3825 130A30D3


  W is
                                              A2B1DC82 42469DEC
      61E738D1 2B3685FA D4D640B4 1C0D4343 03E6A185 17CFF39A
      3C1FBF1B CBEF2B69 EB2C9A9D A76F5F49 D1BF3825 130A30D3


returned_bits is
                                              A2B1DC82 42469DEC
```

```
        61E738D1 2B3685FA D4D640B4 1C0D4343 03E6A185 17CFF39A
        3C1FBF1B CBEF2B69 EB2C9A9D A76F5F49 D1BF3825 130A30D3


---------------------------

  Update V

    0x03||V is
                                              03DD3118 D6D22089
        FFDD07D0 EF34F357 44B0FB3E 6C49C299 63560EB8 17EB5488
        B98FBB9C 0CC43F69 2495042C 4934D1EB 676CE964 D7847650


    H is
                                                    6FD91259
        78571F75 B50237AB EC52277E 95C7D59F A5CCB232 F080A043


  Updated values

  V is
                                                D80FE4 9F76D7BD
        F9860BC0 A72DBCAB 7905CEB9 99963951 E5E0A90C EB5509D2
        AC850CE6 CF21F4FA 1142036C C796E5A6 0C0FC7CA E56F6CA9


  reseed_counter is
                                                  0000 00000003


rnd_val is
                                              A2B1DC82 42469DEC
        61E738D1 2B3685FA D4D640B4 1C0D4343 03E6A185 17CFF39A
        3C1FBF1B CBEF2B69 EB2C9A9D A76F5F49 D1BF3825 130A30D3


###############################################################

Hash_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "NOT ENABLED"
```

```
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString =
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

Hash_DRBG_Instantiate_algorithm
```

```
    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                  202122 23242526


    personal_str is
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                             0100
        0001B800 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
                                                        E2524D0E
        2D695606 3403E137 3C2A0310 5C27C33E FD4BE0E0 CB7462D9


    temp =
                                                        E2524D0E
        2D695606 3403E137 3C2A0310 5C27C33E FD4BE0E0 CB7462D9


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                            0200
        0001B800 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        5FEA7A53
        F4A6C635 DC5FED69 1F36A168 A07266E7 75A7FB60 7BE9D680


    temp =
                                              E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


  V is
                                              E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            00E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
```

```
    53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                            01 000001B8 00E2524D 0E2D6956
    063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
    53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


Hash(counter||no_of_bits_to_return||input_string) is
                                                    FADECBC8
    A4B733F9 A903EFB7 F8C95434 54D37B2D 4C76B882 8A9A5463


temp =
                                                    FADECBC8
    A4B733F9 A903EFB7 F8C95434 54D37B2D 4C76B882 8A9A5463


------------

i = 2

counter||no_of_bits_to_return||input_string is
                            02 000001B8 00E2524D 0E2D6956
    063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
    53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


Hash(counter||no_of_bits_to_return||input_string) is
                                                    90A2F07A
    9E31D50D 5B7DE500 5AD7C1E8 9A3E1AFE D62C331D 6A561403


temp =
                                              FADECB C8A4B733
    F9A903EF B7F8C954 3454D37B 2D4C76B8 828A9A54 6390A2F0
    7A9E31D5 0D5B7DE5 005AD7C1 E89A3E1A FED62C33 1D6A5614
```

C is
                                                FADECB C8A4B733
      F9A903EF B7F8C954 3454D37B 2D4C76B8 828A9A54 6390A2F0
      7A9E31D5 0D5B7DE5 005AD7C1 E89A3E1A FED62C33 1D6A5614

First call to Generate

****

Hash_DRBG_Generate_algorithm

requested_number_of_bits = 448

additional_input
                                                606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596

Process additional_input

0x02||V||additional_input is
                          02E252 4D0E2D69 56063403 E1373C2A
      03105C27 C33EFD4B E0E0CB74 62D95FEA 7A53F4A6 C635DC5F
      ED691F36 A168A072 66E775A7 FB607BE9 D6606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596

w=Hash(0x02||V||additional_input) is
                                                      FC650A81
      245264C9 C4784731 6CC37582 91DDA47F 4276B81A 036889B5

V is
                                                E2524D 0E2D6956
      063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7463 D5C4F4FB
      78470B8F FA54A71E D5E2AC23 FA7E16E6 29EC6015 63E4738B

```
Hashgen

  requested_no_of_bits  = 448

  ------------

  i = 1

  data is
                                                E2524D 0E2D6956
      063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7463 D5C4F4FB
      78470B8F FA54A71E D5E2AC23 FA7E16E6 29EC6015 63E4738B


  w_i is
                                                       AE2E703E
      D178DC74 31D2B9C3 09C52AE4 AE5742AF C119A0FB 8F500FDD


  W is
                                                       AE2E703E
      D178DC74 31D2B9C3 09C52AE4 AE5742AF C119A0FB 8F500FDD


  ------------

  i = 2

  data is
                                                E2524D 0E2D6956
      063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7463 D5C4F4FB
      78470B8F FA54A71E D5E2AC23 FA7E16E6 29EC6015 63E4738C


  w_i is
                                                       83F17226
      1AD9FA6D 6203E549 33B07E9C B635CEA8 3F1F80FB 7A7153A1


  W is
                                             AE2E703E D178DC74
      31D2B9C3 09C52AE4 AE5742AF C119A0FB 8F500FDD 83F17226
      1AD9FA6D 6203E549 33B07E9C B635CEA8 3F1F80FB 7A7153A1
```

```
  returned_bits is
                                                AE2E703E D178DC74
        31D2B9C3 09C52AE4 AE5742AF C119A0FB 8F500FDD 83F17226
        1AD9FA6D 6203E549 33B07E9C B635CEA8 3F1F80FB 7A7153A1


--------------------------

  Update V

    0x03||V is
                                                03E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7463 D5C4F4FB
        78470B8F FA54A71E D5E2AC23 FA7E16E6 29EC6015 63E4738B


    H is
                                                            DA5B71E5
        F0C9872F A4BB580D ED2D80A5 7DB2582B FE2FB539 8C52A5F7


  Updated values

  V is
                                                  DD3118 D6D22089
        FFDD07D0 EF34F357 44B0FB3E 6C49C299 63560EB9 13B109D1
        E3AEC494 AC6B7D11 C36B048B 60CAAD2D 26F24182 0DA16F97


  reseed_counter is
                                                     0000 00000002


rnd_val is
                                                AE2E703E D178DC74
        31D2B9C3 09C52AE4 AE5742AF C119A0FB 8F500FDD 83F17226
        1AD9FA6D 6203E549 33B07E9C B635CEA8 3F1F80FB 7A7153A1


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm
```

```
  requested_number_of_bits = 448

  additional_input
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Process additional_input

    0x02||V||additional_input is
                           02DD31 18D6D220 89FFDD07 D0EF34F3
        5744B0FB 3E6C49C2 9963560E B913B109 D1E3AEC4 94AC6B7D
        11C36B04 8B60CAAD 2D26F241 820DA16F 97A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    w=Hash(0x02||V||additional_input) is
                                                        B90A7495
        AA5FCC34 49236DF0 7084B861 AE7B5FC3 50839FFE DB6589CC


    V is
                                                  DD3118 D6D22089
        FFDD07D0 EF34F357 44B0FB3E 6C49C299 63560EB9 CCBB7E67
        8E0E90C8 F58EEB02 33EFBCED 0F460CF0 7775E180 E906F963


---------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------

    i = 1

    data is
                                                  DD3118 D6D22089
        FFDD07D0 EF34F357 44B0FB3E 6C49C299 63560EB9 CCBB7E67
        8E0E90C8 F58EEB02 33EFBCED 0F460CF0 7775E180 E906F963
```

```
    w_i is
                                                          E3C91764
        215E04D2 9751C152 8D7CBBF8 4E7CC370 2ADA3A1F 79F87DBB


    W is
                                                          E3C91764
        215E04D2 9751C152 8D7CBBF8 4E7CC370 2ADA3A1F 79F87DBB


    ------------

    i = 2

    data is
                                                DD3118 D6D22089
        FFDD07D0 EF34F357 44B0FB3E 6C49C299 63560EB9 CCBB7E67
        8E0E90C8 F58EEB02 33EFBCED 0F460CF0 7775E180 E906F964


    w_i is
                                                          6043202F
        F7450A58 A73B95E3 2E4C0513 D0B6118A 677592EB ACC49FBE


    W is
                                              E3C91764 215E04D2
        9751C152 8D7CBBF8 4E7CC370 2ADA3A1F 79F87DBB 6043202F
        F7450A58 A73B95E3 2E4C0513 D0B6118A 677592EB ACC49FBE


  returned_bits is
                                              E3C91764 215E04D2
        9751C152 8D7CBBF8 4E7CC370 2ADA3A1F 79F87DBB 6043202F
        F7450A58 A73B95E3 2E4C0513 D0B6118A 677592EB ACC49FBE


--------------------------

  Update V

    0x03||V is
                                              03DD3118 D6D22089
        FFDD07D0 EF34F357 44B0FB3E 6C49C299 63560EB9 CCBB7E67
```

```
        8E0E90C8 F58EEB02 33EFBCED 0F460CF0 7775E180 E906F963


    H is
                                                        0C16F778
        4D6335D4 B4509A6E 9F6A44F5 364BC454 8A6582C2 C20D1FCB


  Updated values

  V is
                                                  D80FE4 9F76D7BD
        F9860BC0 A72DBCAB 7905CEB9 99963951 E5E0A90E 3C6318D0
        560FF872 B73B0355 D3B4D9A4 2E2C0F60 00B19076 C87E6F44


  reseed_counter is
                                                     0000 00000003


rnd_val is
                                               E3C91764 215E04D2
        9751C152 8D7CBBF8 4E7CC370 2ADA3A1F 79F87DBB 6043202F
        F7450A58 A73B95E3 2E4C0513 D0B6118A 677592EB ACC49FBE


###############################################################

Hash_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

```
    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                  202122 23242526


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                               0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    no_of_bits_to_return = 440
```

```
   ------------

   i = 1

   counter||no_of_bits_to_return||input_string is
                  010000 01B80001 02030405 06070809 0A0B0C0D
       0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
       26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


   Hash(counter||no_of_bits_to_return||input_string) is
                                                      0BB6E53D
       916573A7 AC796702 CA6DD2E3 0D13B8A3 ACFD7E23 905D6F8A


   temp =
                                                      0BB6E53D
       916573A7 AC796702 CA6DD2E3 0D13B8A3 ACFD7E23 905D6F8A


   ------------

   i = 2

   counter||no_of_bits_to_return||input_string is
                  020000 01B80001 02030405 06070809 0A0B0C0D
       0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
       26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


   Hash(counter||no_of_bits_to_return||input_string) is
                                                      33D18070
       2841C3D3 7CA40F35 645ECB1A A6548550 7F577CA9 8F418A0E


   temp =
                                                0BB6E5 3D916573
       A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
       702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


V is
                                                0BB6E5 3D916573
       A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
       702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A
```

```
---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                                 000BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 000BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


    Hash(counter||no_of_bits_to_return||input_string) is
                                                       E5B7AE6C
        8607715A F6CCCF35 2696C291 F43D10D1 E48E9FD0 717320C0


    temp =
                                                       E5B7AE6C
        8607715A F6CCCF35 2696C291 F43D10D1 E48E9FD0 717320C0


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                               02 000001B8 000BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


    Hash(counter||no_of_bits_to_return||input_string) is
                                                       11F35DAE
```

```
        12883480 7F41DD3A A952DE09 0AB3C78C C4D38F67 F13F7896


    temp =
                                                E5B7AE 6C860771
        5AF6CCCF 352696C2 91F43D10 D1E48E9F D0717320 C011F35D
        AE128834 807F41DD 3AA952DE 090AB3C7 8CC4D38F 67F13F78


  C is
                                                E5B7AE 6C860771
        5AF6CCCF 352696C2 91F43D10 D1E48E9F D0717320 C011F35D
        AE128834 807F41DD 3AA952DE 090AB3C7 8CC4D38F 67F13F78


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                             010BB6 E53D9165 73A7AC79 6702CA6D
```

```
    D2E30D13 B8A3ACFD 7E23905D 6F8A33D1 80702841 C3D37CA4
    0F35645E CB1AA654 85507F57 7CA98F41 8A808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
             01000001 B8010BB6 E53D9165 73A7AC79 6702CA6D
    D2E30D13 B8A3ACFD 7E23905D 6F8A33D1 80702841 C3D37CA4
    0F35645E CB1AA654 85507F57 7CA98F41 8A808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


Hash(counter||no_of_bits_to_return||input_string) is
                                                 61745177
    968386F7 F279CA4A 2434BF94 97B5DF91 29D19843 184B652B


temp =
                                                 61745177
    968386F7 F279CA4A 2434BF94 97B5DF91 29D19843 184B652B


------------

i = 2

counter||no_of_bits_to_return||input_string is
             02000001 B8010BB6 E53D9165 73A7AC79 6702CA6D
    D2E30D13 B8A3ACFD 7E23905D 6F8A33D1 80702841 C3D37CA4
    0F35645E CB1AA654 85507F57 7CA98F41 8A808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


Hash(counter||no_of_bits_to_return||input_string) is
                                                 EF41D39F
    DC19F1E4 C54298AD 29F596FA 8D4F47CD 0081697F AFB07A4B
```

```
    temp =
                                                 617451 77968386
        F7F279CA 4A2434BF 9497B5DF 9129D198 43184B65 2BEF41D3
        9FDC19F1 E4C54298 AD29F596 FA8D4F47 CD008169 7FAFB07A


  V is
                                                 617451 77968386
        F7F279CA 4A2434BF 9497B5DF 9129D198 43184B65 2BEF41D3
        9FDC19F1 E4C54298 AD29F596 FA8D4F47 CD008169 7FAFB07A


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                               00617451 77968386
        F7F279CA 4A2434BF 9497B5DF 9129D198 43184B65 2BEF41D3
        9FDC19F1 E4C54298 AD29F596 FA8D4F47 CD008169 7FAFB07A


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 00617451 77968386
        F7F279CA 4A2434BF 9497B5DF 9129D198 43184B65 2BEF41D3
        9FDC19F1 E4C54298 AD29F596 FA8D4F47 CD008169 7FAFB07A


    Hash(counter||no_of_bits_to_return||input_string) is
                                                     E5912949
        19DD3D92 743988D8 6C7927A6 94A6D90C 502FA7AA 5414F501


    temp =
                                                     E5912949
        19DD3D92 743988D8 6C7927A6 94A6D90C 502FA7AA 5414F501


    ------------
```

```
    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00617451 77968386
        F7F279CA 4A2434BF 9497B5DF 9129D198 43184B65 2BEF41D3
        9FDC19F1 E4C54298 AD29F596 FA8D4F47 CD008169 7FAFB07A


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        0A2967F3
        30B7C64E 191BDC23 0C6CF679 4031D63D 1E92E4D9 151FF346


    temp =
                                              E59129 4919DD3D
        92743988 D86C7927 A694A6D9 0C502FA7 AA5414F5 010A2967
        F330B7C6 4E191BDC 230C6CF6 794031D6 3D1E92E4 D9151FF3


  C is
                                              E59129 4919DD3D
        92743988 D86C7927 A694A6D9 0C502FA7 AA5414F5 010A2967
        F330B7C6 4E191BDC 230C6CF6 794031D6 3D1E92E4 D9151FF3


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------

    i = 1

    data is
                                              617451 77968386
```

```
        F7F279CA 4A2434BF 9497B5DF 9129D198 43184B65 2BEF41D3
        9FDC19F1 E4C54298 AD29F596 FA8D4F47 CD008169 7FAFB07A


    w_i is
                                                        3FE2AD85
        24CE60E7 C21C38A1 DAB02F3C 20501182 F389EE69 9F03FD87


    W is
                                                        3FE2AD85
        24CE60E7 C21C38A1 DAB02F3C 20501182 F389EE69 9F03FD87


    ------------

    i = 2

    data is
                                              617451 77968386
        F7F279CA 4A2434BF 9497B5DF 9129D198 43184B65 2BEF41D3
        9FDC19F1 E4C54298 AD29F596 FA8D4F47 CD008169 7FAFB07B


    w_i is
                                                        79ED17C6
        5B87ACEE EBF1D146 E7EE106C EC8955EE AFC18ABB C562A566


    W is
                                              3FE2AD85 24CE60E7
        C21C38A1 DAB02F3C 20501182 F389EE69 9F03FD87 79ED17C6
        5B87ACEE EBF1D146 E7EE106C EC8955EE AFC18ABB C562A566


  returned_bits is
                                              3FE2AD85 24CE60E7
        C21C38A1 DAB02F3C 20501182 F389EE69 9F03FD87 79ED17C6
        5B87ACEE EBF1D146 E7EE106C EC8955EE AFC18ABB C562A566


---------------------------

  Update V

    0x03||V is
```

```
                                                03617451 77968386
        F7F279CA 4A2434BF 9497B5DF 9129D198 43184B65 2BEF41D3
        9FDC19F1 E4C54298 AD29F596 FA8D4F47 CD008169 7FAFB07A


    H is
                                                          8F7D2138
        AD260EA2 51ECF405 9CFBA902 98790557 49981439 47C7CE66


  Updated values

  V is
                                                  47057A C0B060C4
        8A66B353 2290ADE7 3B2C5CB8 9D7A013F ED6C605A BC768C74
        4032E05A 84CB527A 6D320B90 0C468675 53B72887 A08C9ED4


  reseed_counter is
                                                     0000 00000002


rnd_val is
                                                3FE2AD85 24CE60E7
        C21C38A1 DAB02F3C 20501182 F389EE69 9F03FD87 79ED17C6
        5B87ACEE EBF1D146 E7EE106C EC8955EE AFC18ABB C562A566


-------------------------------------------------------------

Second call to Generate

*************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

Generate FAILED: Reseed is required
-------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
```

```
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  additional_input <empty>

----------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                           014705 7AC0B060 C48A66B3 532290AD
        E73B2C5C B89D7A01 3FED6C60 5ABC768C 744032E0 5A84CB52
        7A6D320B 900C4686 7553B728 87A08C9E D4C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                 01000001 B8014705 7AC0B060 C48A66B3 532290AD
        E73B2C5C B89D7A01 3FED6C60 5ABC768C 744032E0 5A84CB52
        7A6D320B 900C4686 7553B728 87A08C9E D4C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                      D061978A
        A8FA51B3 48ADD35F 9590A3E0 60826012 749A8AF8 3051C0B1


    temp =
                                                      D061978A
        A8FA51B3 48ADD35F 9590A3E0 60826012 749A8AF8 3051C0B1


    ------------

    i = 2
```

```
    counter||no_of_bits_to_return||input_string is
                02000001 B8014705 7AC0B060 C48A66B3 532290AD
        E73B2C5C B89D7A01 3FED6C60 5ABC768C 744032E0 5A84CB52
        7A6D320B 900C4686 7553B728 87A08C9E D4C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        5D22F7FD
        6C4BABE0 85D0232C 4AABF0AD C434722F B2B4DCBB 85E16C2D


    temp =
                                              D06197 8AA8FA51
        B348ADD3 5F9590A3 E0608260 12749A8A F83051C0 B15D22F7
        FD6C4BAB E085D023 2C4AABF0 ADC43472 2FB2B4DC BB85E16C


  V is
                                              D06197 8AA8FA51
        B348ADD3 5F9590A3 E0608260 12749A8A F83051C0 B15D22F7
        FD6C4BAB E085D023 2C4AABF0 ADC43472 2FB2B4DC BB85E16C


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            00D06197 8AA8FA51
        B348ADD3 5F9590A3 E0608260 12749A8A F83051C0 B15D22F7
        FD6C4BAB E085D023 2C4AABF0 ADC43472 2FB2B4DC BB85E16C


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 00D06197 8AA8FA51
        B348ADD3 5F9590A3 E0608260 12749A8A F83051C0 B15D22F7
        FD6C4BAB E085D023 2C4AABF0 ADC43472 2FB2B4DC BB85E16C
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                                                        708724BF
        4E161788 2C0EEF91 2F98DE09 CFD9B773 AE93E33E 3AD3F48A


    temp =
                                                        708724BF
        4E161788 2C0EEF91 2F98DE09 CFD9B773 AE93E33E 3AD3F48A


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00D06197 8AA8FA51
        B348ADD3 5F9590A3 E0608260 12749A8A F83051C0 B15D22F7
        FD6C4BAB E085D023 2C4AABF0 ADC43472 2FB2B4DC BB85E16C


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        91813DC5
        88497C56 9AAEDFB8 591AF62E E6679F0E 5F696843 D5664DCF


    temp =
                                                708724 BF4E1617
        882C0EEF 912F98DE 09CFD9B7 73AE93E3 3E3AD3F4 8A91813D
        C588497C 569AAEDF B8591AF6 2EE6679F 0E5F6968 43D5664D


  C is
                                                708724 BF4E1617
        882C0EEF 912F98DE 09CFD9B7 73AE93E3 3E3AD3F4 8A91813D
        C588497C 569AAEDF B8591AF6 2EE6679F 0E5F6968 43D5664D


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>
```

```
---------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------

    i = 1

    data is
                                                D06197 8AA8FA51
        B348ADD3 5F9590A3 E0608260 12749A8A F83051C0 B15D22F7
        FD6C4BAB E085D023 2C4AABF0 ADC43472 2FB2B4DC BB85E16C


    w_i is
                                                       8BB49B0B
        9C2FC701 89B24E02 73595458 CD780FBF A5F21612 2421B80B


    W is
                                                       8BB49B0B
        9C2FC701 89B24E02 73595458 CD780FBF A5F21612 2421B80B


    ------------

    i = 2

    data is
                                                D06197 8AA8FA51
        B348ADD3 5F9590A3 E0608260 12749A8A F83051C0 B15D22F7
        FD6C4BAB E085D023 2C4AABF0 ADC43472 2FB2B4DC BB85E16D


    w_i is
                                                       F773D736
        E6E11DEB B42477D6 9668D2F9 40C660F6 A2C1C9B4 179592E0


    W is
                                               8BB49B0B 9C2FC701
        89B24E02 73595458 CD780FBF A5F21612 2421B80B F773D736
        E6E11DEB B42477D6 9668D2F9 40C660F6 A2C1C9B4 179592E0
```

```
  returned_bits is
                                                  8BB49B0B 9C2FC701
        89B24E02 73595458 CD780FBF A5F21612 2421B80B F773D736
        E6E11DEB B42477D6 9668D2F9 40C660F6 A2C1C9B4 179592E0


---------------------------

  Update V

    0x03||V is
                                                  03D06197 8AA8FA51
        B348ADD3 5F9590A3 E0608260 12749A8A F83051C0 B15D22F7
        FD6C4BAB E085D023 2C4AABF0 ADC43472 2FB2B4DC BB85E16C


    H is
                                                              D187B76F
        837D624C C97B272F 04F68758 518D0E71 481D8A26 B15F5374


  Updated values

  V is
                                                    40E8BC 49F71069
        3B74BCC2 F0C52981 EA305C17 86232E6E 366B25B6 0D765BA5
        4671F775 009BA631 E99A4E3F 2E37AA82 862FA86B B0BA9B2E


  reseed_counter is
                                                      0000 00000002


rnd_val is
                                                  8BB49B0B 9C2FC701
        89B24E02 73595458 CD780FBF A5F21612 2421B80B F773D736
        E6E11DEB B42477D6 9668D2F9 40C660F6 A2C1C9B4 179592E0


##############################################################

Hash_DRBG

    Requested Security Strength = 112
```

```
    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

Hash_DRBG_Instantiate_algorithm
```

```
    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                  202122 23242526


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                               0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                    010000 01B80001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        0BB6E53D
        916573A7 AC796702 CA6DD2E3 0D13B8A3 ACFD7E23 905D6F8A


    temp =
                                                        0BB6E53D
        916573A7 AC796702 CA6DD2E3 0D13B8A3 ACFD7E23 905D6F8A
```

```
    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                  020000 01B80001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    Hash(counter||no_of_bits_to_return||input_string) is
                                                       33D18070
        2841C3D3 7CA40F35 645ECB1A A6548550 7F577CA9 8F418A0E


    temp =
                                              0BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


  V is
                                              0BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                           000BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 000BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
```

```
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        E5B7AE6C
        8607715A F6CCCF35 2696C291 F43D10D1 E48E9FD0 717320C0


    temp =
                                                        E5B7AE6C
        8607715A F6CCCF35 2696C291 F43D10D1 E48E9FD0 717320C0


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 000BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        11F35DAE
        12883480 7F41DD3A A952DE09 0AB3C78C C4D38F67 F13F7896


    temp =
                                                  E5B7AE 6C860771
        5AF6CCCF 352696C2 91F43D10 D1E48E9F D0717320 C011F35D
        AE128834 807F41DD 3AA952DE 090AB3C7 8CC4D38F 67F13F78


  C is
                                                  E5B7AE 6C860771
        5AF6CCCF 352696C2 91F43D10 D1E48E9F D0717320 C011F35D
        AE128834 807F41DD 3AA952DE 090AB3C7 8CC4D38F 67F13F78


------------------------------------------------------------

First call to Generate

************************************************************
```

```
Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            010B B6E53D91 6573A7AC 796702CA 6DD2E30D 13B8A3AC
        FD7E2390 5D6F8A33 D1807028 41C3D37C A40F3564 5ECB1AA6
        5485507F 577CA98F 418A8081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    no_of_bits_to_return = 440

    ------------

    i = 1
```

```
counter||no_of_bits_to_return||input_string is
                                                        010000
    01B8010B B6E53D91 6573A7AC 796702CA 6DD2E30D 13B8A3AC
    FD7E2390 5D6F8A33 D1807028 41C3D37C A40F3564 5ECB1AA6
    5485507F 577CA98F 418A8081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Hash(counter||no_of_bits_to_return||input_string) is
                                                      FCAB6277
    48788F7F EEF50098 68779B47 3D608D85 D2214B8B 231262E1


temp =
                                                      FCAB6277
    48788F7F EEF50098 68779B47 3D608D85 D2214B8B 231262E1


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                        020000
    01B8010B B6E53D91 6573A7AC 796702CA 6DD2E30D 13B8A3AC
    FD7E2390 5D6F8A33 D1807028 41C3D37C A40F3564 5ECB1AA6
    5485507F 577CA98F 418A8081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Hash(counter||no_of_bits_to_return||input_string) is
                                                      20DE6D88
    52E4679D 02FF39FF D6260E0D D59B11E1 22FD190F 2120DE4B


temp =
                                              FCAB62 7748788F
    7FEEF500 9868779B 473D608D 85D2214B 8B231262 E120DE6D
    8852E467 9D02FF39 FFD6260E 0DD59B11 E122FD19 0F2120DE
```

```
  V is
                                                 FCAB62 7748788F
        7FEEF500 9868779B 473D608D 85D2214B 8B231262 E120DE6D
        8852E467 9D02FF39 FFD6260E 0DD59B11 E122FD19 0F2120DE


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                               00FCAB62 7748788F
        7FEEF500 9868779B 473D608D 85D2214B 8B231262 E120DE6D
        8852E467 9D02FF39 FFD6260E 0DD59B11 E122FD19 0F2120DE


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 00FCAB62 7748788F
        7FEEF500 9868779B 473D608D 85D2214B 8B231262 E120DE6D
        8852E467 9D02FF39 FFD6260E 0DD59B11 E122FD19 0F2120DE


    Hash(counter||no_of_bits_to_return||input_string) is
                                                     37284C74
        6B01798D F00645F4 4F45B16F 162E3308 EABE1298 D80B27C8


    temp =
                                                     37284C74
        6B01798D F00645F4 4F45B16F 162E3308 EABE1298 D80B27C8


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                               02 000001B8 00FCAB62 7748788F
```

```
        7FEEF500 9868779B 473D608D 85D2214B 8B231262 E120DE6D
        8852E467 9D02FF39 FFD6260E 0DD59B11 E122FD19 0F2120DE


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        B59DBCB6
        5FE5CD7C 622751F2 14389150 1ED1BFCD 702D7DE5 326A5822


    temp =
                                              37284C 746B0179
        8DF00645 F44F45B1 6F162E33 08EABE12 98D80B27 C8B59DBC
        B65FE5CD 7C622751 F2143891 501ED1BF CD702D7D E5326A58


  C is
                                              37284C 746B0179
        8DF00645 F44F45B1 6F162E33 08EABE12 98D80B27 C8B59DBC
        B65FE5CD 7C622751 F2143891 501ED1BF CD702D7D E5326A58


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------

    i = 1

    data is
                                              FCAB62 7748788F
        7FEEF500 9868779B 473D608D 85D2214B 8B231262 E120DE6D
        8852E467 9D02FF39 FFD6260E 0DD59B11 E122FD19 0F2120DE


    w_i is
```

```
                                                        DE976A14
        41A637C1 B1B12E51 B6D08E77 4F6257D3 4A5D8415 D7334287


    W is
                                                        DE976A14
        41A637C1 B1B12E51 B6D08E77 4F6257D3 4A5D8415 D7334287


    ------------

    i = 2

    data is
                                              FCAB62 7748788F
        7FEEF500 9868779B 473D608D 85D2214B 8B231262 E120DE6D
        8852E467 9D02FF39 FFD6260E 0DD59B11 E122FD19 0F2120DF


    w_i is
                                                        EE68606D
        6936A310 A079D934 1BC828B4 D1BB7A94 D0BCB9F9 BDD3C926


    W is
                                              DE976A14 41A637C1
        B1B12E51 B6D08E77 4F6257D3 4A5D8415 D7334287 EE68606D
        6936A310 A079D934 1BC828B4 D1BB7A94 D0BCB9F9 BDD3C926


  returned_bits is
                                              DE976A14 41A637C1
        B1B12E51 B6D08E77 4F6257D3 4A5D8415 D7334287 EE68606D
        6936A310 A079D934 1BC828B4 D1BB7A94 D0BCB9F9 BDD3C926


--------------------------

  Update V

    0x03||V is
                                              03FCAB62 7748788F
        7FEEF500 9868779B 473D608D 85D2214B 8B231262 E120DE6D
        8852E467 9D02FF39 FFD6260E 0DD59B11 E122FD19 0F2120DE
```

```
    H is
                                                          D13D8EA6
        39863AC1 6CE34F4C D36365E0 D1A2EF5B 21314144 A950CAE2


  Updated values

  V is
                                                 33D3AE EBB37A09
        0DDEFB46 8CB7BD4C B6538EC0 8EBCDF5E 23FB1D8B 7B140AD0
        783904F6 864875D8 C54DC480 2F975C2C CFC46BDB 9DA45619


  reseed_counter is
                                                    0000 00000002


rnd_val is
                                               DE976A14 41A637C1
        B1B12E51 B6D08E77 4F6257D3 4A5D8415 D7334287 EE68606D
        6936A310 A079D934 1BC828B4 D1BB7A94 D0BCB9F9 BDD3C926


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
---------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                 C0C1C2 C3C4C5C6
```

```
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  additional_input
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0133 D3AEEBB3 7A090DDE FB468CB7 BD4CB653 8EC08EBC
        DF5E23FB 1D8B7B14 0AD07839 04F68648 75D8C54D C4802F97
        5C2CCFC4 6BDB9DA4 5619C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                        010000
        01B80133 D3AEEBB3 7A090DDE FB468CB7 BD4CB653 8EC08EBC
        DF5E23FB 1D8B7B14 0AD07839 04F68648 75D8C54D C4802F97
        5C2CCFC4 6BDB9DA4 5619C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                      609F2481
        705555CB 3B3FF6E7 70C6115B F69D1239 478D7E77 D862349E
```

```
    temp =
                                                          609F2481
        705555CB 3B3FF6E7 70C6115B F69D1239 478D7E77 D862349E


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                            020000
        01B80133 D3AEEBB3 7A090DDE FB468CB7 BD4CB653 8EC08EBC
        DF5E23FB 1D8B7B14 0AD07839 04F68648 75D8C54D C4802F97
        5C2CCFC4 6BDB9DA4 5619C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                          91A91BD5
        D0043690 034687A4 27F9B505 9AFF2774 B32688BA 9C8675CB


    temp =
                                                609F24 81705555
        CB3B3FF6 E770C611 5BF69D12 39478D7E 77D86234 9E91A91B
        D5D00436 90034687 A427F9B5 059AFF27 74B32688 BA9C8675


  V is
                                                609F24 81705555
        CB3B3FF6 E770C611 5BF69D12 39478D7E 77D86234 9E91A91B
        D5D00436 90034687 A427F9B5 059AFF27 74B32688 BA9C8675


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                               00609F24 81705555
        CB3B3FF6 E770C611 5BF69D12 39478D7E 77D86234 9E91A91B
        D5D00436 90034687 A427F9B5 059AFF27 74B32688 BA9C8675
```

```
  no_of_bits_to_return = 440

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                              01 000001B8 00609F24 81705555
      CB3B3FF6 E770C611 5BF69D12 39478D7E 77D86234 9E91A91B
      D5D00436 90034687 A427F9B5 059AFF27 74B32688 BA9C8675


  Hash(counter||no_of_bits_to_return||input_string) is
                                                    C0CCD185
      2BE68FE5 1D3B077B DC14D672 15306286 FAE0F914 4FB4755E


  temp =
                                                    C0CCD185
      2BE68FE5 1D3B077B DC14D672 15306286 FAE0F914 4FB4755E


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                              02 000001B8 00609F24 81705555
      CB3B3FF6 E770C611 5BF69D12 39478D7E 77D86234 9E91A91B
      D5D00436 90034687 A427F9B5 059AFF27 74B32688 BA9C8675


  Hash(counter||no_of_bits_to_return||input_string) is
                                                    7F045F9F
      75650E14 6FDFF3D4 7A492886 14E6C930 990BDB18 349833AB


  temp =
                                            C0CCD1 852BE68F
      E51D3B07 7BDC14D6 72153062 86FAE0F9 144FB475 5E7F045F
      9F75650E 146FDFF3 D47A4928 8614E6C9 30990BDB 18349833


C is
                                            C0CCD1 852BE68F
```

```
        E51D3B07 7BDC14D6 72153062 86FAE0F9 144FB475 5E7F045F
        9F75650E 146FDFF3 D47A4928 8614E6C9 30990BDB 18349833


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------

    i = 1

    data is
                                                609F24 81705555
        CB3B3FF6 E770C611 5BF69D12 39478D7E 77D86234 9E91A91B
        D5D00436 90034687 A427F9B5 059AFF27 74B32688 BA9C8675


    w_i is
                                                        E8593358
        63B8A94D 3A2CD1CD 810939EC F9E41B82 74A95724 0324C575


    W is
                                                        E8593358
        63B8A94D 3A2CD1CD 810939EC F9E41B82 74A95724 0324C575


    ------------

    i = 2

    data is
                                                609F24 81705555
        CB3B3FF6 E770C611 5BF69D12 39478D7E 77D86234 9E91A91B
        D5D00436 90034687 A427F9B5 059AFF27 74B32688 BA9C8676
```

```
    w_i is
                                                            7737A885
        78F0F807 1B1E5433 8CC81A72 6BC3836F 8941BF64 EC34B884


    W is
                                                E8593358 63B8A94D
        3A2CD1CD 810939EC F9E41B82 74A95724 0324C575 7737A885
        78F0F807 1B1E5433 8CC81A72 6BC3836F 8941BF64 EC34B884


  returned_bits is
                                                E8593358 63B8A94D
        3A2CD1CD 810939EC F9E41B82 74A95724 0324C575 7737A885
        78F0F807 1B1E5433 8CC81A72 6BC3836F 8941BF64 EC34B884


---------------------------

  Update V

    0x03||V is
                                                03609F24 81705555
        CB3B3FF6 E770C611 5BF69D12 39478D7E 77D86234 9E91A91B
        D5D00436 90034687 A427F9B5 059AFF27 74B32688 BA9C8675


    H is
                                                            F2FA7521
        1A83F14A 56A33E25 85992F86 12AD78B7 354FE28A 1D1DFB0D


  Updated values

  V is
                                                  216BF6 069C3BE5
        B0587AFE 634CDAE7 CE0BCD74 C0426E77 8C2816AA F00B229C
        8FC95A8E FB1664A0 FE3B7263 9E5D5EA7 DA9C14ED EFEF19B6


  reseed_counter is
                                                    0000 00000002
```

```
rnd_val is
                                                E8593358 63B8A94D
        3A2CD1CD 810939EC F9E41B82 74A95724 0324C575 7737A885
        78F0F807 1B1E5433 8CC81A72 6BC3836F 8941BF64 EC34B884


##############################################################

Hash_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString =
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

##############################################################
```

```
**************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                 202122 23242526


    personal_str is
                                                 404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                           0100
        0001B800 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
```

```
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        E2524D0E
        2D695606 3403E137 3C2A0310 5C27C33E FD4BE0E0 CB7462D9


    temp =
                                                        E2524D0E
        2D695606 3403E137 3C2A0310 5C27C33E FD4BE0E0 CB7462D9


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                              0200
        0001B800 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        5FEA7A53
        F4A6C635 DC5FED69 1F36A168 A07266E7 75A7FB60 7BE9D680


    temp =
                                                E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


  V is
                                                E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


--------------------------
```

```
Hash_df - Generate C - Step 4

  0x00||V is
                                              00E2524D 0E2D6956
      063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
      53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


  no_of_bits_to_return = 440

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                              01 000001B8 00E2524D 0E2D6956
      063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
      53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


  Hash(counter||no_of_bits_to_return||input_string) is
                                                    FADECBC8
      A4B733F9 A903EFB7 F8C95434 54D37B2D 4C76B882 8A9A5463


  temp =
                                                    FADECBC8
      A4B733F9 A903EFB7 F8C95434 54D37B2D 4C76B882 8A9A5463


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                              02 000001B8 00E2524D 0E2D6956
      063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
      53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


  Hash(counter||no_of_bits_to_return||input_string) is
                                                    90A2F07A
      9E31D50D 5B7DE500 5AD7C1E8 9A3E1AFE D62C331D 6A561403


  temp =
```

                                                FADECB C8A4B733
        F9A903EF B7F8C954 3454D37B 2D4C76B8 828A9A54 6390A2F0
        7A9E31D5 0D5B7DE5 005AD7C1 E89A3E1A FED62C33 1D6A5614

  C is
                                                FADECB C8A4B733
        F9A903EF B7F8C954 3454D37B 2D4C76B8 828A9A54 6390A2F0
        7A9E31D5 0D5B7DE5 005AD7C1 E89A3E1A FED62C33 1D6A5614

First call to Generate

****

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

Generate FAILED: Reseed is required

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6

  additional_input <empty>

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                            01E252 4D0E2D69 56063403 E1373C2A
        03105C27 C33EFD4B E0E0CB74 62D95FEA 7A53F4A6 C635DC5F
        ED691F36 A168A072 66E775A7 FB607BE9 D6808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6

```
no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
             01000001 B801E252 4D0E2D69 56063403 E1373C2A
    03105C27 C33EFD4B E0E0CB74 62D95FEA 7A53F4A6 C635DC5F
    ED691F36 A168A072 66E775A7 FB607BE9 D6808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


Hash(counter||no_of_bits_to_return||input_string) is
                                                564A35DB
    8325A793 1214594B CFC4A00D B9F4129E 89BA79BA 5FE29EDC


temp =
                                                564A35DB
    8325A793 1214594B CFC4A00D B9F4129E 89BA79BA 5FE29EDC


------------

i = 2

counter||no_of_bits_to_return||input_string is
             02000001 B801E252 4D0E2D69 56063403 E1373C2A
    03105C27 C33EFD4B E0E0CB74 62D95FEA 7A53F4A6 C635DC5F
    ED691F36 A168A072 66E775A7 FB607BE9 D6808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


Hash(counter||no_of_bits_to_return||input_string) is
                                                610C0841
    28F1C76C 654FD153 BDCA19F1 C1C076B7 4B8DC995 4767B399


temp =
                                              564A35 DB8325A7
    93121459 4BCFC4A0 0DB9F412 9E89BA79 BA5FE29E DC610C08
```

```
        4128F1C7 6C654FD1 53BDCA19 F1C1C076 B74B8DC9 954767B3


  V is
                                                564A35 DB8325A7
        93121459 4BCFC4A0 0DB9F412 9E89BA79 BA5FE29E DC610C08
        4128F1C7 6C654FD1 53BDCA19 F1C1C076 B74B8DC9 954767B3


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                             00564A35 DB8325A7
        93121459 4BCFC4A0 0DB9F412 9E89BA79 BA5FE29E DC610C08
        4128F1C7 6C654FD1 53BDCA19 F1C1C076 B74B8DC9 954767B3


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 00564A35 DB8325A7
        93121459 4BCFC4A0 0DB9F412 9E89BA79 BA5FE29E DC610C08
        4128F1C7 6C654FD1 53BDCA19 F1C1C076 B74B8DC9 954767B3


    Hash(counter||no_of_bits_to_return||input_string) is
                                                       4D3FC5A7
        AF736648 D9432578 04E5A34F EE10D86A 1DAE2041 8A14EF1A


    temp =
                                                       4D3FC5A7
        AF736648 D9432578 04E5A34F EE10D86A 1DAE2041 8A14EF1A


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
```

```
                                02 000001B8 00564A35 DB8325A7
        93121459 4BCFC4A0 0DB9F412 9E89BA79 BA5FE29E DC610C08
        4128F1C7 6C654FD1 53BDCA19 F1C1C076 B74B8DC9 954767B3


    Hash(counter||no_of_bits_to_return||input_string) is
                                                      56D55D4B
        B3D34A32 385822C3 BDB2BE83 0AAFD635 679F60CE 5790A03E


    temp =
                                               4D3FC5 A7AF7366
        48D94325 7804E5A3 4FEE10D8 6A1DAE20 418A14EF 1A56D55D
        4BB3D34A 32385822 C3BDB2BE 830AAFD6 35679F60 CE5790A0


  C is
                                               4D3FC5 A7AF7366
        48D94325 7804E5A3 4FEE10D8 6A1DAE20 418A14EF 1A56D55D
        4BB3D34A 32385822 C3BDB2BE 830AAFD6 35679F60 CE5790A0


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------

    i = 1

    data is
                                               564A35 DB8325A7
        93121459 4BCFC4A0 0DB9F412 9E89BA79 BA5FE29E DC610C08
        4128F1C7 6C654FD1 53BDCA19 F1C1C076 B74B8DC9 954767B3
```

```
    w_i is
                                                          B390977A
        DEFACF7D 3DF3C5B2 533FCC45 113DAEB1 9366DF1E 0A6EA52B


    W is
                                                          B390977A
        DEFACF7D 3DF3C5B2 533FCC45 113DAEB1 9366DF1E 0A6EA52B


    ------------

    i = 2

    data is
                                                 564A35 DB8325A7
        93121459 4BCFC4A0 0DB9F412 9E89BA79 BA5FE29E DC610C08
        4128F1C7 6C654FD1 53BDCA19 F1C1C076 B74B8DC9 954767B4


    w_i is
                                                          4D35B60C
        584D75A0 D8E6A31C 6941C885 A7B25EBB 61C220E0 2DDB0426


    W is
                                                 B390977A DEFACF7D
        3DF3C5B2 533FCC45 113DAEB1 9366DF1E 0A6EA52B 4D35B60C
        584D75A0 D8E6A31C 6941C885 A7B25EBB 61C220E0 2DDB0426


  returned_bits is
                                                 B390977A DEFACF7D
        3DF3C5B2 533FCC45 113DAEB1 9366DF1E 0A6EA52B 4D35B60C
        584D75A0 D8E6A31C 6941C885 A7B25EBB 61C220E0 2DDB0426


---------------------------

  Update V

    0x03||V is
                                                 03564A35 DB8325A7
        93121459 4BCFC4A0 0DB9F412 9E89BA79 BA5FE29E DC610C08
        4128F1C7 6C654FD1 53BDCA19 F1C1C076 B74B8DC9 954767B3
```

```
    H is
                                                          380EBE6A
         AFD83737 E58795AC 92561432 F333A595 34DADC6C 94D69945


  Updated values

  V is
                                                  A389FB 8332990D
         DBEB577E C3D4AA43 5DA804EB 08A76899 FBE9F78E 2EC69FD0
         3CB4FC49 84253DA0 A9D1910B 680015E2 218E0996 F8759199


  reseed_counter is
                                                    0000 00000002


rnd_val is
                                                 B390977A DEFACF7D
         3DF3C5B2 533FCC45 113DAEB1 9366DF1E 0A6EA52B 4D35B60C
         584D75A0 D8E6A31C 6941C885 A7B25EBB 61C220E0 2DDB0426


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                  C0C1C2 C3C4C5C6
         C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
         DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
```

```
  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                            01A389 FB833299 0DDBEB57 7EC3D4AA
        435DA804 EB08A768 99FBE9F7 8E2EC69F D03CB4FC 4984253D
        A0A9D191 0B680015 E2218E09 96F87591 99C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                 01000001 B801A389 FB833299 0DDBEB57 7EC3D4AA
        435DA804 EB08A768 99FBE9F7 8E2EC69F D03CB4FC 4984253D
        A0A9D191 0B680015 E2218E09 96F87591 99C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                    C792A300
        9915EAC0 3FE567B3 70AB5B70 D7C8B9FE 1D8BA65B 73054353


    temp =
                                                    C792A300
        9915EAC0 3FE567B3 70AB5B70 D7C8B9FE 1D8BA65B 73054353


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                 02000001 B801A389 FB833299 0DDBEB57 7EC3D4AA
        435DA804 EB08A768 99FBE9F7 8E2EC69F D03CB4FC 4984253D
```

```
        A0A9D191 0B680015 E2218E09 96F87591 99C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        D761BD4D
        04B6964D AC8FC294 83E3E3F0 A584B853 2BB01E0F 18FEE1D1


    temp =
                                              C792A3 009915EA
        C03FE567 B370AB5B 70D7C8B9 FE1D8BA6 5B730543 53D761BD
        4D04B696 4DAC8FC2 9483E3E3 F0A584B8 532BB01E 0F18FEE1


  V is
                                              C792A3 009915EA
        C03FE567 B370AB5B 70D7C8B9 FE1D8BA6 5B730543 53D761BD
        4D04B696 4DAC8FC2 9483E3E3 F0A584B8 532BB01E 0F18FEE1


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            00C792A3 009915EA
        C03FE567 B370AB5B 70D7C8B9 FE1D8BA6 5B730543 53D761BD
        4D04B696 4DAC8FC2 9483E3E3 F0A584B8 532BB01E 0F18FEE1


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 00C792A3 009915EA
        C03FE567 B370AB5B 70D7C8B9 FE1D8BA6 5B730543 53D761BD
        4D04B696 4DAC8FC2 9483E3E3 F0A584B8 532BB01E 0F18FEE1


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        C9B79D99
```

```
        F0E8F7C2 0325C58E F8DCF907 6255EDF4 820DC35B A1DA01B7


    temp =
                                                        C9B79D99
        F0E8F7C2 0325C58E F8DCF907 6255EDF4 820DC35B A1DA01B7


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00C792A3 009915EA
        C03FE567 B370AB5B 70D7C8B9 FE1D8BA6 5B730543 53D761BD
        4D04B696 4DAC8FC2 9483E3E3 F0A584B8 532BB01E 0F18FEE1


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        CA142C8D
        58157FD7 76D401A9 55995DB7 08141880 A4F8E118 7C919F17


    temp =
                                              C9B79D 99F0E8F7
        C20325C5 8EF8DCF9 076255ED F4820DC3 5BA1DA01 B7CA142C
        8D58157F D776D401 A955995D B7081418 80A4F8E1 187C919F


  C is
                                              C9B79D 99F0E8F7
        C20325C5 8EF8DCF9 076255ED F4820DC3 5BA1DA01 B7CA142C
        8D58157F D776D401 A955995D B7081418 80A4F8E1 187C919F


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

----------------------------

  Hashgen
```

```
  requested_no_of_bits  = 448

  ------------

  i = 1

  data is
                                              C792A3 009915EA
      C03FE567 B370AB5B 70D7C8B9 FE1D8BA6 5B730543 53D761BD
      4D04B696 4DAC8FC2 9483E3E3 F0A584B8 532BB01E 0F18FEE1


  w_i is
                                                    258437C9
      CF68A286 1F3BE81F 80AC7864 78B65211 3613F79C 6D21C020


  W is
                                                    258437C9
      CF68A286 1F3BE81F 80AC7864 78B65211 3613F79C 6D21C020


  ------------

  i = 2

  data is
                                              C792A3 009915EA
      C03FE567 B370AB5B 70D7C8B9 FE1D8BA6 5B730543 53D761BD
      4D04B696 4DAC8FC2 9483E3E3 F0A584B8 532BB01E 0F18FEE2


  w_i is
                                                    B6CA5DFC
      35875873 10777745 B0B49B04 3EC0E4CD E1A31A57 C187E64D


  W is
                                           258437C9 CF68A286
      1F3BE81F 80AC7864 78B65211 3613F79C 6D21C020 B6CA5DFC
      35875873 10777745 B0B49B04 3EC0E4CD E1A31A57 C187E64D


returned_bits is
                                           258437C9 CF68A286
```

```
        1F3BE81F 80AC7864 78B65211 3613F79C 6D21C020 B6CA5DFC
        35875873 10777745 B0B49B04 3EC0E4CD E1A31A57 C187E64D


---------------------------

  Update V

    0x03||V is
                                              03C792A3 009915EA
        C03FE567 B370AB5B 70D7C8B9 FE1D8BA6 5B730543 53D761BD
        4D04B696 4DAC8FC2 9483E3E3 F0A584B8 532BB01E 0F18FEE1


    H is
                                                    6E801A28
        3CFDD3FA 7520BDAF 88C6FE83 2175EA33 567F3946 5F991C69


  Updated values

  V is
                                                914A40 9A89FEE2
        82430B2D 42698854 783A1EA7 F29F9969 B714DF45 7A219012
        175AA010 9A442173 C6A07BC4 C9238304 2A4FE245 872EACEA


  reseed_counter is
                                                  0000 00000002


rnd_val is
                                              258437C9 CF68A286
        1F3BE81F 80AC7864 78B65211 3613F79C 6D21C020 B6CA5DFC
        35875873 10777745 B0B49B04 3EC0E4CD E1A31A57 C187E64D


################################################################

Hash_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "ENABLED"
```

```
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString =
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

Hash_DRBG_Instantiate_algorithm
```

```
    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                  202122 23242526


    personal_str is
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                              0100
        0001B800 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
                                                        E2524D0E
        2D695606 3403E137 3C2A0310 5C27C33E FD4BE0E0 CB7462D9


    temp =
                                                        E2524D0E
        2D695606 3403E137 3C2A0310 5C27C33E FD4BE0E0 CB7462D9


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                            0200
        0001B800 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        5FEA7A53
        F4A6C635 DC5FED69 1F36A168 A07266E7 75A7FB60 7BE9D680


    temp =
                                              E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


  V is
                                              E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            00E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
```

```
    53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                            01 000001B8 00E2524D 0E2D6956
    063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
    53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


Hash(counter||no_of_bits_to_return||input_string) is
                                                    FADECBC8
    A4B733F9 A903EFB7 F8C95434 54D37B2D 4C76B882 8A9A5463


temp =
                                                    FADECBC8
    A4B733F9 A903EFB7 F8C95434 54D37B2D 4C76B882 8A9A5463


------------

i = 2

counter||no_of_bits_to_return||input_string is
                            02 000001B8 00E2524D 0E2D6956
    063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
    53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


Hash(counter||no_of_bits_to_return||input_string) is
                                                    90A2F07A
    9E31D50D 5B7DE500 5AD7C1E8 9A3E1AFE D62C331D 6A561403


temp =
                                              FADECB C8A4B733
    F9A903EF B7F8C954 3454D37B 2D4C76B8 828A9A54 6390A2F0
    7A9E31D5 0D5B7DE5 005AD7C1 E89A3E1A FED62C33 1D6A5614
```

```
  C is
                                                FADECB C8A4B733
        F9A903EF B7F8C954 3454D37B 2D4C76B8 828A9A54 6390A2F0
        7A9E31D5 0D5B7DE5 005AD7C1 E89A3E1A FED62C33 1D6A5614


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01E2 524D0E2D 69560634 03E1373C 2A03105C 27C33EFD
        4BE0E0CB 7462D95F EA7A53F4 A6C635DC 5FED691F 36A168A0
```

```
    7266E775 A7FB607B E9D68081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                                      010000
    01B801E2 524D0E2D 69560634 03E1373C 2A03105C 27C33EFD
    4BE0E0CB 7462D95F EA7A53F4 A6C635DC 5FED691F 36A168A0
    7266E775 A7FB607B E9D68081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Hash(counter||no_of_bits_to_return||input_string) is
                                                    96C7FF18
    C18C5000 958F19BD D20537ED A5A01AA0 E0ACBD40 F3E77215


temp =
                                                    96C7FF18
    C18C5000 958F19BD D20537ED A5A01AA0 E0ACBD40 F3E77215


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
    01B801E2 524D0E2D 69560634 03E1373C 2A03105C 27C33EFD
    4BE0E0CB 7462D95F EA7A53F4 A6C635DC 5FED691F 36A168A0
    7266E775 A7FB607B E9D68081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
```

```
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        46E4741C
        7BB1E820 3272FFA4 1A565735 65884C04 59569DDA D61A7A9F


    temp =
                                              96C7FF 18C18C50
        00958F19 BDD20537 EDA5A01A A0E0ACBD 40F3E772 1546E474
        1C7BB1E8 203272FF A41A5657 3565884C 0459569D DAD61A7A


  V is
                                              96C7FF 18C18C50
        00958F19 BDD20537 EDA5A01A A0E0ACBD 40F3E772 1546E474
        1C7BB1E8 203272FF A41A5657 3565884C 0459569D DAD61A7A


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            0096C7FF 18C18C50
        00958F19 BDD20537 EDA5A01A A0E0ACBD 40F3E772 1546E474
        1C7BB1E8 203272FF A41A5657 3565884C 0459569D DAD61A7A


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 0096C7FF 18C18C50
        00958F19 BDD20537 EDA5A01A A0E0ACBD 40F3E772 1546E474
        1C7BB1E8 203272FF A41A5657 3565884C 0459569D DAD61A7A


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        3E4105EB
        0DB7617D 06346DA9 3405164C 23FA5247 E549890C 761D7990
```

```
    temp =
                                                        3E4105EB
        0DB7617D 06346DA9 3405164C 23FA5247 E549890C 761D7990


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                               02 000001B8 0096C7FF 18C18C50
        00958F19 BDD20537 EDA5A01A A0E0ACBD 40F3E772 1546E474
        1C7BB1E8 203272FF A41A5657 3565884C 0459569D DAD61A7A


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        B06074C0
        564F00E0 010D23D2 DF8FABBC 5CE4A434 14A46EF8 A63C0BDC


    temp =
                                                  3E4105 EB0DB761
        7D06346D A9340516 4C23FA52 47E54989 0C761D79 90B06074
        C0564F00 E0010D23 D2DF8FAB BC5CE4A4 3414A46E F8A63C0B


  C is
                                                  3E4105 EB0DB761
        7D06346D A9340516 4C23FA52 47E54989 0C761D79 90B06074
        C0564F00 E0010D23 D2DF8FAB BC5CE4A4 3414A46E F8A63C0B


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 448
```

```
  ------------

  i = 1

  data is
                                                96C7FF 18C18C50
      00958F19 BDD20537 EDA5A01A A0E0ACBD 40F3E772 1546E474
      1C7BB1E8 203272FF A41A5657 3565884C 0459569D DAD61A7A


  w_i is
                                                       E41DCEFB
      B418588E 7AB62A63 0D52A955 E55CE37A 79DB568B CFA10A57


  W is
                                                       E41DCEFB
      B418588E 7AB62A63 0D52A955 E55CE37A 79DB568B CFA10A57


  ------------

  i = 2

  data is
                                                96C7FF 18C18C50
      00958F19 BDD20537 EDA5A01A A0E0ACBD 40F3E772 1546E474
      1C7BB1E8 203272FF A41A5657 3565884C 0459569D DAD61A7B


  w_i is
                                                       CD89C490
      447D43A8 83CDF14C F6367FC1 9EA52A46 3A1FE2EB 7DF168F6


  W is
                                             E41DCEFB B418588E
      7AB62A63 0D52A955 E55CE37A 79DB568B CFA10A57 CD89C490
      447D43A8 83CDF14C F6367FC1 9EA52A46 3A1FE2EB 7DF168F6


returned_bits is
                                             E41DCEFB B418588E
      7AB62A63 0D52A955 E55CE37A 79DB568B CFA10A57 CD89C490
      447D43A8 83CDF14C F6367FC1 9EA52A46 3A1FE2EB 7DF168F6
```

```
---------------------------

  Update V

    0x03||V is
                                                0396C7FF 18C18C50
        00958F19 BDD20537 EDA5A01A A0E0ACBD 40F3E772 1546E474
        1C7BB1E8 203272FF A41A5657 3565884C 0459569D DAD61A7A


    H is
                                                          8A397569
        1FBBD432 E574BB4E 64A74C4F 76506178 425EC799 1305F482


  Updated values

  V is
                                                  D50905 03CF43B1
        7D9BC387 67060A4E 39C99A6C E8C5F646 4D6A04EC 3030BA51
        FC8DD51B E5A83B71 DBA13252 6812CE68 7ACCC2A5 E6824B08


  reseed_counter is
                                                     0000 00000002


rnd_val is
                                                E41DCEFB B418588E
        7AB62A63 0D52A955 E55CE37A 79DB568B CFA10A57 CD89C490
        447D43A8 83CDF14C F6367FC1 9EA52A46 3A1FE2EB 7DF168F6


-------------------------------------------------------------

Second call to Generate

*************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input
```

```
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  additional_input
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01D5 090503CF 43B17D9B C3876706 0A4E39C9 9A6CE8C5
        F6464D6A 04EC3030 BA51FC8D D51BE5A8 3B71DBA1 32526812
        CE687ACC C2A5E682 4B08C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                        010000
        01B801D5 090503CF 43B17D9B C3876706 0A4E39C9 9A6CE8C5
        F6464D6A 04EC3030 BA51FC8D D51BE5A8 3B71DBA1 32526812
```

```
        CE687ACC C2A5E682 4B08C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        FCC6C861
        900DDB57 BDC97001 8F6CF691 59C1B68E BA85E4B0 A9E2FDF3


    temp =
                                                        FCC6C861
        900DDB57 BDC97001 8F6CF691 59C1B68E BA85E4B0 A9E2FDF3


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                          020000
        01B801D5 090503CF 43B17D9B C3876706 0A4E39C9 9A6CE8C5
        F6464D6A 04EC3030 BA51FC8D D51BE5A8 3B71DBA1 32526812
        CE687ACC C2A5E682 4B08C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        CEAB36C7
        DC9BC0A1 4BB7AB98 7481DB03 C014DAE1 3E734896 007224AA


    temp =
                                                FCC6C8 61900DDB
        57BDC970 018F6CF6 9159C1B6 8EBA85E4 B0A9E2FD F3CEAB36
        C7DC9BC0 A14BB7AB 987481DB 03C014DA E13E7348 96007224


V is
                                                FCC6C8 61900DDB
        57BDC970 018F6CF6 9159C1B6 8EBA85E4 B0A9E2FD F3CEAB36
```

```
        C7DC9BC0 A14BB7AB 987481DB 03C014DA E13E7348 96007224


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              00FCC6C8 61900DDB
        57BDC970 018F6CF6 9159C1B6 8EBA85E4 B0A9E2FD F3CEAB36
        C7DC9BC0 A14BB7AB 987481DB 03C014DA E13E7348 96007224


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 00FCC6C8 61900DDB
        57BDC970 018F6CF6 9159C1B6 8EBA85E4 B0A9E2FD F3CEAB36
        C7DC9BC0 A14BB7AB 987481DB 03C014DA E13E7348 96007224


    Hash(counter||no_of_bits_to_return||input_string) is
                                                    3618B297
        02390319 E360A7FC 627EC87B B6B1DA4A 36D40BB4 2030D850


    temp =
                                                    3618B297
        02390319 E360A7FC 627EC87B B6B1DA4A 36D40BB4 2030D850


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                               02 000001B8 00FCC6C8 61900DDB
        57BDC970 018F6CF6 9159C1B6 8EBA85E4 B0A9E2FD F3CEAB36
        C7DC9BC0 A14BB7AB 987481DB 03C014DA E13E7348 96007224


    Hash(counter||no_of_bits_to_return||input_string) is
```

                                                    D6FEBBB0
        BFC783A8 034F3B2F 02F272FD 91507588 6A0F6C44 3DD2FEFD

    temp =
                                                  3618B2 97023903
        19E360A7 FC627EC8 7BB6B1DA 4A36D40B B42030D8 50D6FEBB
        B0BFC783 A8034F3B 2F02F272 FD915075 886A0F6C 443DD2FE

  C is
                                                  3618B2 97023903
        19E360A7 FC627EC8 7BB6B1DA 4A36D40B B42030D8 50D6FEBB
        B0BFC783 A8034F3B 2F02F272 FD915075 886A0F6C 443DD2FE

****

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

  Hashgen

    requested_no_of_bits = 448

    ----

    i = 1

    data is
                                                  FCC6C8 61900DDB
        57BDC970 018F6CF6 9159C1B6 8EBA85E4 B0A9E2FD F3CEAB36
        C7DC9BC0 A14BB7AB 987481DB 03C014DA E13E7348 96007224

    w_i is
                                                    098BD7FB
        3E7B0673 F319E2ED A9240C9F 7A657200 C0F5482E BEE4EEC1

    W is

                                                    098BD7FB
        3E7B0673 F319E2ED A9240C9F 7A657200 C0F5482E BEE4EEC1

    ----

    i = 2

    data is
                                                  FCC6C8 61900DDB
        57BDC970 018F6CF6 9159C1B6 8EBA85E4 B0A9E2FD F3CEAB36
        C7DC9BC0 A14BB7AB 987481DB 03C014DA E13E7348 96007225

    w_i is
                                                    C6395339
        E48B0B7A 01456745 BE894FC1 8A98B252 258DAEC4 D878C086

    W is
                                            098BD7FB 3E7B0673
        F319E2ED A9240C9F 7A657200 C0F5482E BEE4EEC1 C6395339
        E48B0B7A 01456745 BE894FC1 8A98B252 258DAEC4 D878C086

  returned_bits is
                                            098BD7FB 3E7B0673
        F319E2ED A9240C9F 7A657200 C0F5482E BEE4EEC1 C6395339
        E48B0B7A 01456745 BE894FC1 8A98B252 258DAEC4 D878C086

  Update V

    0x03||V is
                                            03FCC6C8 61900DDB
        57BDC970 018F6CF6 9159C1B6 8EBA85E4 B0A9E2FD F3CEAB36
        C7DC9BC0 A14BB7AB 987481DB 03C014DA E13E7348 96007224

    H is
                                                    CAED9D58
        9C88C301 C7611C02 E83ABC6F D76797DC CCCA8788 D91A3DB6

Updated values

V is

32DF7A F89246DE
71A12A17 FDF1EBBF 0D107390 D8F159F0 64CA13D7 0F93474B
15252646 10B022E9 AFB230BD D8B8FD2D 36730A3D B35882D9

reseed_counter is

0000 00000002

rnd_val is

098BD7FB 3E7B0673
F319E2ED A9240C9F 7A657200 C0F5482E BEE4EEC1 C6395339
E48B0B7A 01456745 BE894FC1 8A98B252 258DAEC4 D878C086

```
################################################################

Hash_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                 20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    nonce is
                                                20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                              000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                 01000001 B8000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    Hash(counter||no_of_bits_to_return||input_string) is
                                               AB41CDE4 37AB8B09
        1CA7C575 5D10F011 0C1DBD46 2F226CFD ABFBB04A 8BCDEF95


    temp =
                                               AB41CDE4 37AB8B09
        1CA7C575 5D10F011 0C1DBD46 2F226CFD ABFBB04A 8BCDEF95


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
```

```
                02000001 B8000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    Hash(counter||no_of_bits_to_return||input_string) is
                                              167D84AF 64128C0D
        71F4D5B8 C0EDFBBE 3DF40448 D2D8E12F A91BA8B0 97969506


    temp =
                                                AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


  V is
                                                AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              00AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 00AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    Hash(counter||no_of_bits_to_return||input_string) is
                                              E15DE4A8 E3B1419B
```

```
        61D534F1 5DBD31EE 19EC595F 8B98111A 94F52237 AD5D66F0


    temp =
                                              E15DE4A8 E3B1419B
        61D534F1 5DBD31EE 19EC595F 8B98111A 94F52237 AD5D66F0


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    Hash(counter||no_of_bits_to_return||input_string) is
                                              CFAAFDDC 90195902
        E979F79B 65357FEA 85998E4E 37D2C1D4 FD0F0D66 3A829565


    temp =
                                                E15DE4 A8E3B141
        9B61D534 F15DBD31 EE19EC59 5F8B9811 1A94F522 37AD5D66
        F0CFAAFD DC901959 02E979F7 9B65357F EA85998E 4E37D2C1


  C is
                                                E15DE4 A8E3B141
        9B61D534 F15DBD31 EE19EC59 5F8B9811 1A94F522 37AD5D66
        F0CFAAFD DC901959 02E979F7 9B65357F EA85998E 4E37D2C1


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>
```

```
---------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1

    data is
                                                AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    w_i is
                                               77E05A0E 7DC78AB5
        D8934D5E 93E82C06 A07C04CE E6C9C530 45EEB485 872777CF


    W is
                                               77E05A0E 7DC78AB5
        D8934D5E 93E82C06 A07C04CE E6C9C530 45EEB485 872777CF


    ------------

    i = 2

    data is
                                                AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E2


    w_i is
                                               3B3E35C4 74F976B8
        94BF301A 86FA651F 463970E8 9D4A0534 B2ECAD29 EC044E7E


    W is
                           77E05A0E 7DC78AB5 D8934D5E 93E82C06
        A07C04CE E6C9C530 45EEB485 872777CF 3B3E35C4 74F976B8
        94BF301A 86FA651F 463970E8 9D4A0534 B2ECAD29 EC044E7E
```

```
  returned_bits is
                          77E05A0E 7DC78AB5 D8934D5E 93E82C06
        A07C04CE E6C9C530 45EEB485 872777CF 3B3E35C4 74F976B8
        94BF301A 86FA651F 463970E8 9D4A0534 B2ECAD29 EC044E7E


---------------------------

  Update V

    0x03||V is
                                               03AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    H is
                                               FC0D84A6 B4556DFF
        3915BE7E 63044692 5ABC4032 81175379 3AFAD856 3240C4EC


  Updated values

  V is
                                                 8C9FB2 8D1B5CCC
        A47E7CFA 66BACE21 FF260A16 A5BABA7F 144E7579 368E9955
        BEFBE700 EEF87277 6B17AEFF D53D76F4 E3BE65E8 C94B708F


  reseed_counter is
                                                    0000 00000002


rnd_val is
                          77E05A0E 7DC78AB5 D8934D5E 93E82C06
        A07C04CE E6C9C530 45EEB485 872777CF 3B3E35C4 74F976B8
        94BF301A 86FA651F 463970E8 9D4A0534 B2ECAD29 EC044E7E


-------------------------------------------------------------

Second call to Generate

*************************************************************
```

```
Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1

    data is
                                                8C9FB2 8D1B5CCC
        A47E7CFA 66BACE21 FF260A16 A5BABA7F 144E7579 368E9955
        BEFBE700 EEF87277 6B17AEFF D53D76F4 E3BE65E8 C94B708F


    w_i is
                                               5FF4BA49 3C40CFFF
        3B01E472 C575668C CE3880B9 290B05BF EDE5EC96 ED5E9B28


    W is
                                               5FF4BA49 3C40CFFF
        3B01E472 C575668C CE3880B9 290B05BF EDE5EC96 ED5E9B28


    ------------

    i = 2

    data is
                                                8C9FB2 8D1B5CCC
        A47E7CFA 66BACE21 FF260A16 A5BABA7F 144E7579 368E9955
        BEFBE700 EEF87277 6B17AEFF D53D76F4 E3BE65E8 C94B7090


    w_i is
                                               98508B09 BC800EEE
        099A3C90 602ABD4B 1D4F343D 497C6055 C87BB956 D53BF351
```

```
    W is
                          5FF4BA49 3C40CFFF 3B01E472 C575668C
        CE3880B9 290B05BF EDE5EC96 ED5E9B28 98508B09 BC800EEE
        099A3C90 602ABD4B 1D4F343D 497C6055 C87BB956 D53BF351


  returned_bits is
                          5FF4BA49 3C40CFFF 3B01E472 C575668C
        CE3880B9 290B05BF EDE5EC96 ED5E9B28 98508B09 BC800EEE
        099A3C90 602ABD4B 1D4F343D 497C6055 C87BB956 D53BF351


---------------------------

  Update V

    0x03||V is
                                               038C9FB2 8D1B5CCC
        A47E7CFA 66BACE21 FF260A16 A5BABA7F 144E7579 368E9955
        BEFBE700 EEF87277 6B17AEFF D53D76F4 E3BE65E8 C94B708F


    H is
                                               15D2C146 0EDF2565
        20C61E8A E5EEBBC5 6D12F9B0 FBF299BF B232B53F 0A43EC3F


  Updated values

  V is
                                                 6DFD97 35FF0E0E
        3FE0522F 58188B53 ED3FF670 05465290 44B62BE1 7D1B1C21
        D091B089 B1774795 DB1422A8 6C954634 8076B4B6 21C72F91


  reseed_counter is
                                                   0000 00000003


rnd_val is
                          5FF4BA49 3C40CFFF 3B01E472 C575668C
        CE3880B9 290B05BF EDE5EC96 ED5E9B28 98508B09 BC800EEE
        099A3C90 602ABD4B 1D4F343D 497C6055 C87BB956 D53BF351
```

```
################################################################

Hash_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
```

```
################################################################

****************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                               20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                 01000001 B8000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    Hash(counter||no_of_bits_to_return||input_string) is
                                               AB41CDE4 37AB8B09
        1CA7C575 5D10F011 0C1DBD46 2F226CFD ABFBB04A 8BCDEF95
```

```
    temp =
                                                AB41CDE4 37AB8B09
        1CA7C575 5D10F011 0C1DBD46 2F226CFD ABFBB04A 8BCDEF95


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                 02000001 B8000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    Hash(counter||no_of_bits_to_return||input_string) is
                                                167D84AF 64128C0D
        71F4D5B8 C0EDFBBE 3DF40448 D2D8E12F A91BA8B0 97969506


    temp =
                                                  AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


  V is
                                                  AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                                00AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    no_of_bits_to_return = 440

    ------------
```

```
  i = 1

  counter||no_of_bits_to_return||input_string is
                              01 000001B8 00AB41CD E437AB8B
      091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
      95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


  Hash(counter||no_of_bits_to_return||input_string) is
                                          E15DE4A8 E3B1419B
      61D534F1 5DBD31EE 19EC595F 8B98111A 94F52237 AD5D66F0


  temp =
                                          E15DE4A8 E3B1419B
      61D534F1 5DBD31EE 19EC595F 8B98111A 94F52237 AD5D66F0


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                              02 000001B8 00AB41CD E437AB8B
      091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
      95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


  Hash(counter||no_of_bits_to_return||input_string) is
                                          CFAAFDDC 90195902
      E979F79B 65357FEA 85998E4E 37D2C1D4 FD0F0D66 3A829565


  temp =
                                            E15DE4 A8E3B141
      9B61D534 F15DBD31 EE19EC59 5F8B9811 1A94F522 37AD5D66
      F0CFAAFD DC901959 02E979F7 9B65357F EA85998E 4E37D2C1


C is
                                            E15DE4 A8E3B141
      9B61D534 F15DBD31 EE19EC59 5F8B9811 1A94F522 37AD5D66
      F0CFAAFD DC901959 02E979F7 9B65357F EA85998E 4E37D2C1
```

```
-------------------------------------------------------------

First call to Generate

*************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


---------------------------

  Process additional_input

    0x02||V||additional_input is
                           02AB41 CDE437AB 8B091CA7 C5755D10
        F0110C1D BD462F22 6CFDABFB B04A8BCD EF95167D 84AF6412
        8C0D71F4 D5B8C0ED FBBE3DF4 0448D2D8 E1606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    w=Hash(0x02||V||additional_input) is
                                               5A0FEBC5 0A3DBB70
        91C99849 CCF32413 F39B9382 05D3ECF0 F67DBFF3 49CE00B9


    V is
                                                 AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226D 57BBE775 54C98960
        26E015CE 7C5736A0 010D8857 BE94DAEC B4BBB3F7 92A0D99A


---------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------
```

```
  i = 1

  data is
                                                AB41CD E437AB8B
      091CA7C5 755D10F0 110C1DBD 462F226D 57BBE775 54C98960
      26E015CE 7C5736A0 010D8857 BE94DAEC B4BBB3F7 92A0D99A


  w_i is
                                              510724B9 3AE9A182
      70E48473 711D8824 631BAA7F 1D9AC928 4E7EC8F3 637F7A74


  W is
                                              510724B9 3AE9A182
      70E48473 711D8824 631BAA7F 1D9AC928 4E7EC8F3 637F7A74


  ------------

  i = 2

  data is
                                                AB41CD E437AB8B
      091CA7C5 755D10F0 110C1DBD 462F226D 57BBE775 54C98960
      26E015CE 7C5736A0 010D8857 BE94DAEC B4BBB3F7 92A0D99B


  w_i is
                                              3B3644EB 96C98627
      C8FD405A 7A4603F3 8CFF7C89 E9C133F5 851F40E9 2030FEA2


  W is
                        510724B9 3AE9A182 70E48473 711D8824
      631BAA7F 1D9AC928 4E7EC8F3 637F7A74 3B3644EB 96C98627
      C8FD405A 7A4603F3 8CFF7C89 E9C133F5 851F40E9 2030FEA2


returned_bits is
                        510724B9 3AE9A182 70E48473 711D8824
      631BAA7F 1D9AC928 4E7EC8F3 637F7A74 3B3644EB 96C98627
      C8FD405A 7A4603F3 8CFF7C89 E9C133F5 851F40E9 2030FEA2
```

```
--------------------------

  Update V

    0x03||V is
                                                03AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226D 57BBE775 54C98960
        26E015CE 7C5736A0 010D8857 BE94DAEC B4BBB3F7 92A0D99A


    H is
                                                AD825E98 ED18CBD2
        F80AA598 A9962F17 547ABD64 E6E5AE71 E28EFF9C FF1EDD85


  Updated values

  V is
                                                  8C9FB2 8D1B5CCC
        A47E7CFA 66BACE21 FF260A16 A5BABA7F 1FD33B30 798FB29A
        0FBA6665 027D7F10 5871BFB4 40DFBEDE 81D04D22 DFF789E1


  reseed_counter is
                                                    0000 00000002


rnd_val is
                          510724B9 3AE9A182 70E48473 711D8824
        631BAA7F 1D9AC928 4E7EC8F3 637F7A74 3B3644EB 96C98627
        C8FD405A 7A4603F3 8CFF7C89 E9C133F5 851F40E9 2030FEA2


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
```

```
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Process additional_input

    0x02||V||additional_input is
                           028C9F B28D1B5C CCA47E7C FA66BACE
        21FF260A 16A5BABA 7F1FD33B 30798FB2 9A0FBA66 65027D7F
        105871BF B440DFBE DE81D04D 22DFF789 E1A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    w=Hash(0x02||V||additional_input) is
                                              2E5668C1 70F5B45B
        F61C9814 6C3D84D7 B3A218D1 4FA4D6F7 6BE092AC E9905ADD


    V is
                                                8C9FB2 8D1B5CCC
        A47E7CFA 66BACE21 FF260A16 A5BABA7F 4E29A3F1 EA8566F6
        05D6FE79 6EBB03E8 0C13D885 908495D5 EDB0DFCF C987E4BE


---------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1

    data is
                                                8C9FB2 8D1B5CCC
        A47E7CFA 66BACE21 FF260A16 A5BABA7F 4E29A3F1 EA8566F6
        05D6FE79 6EBB03E8 0C13D885 908495D5 EDB0DFCF C987E4BE


    w_i is
                                              6253DA3A AE8B88A3
        B746E4C8 B2635C54 0F6E9EA7 157EE69D D71EFB2E 8FF7BBE1
```

```
    W is
                                              6253DA3A AE8B88A3
        B746E4C8 B2635C54 0F6E9EA7 157EE69D D71EFB2E 8FF7BBE1


    ------------

    i = 2

    data is
                                                8C9FB2 8D1B5CCC
        A47E7CFA 66BACE21 FF260A16 A5BABA7F 4E29A3F1 EA8566F6
        05D6FE79 6EBB03E8 0C13D885 908495D5 EDB0DFCF C987E4BF


    w_i is
                                              E3336888 38DD7DE4
        9CC88990 309C96CD B2AB9295 7436BF83 D1BD8308 19C748CA


    W is
                           6253DA3A AE8B88A3 B746E4C8 B2635C54
        0F6E9EA7 157EE69D D71EFB2E 8FF7BBE1 E3336888 38DD7DE4
        9CC88990 309C96CD B2AB9295 7436BF83 D1BD8308 19C748CA


  returned_bits is
                           6253DA3A AE8B88A3 B746E4C8 B2635C54
        0F6E9EA7 157EE69D D71EFB2E 8FF7BBE1 E3336888 38DD7DE4
        9CC88990 309C96CD B2AB9295 7436BF83 D1BD8308 19C748CA


--------------------------

  Update V

    0x03||V is
                                              038C9FB2 8D1B5CCC
        A47E7CFA 66BACE21 FF260A16 A5BABA7F 4E29A3F1 EA8566F6
        05D6FE79 6EBB03E8 0C13D885 908495D5 EDB0DFCF C987E4BE


    H is
                                              78BDC1C4 0B7665A8
        0B03BCC3 5B54885F A183D8CE 23C628A8 F6435398 931F0A4F
```

```
  Updated values

  V is
                                                 6DFD97 35FF0E0E
        3FE0522F 58188B53 ED3FF670 05465290 E17C5AD8 2DA92A05
        01AA663A A69FA5A0 B0812B4B 4FAFF3FE CE79CCF6 AADEC1D0


  reseed_counter is
                                                   0000 00000003


rnd_val is
                          6253DA3A AE8B88A3 B746E4C8 B2635C54
        0F6E9EA7 157EE69D D71EFB2E 8FF7BBE1 E3336888 38DD7DE4
        9CC88990 309C96CD B2AB9295 7436BF83 D1BD8308 19C748CA


################################################################

Hash_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                 C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
```

```
    Nonce =
                                                20212223 24252627


    PersonalizationString =
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

###############################################################

***************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                20212223 24252627


    personal_str is
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
```

```
    5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                                        010000
    01B80001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36202122 23242526 27404142 43444546
    4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
    5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


Hash(counter||no_of_bits_to_return||input_string) is
                                        A3E94E39 26FDA169
    C303D664 383905E0 D79962D1 65446D63 BDA654D1 32F72DB4


temp =
                                        A3E94E39 26FDA169
    C303D664 383905E0 D79962D1 65446D63 BDA654D1 32F72DB4


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                        020000
    01B80001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36202122 23242526 27404142 43444546
    4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
    5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


Hash(counter||no_of_bits_to_return||input_string) is
                                        71564B45 6FF2EEC8
    36422ACC 5A029935 A7992990 94A1CA74 1B916DC0 26A7E107
```

```
    temp =
                                                A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


  V is
                                                A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              00A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 00A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


    Hash(counter||no_of_bits_to_return||input_string) is
                                              44748A78 B16E7555
        9F881D51 C15DFE6C 52CFB0BB 71620169 C7933427 67E7F887


    temp =
                                              44748A78 B16E7555
        9F881D51 C15DFE6C 52CFB0BB 71620169 C7933427 67E7F887


    ------------
```

```
    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


    Hash(counter||no_of_bits_to_return||input_string) is
                                              5F42CB6A 20C89D7C
        6EF3DC61 0D8FF203 D6766CED 1919D094 ED485EF7 FADDB668


    temp =
                                               44748A 78B16E75
        559F881D 51C15DFE 6C52CFB0 BB716201 69C79334 2767E7F8
        875F42CB 6A20C89D 7C6EF3DC 610D8FF2 03D6766C ED1919D0


  C is
                                               44748A 78B16E75
        559F881D 51C15DFE 6C52CFB0 BB716201 69C79334 2767E7F8
        875F42CB 6A20C89D 7C6EF3DC 610D8FF2 03D6766C ED1919D0


-------------------------------------------------------------

First call to Generate

*************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1
```

```
    data is
                                                A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


    w_i is
                                               4A62664F 266EE537
        B90D64B0 5E1D813D 28B159A9 79F1509D DE31B71D A43D546E


    W is
                                               4A62664F 266EE537
        B90D64B0 5E1D813D 28B159A9 79F1509D DE31B71D A43D546E


    ------------

    i = 2

    data is
                                                A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CB


    w_i is
                                               E8E78678 202DC237
        AD4AFE7D F310C9A4 13E38AAF 417D2D22 5AA365EC 4A7D2996


    W is
                          4A62664F 266EE537 B90D64B0 5E1D813D
        28B159A9 79F1509D DE31B71D A43D546E E8E78678 202DC237
        AD4AFE7D F310C9A4 13E38AAF 417D2D22 5AA365EC 4A7D2996


  returned_bits is
                          4A62664F 266EE537 B90D64B0 5E1D813D
        28B159A9 79F1509D DE31B71D A43D546E E8E78678 202DC237
        AD4AFE7D F310C9A4 13E38AAF 417D2D22 5AA365EC 4A7D2996


---------------------------
```

```
  Update V

    0x03||V is
                                                03A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


    H is
                                                19B1A221 4356F101
        FFA0E21C BF22F2CF 985EE127 7506C7BD BA35EC15 7A81BADE


  Updated values

  V is
                                                  E85DD8 B1D86C16
        BF628BF3 B5F99704 4D2A6913 8CD6A66E E736DBAA 3BF1D028
        3B717B33 6EB3AE5B DD04172E A26E5A48 F3B3FBAB F82F7679


  reseed_counter is
                                                    0000 00000002


rnd_val is
                          4A62664F 266EE537 B90D64B0 5E1D813D
        28B159A9 79F1509D DE31B71D A43D546E E8E78678 202DC237
        AD4AFE7D F310C9A4 13E38AAF 417D2D22 5AA365EC 4A7D2996


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

---------------------------

  Hashgen
```

```
  requested_no_of_bits  = 512

  ------------

  i = 1

  data is
                                                E85DD8 B1D86C16
      BF628BF3 B5F99704 4D2A6913 8CD6A66E E736DBAA 3BF1D028
      3B717B33 6EB3AE5B DD04172E A26E5A48 F3B3FBAB F82F7679


  w_i is
                                              59583D3C 0AC37130
      C4789A83 11B8CA8F 985EF1E8 F94D954E 32E344A6 21C24B2F


  W is
                                              59583D3C 0AC37130
      C4789A83 11B8CA8F 985EF1E8 F94D954E 32E344A6 21C24B2F


  ------------

  i = 2

  data is
                                                E85DD8 B1D86C16
      BF628BF3 B5F99704 4D2A6913 8CD6A66E E736DBAA 3BF1D028
      3B717B33 6EB3AE5B DD04172E A26E5A48 F3B3FBAB F82F767A


  w_i is
                                              371DA9BA 3C33153F
      09E55145 E762926B 73AC147A 1E8631D1 CCD08567 CF677C72


  W is
                        59583D3C 0AC37130 C4789A83 11B8CA8F
      985EF1E8 F94D954E 32E344A6 21C24B2F 371DA9BA 3C33153F
      09E55145 E762926B 73AC147A 1E8631D1 CCD08567 CF677C72


returned_bits is
                        59583D3C 0AC37130 C4789A83 11B8CA8F
```

```
        985EF1E8 F94D954E 32E344A6 21C24B2F 371DA9BA 3C33153F
        09E55145 E762926B 73AC147A 1E8631D1 CCD08567 CF677C72


---------------------------

  Update V

    0x03||V is
                                              03E85DD8 B1D86C16
        BF628BF3 B5F99704 4D2A6913 8CD6A66E E736DBAA 3BF1D028
        3B717B33 6EB3AE5B DD04172E A26E5A48 F3B3FBAB F82F7679


    H is
                                              B9688961 AE7D4A6C
        5202575B 9AA536DB E355DF79 CD8079E3 04D82BED 33D6CF22


  Updated values

  V is
                                                2CD263 2A89DA8C
        15021411 07BAF502 B97D38C4 48480871 0A66F840 11D7028D
        14D3155A 7379ADD5 3CC8EA84 D0FC641D FC629E06 191F5F6D


  reseed_counter is
                                                  0000 00000003


rnd_val is
                         59583D3C 0AC37130 C4789A83 11B8CA8F
        985EF1E8 F94D954E 32E344A6 21C24B2F 371DA9BA 3C33153F
        09E55145 E762926B 73AC147A 1E8631D1 CCD08567 CF677C72


##############################################################

Hash_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
```

```
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                20212223 24252627


    PersonalizationString =
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

Hash_DRBG_Instantiate_algorithm
```

```
    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                              20212223 24252627


    personal_str is
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                          010000
        01B80001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
                                                A3E94E39 26FDA169
        C303D664 383905E0 D79962D1 65446D63 BDA654D1 32F72DB4


    temp =
                                                A3E94E39 26FDA169
        C303D664 383905E0 D79962D1 65446D63 BDA654D1 32F72DB4


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                              020000
        01B80001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                                                71564B45 6FF2EEC8
        36422ACC 5A029935 A7992990 94A1CA74 1B916DC0 26A7E107


    temp =
                                                  A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


  V is
                                                  A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                                00A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
```

```
    B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                            01 000001B8 00A3E94E 3926FDA1
    69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
    B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


Hash(counter||no_of_bits_to_return||input_string) is
                                        44748A78 B16E7555
    9F881D51 C15DFE6C 52CFB0BB 71620169 C7933427 67E7F887


temp =
                                        44748A78 B16E7555
    9F881D51 C15DFE6C 52CFB0BB 71620169 C7933427 67E7F887


------------

i = 2

counter||no_of_bits_to_return||input_string is
                            02 000001B8 00A3E94E 3926FDA1
    69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
    B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


Hash(counter||no_of_bits_to_return||input_string) is
                                        5F42CB6A 20C89D7C
    6EF3DC61 0D8FF203 D6766CED 1919D094 ED485EF7 FADDB668


temp =
                                          44748A 78B16E75
    559F881D 51C15DFE 6C52CFB0 BB716201 69C79334 2767E7F8
    875F42CB 6A20C89D 7C6EF3DC 610D8FF2 03D6766C ED1919D0
```

```
  C is
                                                  44748A 78B16E75
        559F881D 51C15DFE 6C52CFB0 BB716201 69C79334 2767E7F8
        875F42CB 6A20C89D 7C6EF3DC 610D8FF2 03D6766C ED1919D0


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


---------------------------

  Process additional_input

    0x02||V||additional_input is
                           02A3E9 4E3926FD A169C303 D6643839
        05E0D799 62D16544 6D63BDA6 54D132F7 2DB47156 4B456FF2
        EEC83642 2ACC5A02 9935A799 299094A1 CA606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    w=Hash(0x02||V||additional_input) is
                                                 3CBE9AC4 CEFC9E53
        84B05F3A 13305C81 BB347128 578D087A D9CD6168 A7BBD90A


    V is
                                                  A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D A07C4119 A02F9581
        3921B585 58A04F70 836AB353 23E70B14 0F74FA92 38507AD4


---------------------------
```

Hashgen

requested_no_of_bits = 512

---

i = 1

data is

                                          A3E94E 3926FDA1
    69C303D6 64383905 E0D79962 D165446D A07C4119 A02F9581
    3921B585 58A04F70 836AB353 23E70B14 0F74FA92 38507AD4

w_i is

                                         E0B97C82 1268FD3B
    B2CABFD1 F9548478 AE8A6041 7F7B094A 26139546 062B521C

W is

                                         E0B97C82 1268FD3B
    B2CABFD1 F9548478 AE8A6041 7F7B094A 26139546 062B521C

---

i = 2

data is

                                          A3E94E 3926FDA1
    69C303D6 64383905 E0D79962 D165446D A07C4119 A02F9581
    3921B585 58A04F70 836AB353 23E70B14 0F74FA92 38507AD5

w_i is

                                         FD33E4E3 9B9DCD0A
    3DA15209 C72ADBE5 8C20AB34 07026951 297AD254 307553A5

W is

                        E0B97C82 1268FD3B B2CABFD1 F9548478
    AE8A6041 7F7B094A 26139546 062B521C FD33E4E3 9B9DCD0A
    3DA15209 C72ADBE5 8C20AB34 07026951 297AD254 307553A5

```
  returned_bits is
                           E0B97C82 1268FD3B B2CABFD1 F9548478
        AE8A6041 7F7B094A 26139546 062B521C FD33E4E3 9B9DCD0A
        3DA15209 C72ADBE5 8C20AB34 07026951 297AD254 307553A5


--------------------------

  Update V

    0x03||V is
                                             03A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D A07C4119 A02F9581
        3921B585 58A04F70 836AB353 23E70B14 0F74FA92 38507AD4


    H is
                                             8264A739 7BB8A2B4
        5D09B864 EA8694B4 75668170 5EB44819 680AE7DE AC2CFFE4


  Updated values

  V is
                                               E85DD8 B1D86C16
        BF628BF3 B5F99704 4D2A6913 8CD6A66F 8CA87B87 4350202E
        1D8AB0B5 AD47ACC2 7540289F E3A8E31F 7B5658DD D1969489


  reseed_counter is
                                                 0000 00000002


rnd_val is
                           E0B97C82 1268FD3B B2CABFD1 F9548478
        AE8A6041 7F7B094A 26139546 062B521C FD33E4E3 9B9DCD0A
        3DA15209 C72ADBE5 8C20AB34 07026951 297AD254 307553A5


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm
```

```
  requested_number_of_bits = 512

  additional_input
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Process additional_input

    0x02||V||additional_input is
                           02E85D D8B1D86C 16BF628B F3B5F997
        044D2A69 138CD6A6 6F8CA87B 87435020 2E1D8AB0 B5AD47AC
        C2754028 9FE3A8E3 1F7B5658 DDD19694 89A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    w=Hash(0x02||V||additional_input) is
                                               A2701C07 02B8A337
        615E949D 0B86D42B 002EF072 58584377 ECBF1094 62AFC8AC


    V is
                                                 E85DD8 B1D86C16
        BF628BF3 B5F99704 4D2A6913 8CD6A670 2F18978E 4608C365
        7EE94552 B8CE80ED 756F1912 3C012697 68156972 34465D35


---------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1

    data is
                                                 E85DD8 B1D86C16
        BF628BF3 B5F99704 4D2A6913 8CD6A670 2F18978E 4608C365
        7EE94552 B8CE80ED 756F1912 3C012697 68156972 34465D35
```

```
    w_i is
                                                C1ACD3AD A4C8C495
        BF179DB5 9822C351 BC479ABE 4EB28F84 3957B11E 3C2BC048


    W is
                                                C1ACD3AD A4C8C495
        BF179DB5 9822C351 BC479ABE 4EB28F84 3957B11E 3C2BC048


    ------------

    i = 2

    data is
                                                  E85DD8 B1D86C16
        BF628BF3 B5F99704 4D2A6913 8CD6A670 2F18978E 4608C365
        7EE94552 B8CE80ED 756F1912 3C012697 68156972 34465D36


    w_i is
                                                83964297 975BD72D
        1024ABCF 6F6615D7 F5B4FD1E 40A64EEB 45BA2181 B83937ED


    W is
                            C1ACD3AD A4C8C495 BF179DB5 9822C351
        BC479ABE 4EB28F84 3957B11E 3C2BC048 83964297 975BD72D
        1024ABCF 6F6615D7 F5B4FD1E 40A64EEB 45BA2181 B83937ED


  returned_bits is
                            C1ACD3AD A4C8C495 BF179DB5 9822C351
        BC479ABE 4EB28F84 3957B11E 3C2BC048 83964297 975BD72D
        1024ABCF 6F6615D7 F5B4FD1E 40A64EEB 45BA2181 B83937ED


--------------------------

  Update V

    0x03||V is
                                                03E85DD8 B1D86C16
        BF628BF3 B5F99704 4D2A6913 8CD6A670 2F18978E 4608C365
```

```
        7EE94552 B8CE80ED 756F1912 3C012697 68156972 34465D35


    H is
                                                19978405 921CF6DE
        6BA76D7F 9F5F14C1 8D7A3AC2 2420B3D0 327F4EFB 9ED0F4C6


  Updated values

  V is
                                                  2CD263 2A89DA8C
        15021411 07BAF502 B97D38C4 48480871 B277AEC7 FF8DA23C
        71EFF59D C24E5E4C 7F5847B0 C12F6A59 9E6B2EDA C0306BCD


  reseed_counter is
                                                    0000 00000003


rnd_val is
                         C1ACD3AD A4C8C495 BF179DB5 9822C351
        BC479ABE 4EB28F84 3957B11E 3C2BC048 83964297 975BD72D
        1024ABCF 6F6615D7 F5B4FD1E 40A64EEB 45BA2181 B83937ED


##############################################################

Hash_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

```
    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                               20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                               20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    no_of_bits_to_return = 440
```

```
  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
              01000001 B8000102 03040506 0708090A 0B0C0D0E
      0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
      2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


  Hash(counter||no_of_bits_to_return||input_string) is
                                           AB41CDE4 37AB8B09
      1CA7C575 5D10F011 0C1DBD46 2F226CFD ABFBB04A 8BCDEF95


  temp =
                                           AB41CDE4 37AB8B09
      1CA7C575 5D10F011 0C1DBD46 2F226CFD ABFBB04A 8BCDEF95


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
              02000001 B8000102 03040506 0708090A 0B0C0D0E
      0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
      2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


  Hash(counter||no_of_bits_to_return||input_string) is
                                           167D84AF 64128C0D
      71F4D5B8 C0EDFBBE 3DF40448 D2D8E12F A91BA8B0 97969506


  temp =
                                             AB41CD E437AB8B
      091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
      95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


V is
                                             AB41CD E437AB8B
      091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
      95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1
```

```
---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              00AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 00AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    Hash(counter||no_of_bits_to_return||input_string) is
                                              E15DE4A8 E3B1419B
        61D534F1 5DBD31EE 19EC595F 8B98111A 94F52237 AD5D66F0


    temp =
                                              E15DE4A8 E3B1419B
        61D534F1 5DBD31EE 19EC595F 8B98111A 94F52237 AD5D66F0


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    Hash(counter||no_of_bits_to_return||input_string) is
                                              CFAAFDDC 90195902
```

```
        E979F79B 65357FEA 85998E4E 37D2C1D4 FD0F0D66 3A829565


    temp =
                                                E15DE4 A8E3B141
        9B61D534 F15DBD31 EE19EC59 5F8B9811 1A94F522 37AD5D66
        F0CFAAFD DC901959 02E979F7 9B65357F EA85998E 4E37D2C1


  C is
                                                E15DE4 A8E3B141
        9B61D534 F15DBD31 EE19EC59 5F8B9811 1A94F522 37AD5D66
        F0CFAAFD DC901959 02E979F7 9B65357F EA85998E 4E37D2C1


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                             01AB41 CDE437AB 8B091CA7 C5755D10
```

```
    F0110C1D BD462F22 6CFDABFB B04A8BCD EF95167D 84AF6412
    8C0D71F4 D5B8C0ED FBBE3DF4 0448D2D8 E1808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
             01000001 B801AB41 CDE437AB 8B091CA7 C5755D10
    F0110C1D BD462F22 6CFDABFB B04A8BCD EF95167D 84AF6412
    8C0D71F4 D5B8C0ED FBBE3DF4 0448D2D8 E1808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


Hash(counter||no_of_bits_to_return||input_string) is
                                        3C40E8DC 7172FDA2
    32550A1D 8E1447C1 1F474888 F96CD85C 3863D5E4 84266756


temp =
                                        3C40E8DC 7172FDA2
    32550A1D 8E1447C1 1F474888 F96CD85C 3863D5E4 84266756


------------

i = 2

counter||no_of_bits_to_return||input_string is
             02000001 B801AB41 CDE437AB 8B091CA7 C5755D10
    F0110C1D BD462F22 6CFDABFB B04A8BCD EF95167D 84AF6412
    8C0D71F4 D5B8C0ED FBBE3DF4 0448D2D8 E1808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


Hash(counter||no_of_bits_to_return||input_string) is
                                        28D08885 347C3EFD
    6292FDDC D1A1421E ED51B713 AB090FC9 AFC95C22 731A6AF6
```

```
    temp =
                                                3C40E8 DC7172FD
        A232550A 1D8E1447 C11F4748 88F96CD8 5C3863D5 E4842667
        5628D088 85347C3E FD6292FD DCD1A142 1EED51B7 13AB090F


  V is
                                                3C40E8 DC7172FD
        A232550A 1D8E1447 C11F4748 88F96CD8 5C3863D5 E4842667
        5628D088 85347C3E FD6292FD DCD1A142 1EED51B7 13AB090F


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                               003C40E8 DC7172FD
        A232550A 1D8E1447 C11F4748 88F96CD8 5C3863D5 E4842667
        5628D088 85347C3E FD6292FD DCD1A142 1EED51B7 13AB090F


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 003C40E8 DC7172FD
        A232550A 1D8E1447 C11F4748 88F96CD8 5C3863D5 E4842667
        5628D088 85347C3E FD6292FD DCD1A142 1EED51B7 13AB090F


    Hash(counter||no_of_bits_to_return||input_string) is
                                               E7568384 F264E4A7
        E7AE850D 9D501FD6 3183564F D7D39044 6F5BE5F6 7B50195B


    temp =
                                               E7568384 F264E4A7
        E7AE850D 9D501FD6 3183564F D7D39044 6F5BE5F6 7B50195B


    ------------
```

```
    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 003C40E8 DC7172FD
        A232550A 1D8E1447 C11F4748 88F96CD8 5C3863D5 E4842667
        5628D088 85347C3E FD6292FD DCD1A142 1EED51B7 13AB090F


    Hash(counter||no_of_bits_to_return||input_string) is
                                              5284692A D4B76DFD
        4F524BCF CCAB62C1 309F2515 17DFFD1F 5C4A6B96 ADC6B9D9


    temp =
                                                E75683 84F264E4
        A7E7AE85 0D9D501F D6318356 4FD7D390 446F5BE5 F67B5019
        5B528469 2AD4B76D FD4F524B CFCCAB62 C1309F25 1517DFFD


  C is
                                                E75683 84F264E4
        A7E7AE85 0D9D501F D6318356 4FD7D390 446F5BE5 F67B5019
        5B528469 2AD4B76D FD4F524B CFCCAB62 C1309F25 1517DFFD


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1

    data is
                                                3C40E8 DC7172FD
```

```
        A232550A 1D8E1447 C11F4748 88F96CD8 5C3863D5 E4842667
        5628D088 85347C3E FD6292FD DCD1A142 1EED51B7 13AB090F


    w_i is
                                              92275523 C70E567B
        CF9B35EC 50B933F8 12616DF5 86B7F72E E1BC7735 A5C26543


    W is
                                              92275523 C70E567B
        CF9B35EC 50B933F8 12616DF5 86B7F72E E1BC7735 A5C26543


    ------------

    i = 2

    data is
                                                3C40E8 DC7172FD
        A232550A 1D8E1447 C11F4748 88F96CD8 5C3863D5 E4842667
        5628D088 85347C3E FD6292FD DCD1A142 1EED51B7 13AB0910


    w_i is
                                              73CBBC72 316DFF84
        20A33BF0 2B97AC8D 1952583F 270ACD70 05CC027F 4CF1187E


    W is
                           92275523 C70E567B CF9B35EC 50B933F8
        12616DF5 86B7F72E E1BC7735 A5C26543 73CBBC72 316DFF84
        20A33BF0 2B97AC8D 1952583F 270ACD70 05CC027F 4CF1187E


  returned_bits is
                           92275523 C70E567B CF9B35EC 50B933F8
        12616DF5 86B7F72E E1BC7735 A5C26543 73CBBC72 316DFF84
        20A33BF0 2B97AC8D 1952583F 270ACD70 05CC027F 4CF1187E


---------------------------

  Update V

    0x03||V is
```

```
                                                033C40E8 DC7172FD
        A232550A 1D8E1447 C11F4748 88F96CD8 5C3863D5 E4842667
        5628D088 85347C3E FD6292FD DCD1A142 1EED51B7 13AB090F


    H is
                                                ECBC627D A003201D
        BD527DAB FCBC42D1 3210EB57 AA2A2E2B D3399828 DF1D4E6A


  Updated values

  V is
                                                  23976C 6163D7E2
        4A1A038F 2B2B6467 9750CA9E D8D14069 8D642239 7B02969E
        6ECDD29D ACC5767E 2CC2D0A1 56C87AD0 B3578905 07E03777


  reseed_counter is
                                                    0000 00000002


rnd_val is
                          92275523 C70E567B CF9B35EC 50B933F8
        12616DF5 86B7F72E E1BC7735 A5C26543 73CBBC72 316DFF84
        20A33BF0 2B97AC8D 1952583F 270ACD70 05CC027F 4CF1187E


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

Generate FAILED: Reseed is required
---------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
```

```
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                           012397 6C6163D7 E24A1A03 8F2B2B64
        679750CA 9ED8D140 698D6422 397B0296 9E6ECDD2 9DACC576
        7E2CC2D0 A156C87A D0B35789 0507E037 77C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                 01000001 B8012397 6C6163D7 E24A1A03 8F2B2B64
        679750CA 9ED8D140 698D6422 397B0296 9E6ECDD2 9DACC576
        7E2CC2D0 A156C87A D0B35789 0507E037 77C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                                               E983B166 A92A997E
        ABCC966C 6AA3D3B3 A1681FC5 8F582940 3B48601E C1775494


    temp =
                                               E983B166 A92A997E
        ABCC966C 6AA3D3B3 A1681FC5 8F582940 3B48601E C1775494


    ------------

    i = 2
```

```
    counter||no_of_bits_to_return||input_string is
                02000001 B8012397 6C6163D7 E24A1A03 8F2B2B64
        679750CA 9ED8D140 698D6422 397B0296 9E6ECDD2 9DACC576
        7E2CC2D0 A156C87A D0B35789 0507E037 77C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                                            2E11C1CD 465B7DBE
        2A78CA04 2CF9B305 71FF12E3 B9F6C945 C634B91C 1BAC2021


    temp =
                                              E983B1 66A92A99
        7EABCC96 6C6AA3D3 B3A1681F C58F5829 403B4860 1EC17754
        942E11C1 CD465B7D BE2A78CA 042CF9B3 0571FF12 E3B9F6C9


  V is
                                              E983B1 66A92A99
        7EABCC96 6C6AA3D3 B3A1681F C58F5829 403B4860 1EC17754
        942E11C1 CD465B7D BE2A78CA 042CF9B3 0571FF12 E3B9F6C9


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            00E983B1 66A92A99
        7EABCC96 6C6AA3D3 B3A1681F C58F5829 403B4860 1EC17754
        942E11C1 CD465B7D BE2A78CA 042CF9B3 0571FF12 E3B9F6C9


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 00E983B1 66A92A99
        7EABCC96 6C6AA3D3 B3A1681F C58F5829 403B4860 1EC17754
        942E11C1 CD465B7D BE2A78CA 042CF9B3 0571FF12 E3B9F6C9
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                                              A9775CE1 655BFF95
        1BE0AF5B 7959725C 767D86F1 E19B11B8 9004F697 4DBFA046


    temp =
                                              A9775CE1 655BFF95
        1BE0AF5B 7959725C 767D86F1 E19B11B8 9004F697 4DBFA046


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00E983B1 66A92A99
        7EABCC96 6C6AA3D3 B3A1681F C58F5829 403B4860 1EC17754
        942E11C1 CD465B7D BE2A78CA 042CF9B3 0571FF12 E3B9F6C9


    Hash(counter||no_of_bits_to_return||input_string) is
                                              04458E5C 528E7E1D
        FAB3887B A4AADBD6 FBDE0B31 6F1D9138 F1EB0DD9 2D80C089


    temp =
                                                A9775C E1655BFF
        951BE0AF 5B795972 5C767D86 F1E19B11 B89004F6 974DBFA0
        4604458E 5C528E7E 1DFAB388 7BA4AADB D6FBDE0B 316F1D91


  C is
                                                A9775C E1655BFF
        951BE0AF 5B795972 5C767D86 F1E19B11 B89004F6 974DBFA0
        4604458E 5C528E7E 1DFAB388 7BA4AADB D6FBDE0B 316F1D91


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>
```

```
---------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1

    data is
                                                E983B1 66A92A99
        7EABCC96 6C6AA3D3 B3A1681F C58F5829 403B4860 1EC17754
        942E11C1 CD465B7D BE2A78CA 042CF9B3 0571FF12 E3B9F6C9


    w_i is
                                               681A46B2 AA8694A0
        FE4DEEA7 20927A84 EAAA985E 59C19F8B E0984D8C BEF8C69B


    W is
                                               681A46B2 AA8694A0
        FE4DEEA7 20927A84 EAAA985E 59C19F8B E0984D8C BEF8C69B


    ------------

    i = 2

    data is
                                                E983B1 66A92A99
        7EABCC96 6C6AA3D3 B3A1681F C58F5829 403B4860 1EC17754
        942E11C1 CD465B7D BE2A78CA 042CF9B3 0571FF12 E3B9F6CA


    w_i is
                                               75416764 1946E040
        EE2043E1 CCB29DCF 063C0A50 830E428E 6DCA262E CD77C542


    W is
                           681A46B2 AA8694A0 FE4DEEA7 20927A84
        EAAA985E 59C19F8B E0984D8C BEF8C69B 75416764 1946E040
        EE2043E1 CCB29DCF 063C0A50 830E428E 6DCA262E CD77C542
```

```
  returned_bits is
                          681A46B2 AA8694A0 FE4DEEA7 20927A84
        EAAA985E 59C19F8B E0984D8C BEF8C69B 75416764 1946E040
        EE2043E1 CCB29DCF 063C0A50 830E428E 6DCA262E CD77C542


---------------------------

  Update V

    0x03||V is
                                               03E983B1 66A92A99
        7EABCC96 6C6AA3D3 B3A1681F C58F5829 403B4860 1EC17754
        942E11C1 CD465B7D BE2A78CA 042CF9B3 0571FF12 E3B9F6C9


    H is
                                               3870EB2D 3BBD1F7C
        AF12CAA5 C44D44AE D45E84EF 2789B831 45F27D6C 289E074C


  Updated values

  V is
                                                 92FB0E 480E8699
        13C7AD45 C7E3FD46 1017E5A6 B770F33B 313C3883 F1CC5671
        894521F5 EDE62EAA B083B141 A75B5CC0 22605A8A 3DC71BA7


  reseed_counter is
                                                    0000 00000002


rnd_val is
                          681A46B2 AA8694A0 FE4DEEA7 20927A84
        EAAA985E 59C19F8B E0984D8C BEF8C69B 75416764 1946E040
        EE2043E1 CCB29DCF 063C0A50 830E428E 6DCA262E CD77C542


##############################################################

Hash_DRBG

    Requested Security Strength = 128
```

```
    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                 C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                               20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                 606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

Hash_DRBG_Instantiate_algorithm
```

```
    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                              20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                 01000001 B8000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    Hash(counter||no_of_bits_to_return||input_string) is
                                              AB41CDE4 37AB8B09
        1CA7C575 5D10F011 0C1DBD46 2F226CFD ABFBB04A 8BCDEF95


    temp =
                                              AB41CDE4 37AB8B09
        1CA7C575 5D10F011 0C1DBD46 2F226CFD ABFBB04A 8BCDEF95
```

```
    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                02000001 B8000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    Hash(counter||no_of_bits_to_return||input_string) is
                                              167D84AF 64128C0D
        71F4D5B8 C0EDFBBE 3DF40448 D2D8E12F A91BA8B0 97969506


    temp =
                                                AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


  V is
                                                AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              00AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 00AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
```

```
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    Hash(counter||no_of_bits_to_return||input_string) is
                                              E15DE4A8 E3B1419B
        61D534F1 5DBD31EE 19EC595F 8B98111A 94F52237 AD5D66F0


    temp =
                                              E15DE4A8 E3B1419B
        61D534F1 5DBD31EE 19EC595F 8B98111A 94F52237 AD5D66F0


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    Hash(counter||no_of_bits_to_return||input_string) is
                                              CFAAFDDC 90195902
        E979F79B 65357FEA 85998E4E 37D2C1D4 FD0F0D66 3A829565


    temp =
                                                E15DE4 A8E3B141
        9B61D534 F15DBD31 EE19EC59 5F8B9811 1A94F522 37AD5D66
        F0CFAAFD DC901959 02E979F7 9B65357F EA85998E 4E37D2C1


  C is
                                                E15DE4 A8E3B141
        9B61D534 F15DBD31 EE19EC59 5F8B9811 1A94F522 37AD5D66
        F0CFAAFD DC901959 02E979F7 9B65357F EA85998E 4E37D2C1


----------------------------------------------------------------

First call to Generate

****************************************************************
```

```
Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01AB 41CDE437 AB8B091C A7C5755D 10F0110C 1DBD462F
        226CFDAB FBB04A8B CDEF9516 7D84AF64 128C0D71 F4D5B8C0
        EDFBBE3D F40448D2 D8E18081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    no_of_bits_to_return = 440

    ------------

    i = 1
```

```
counter||no_of_bits_to_return||input_string is
                                                          010000
    01B801AB 41CDE437 AB8B091C A7C5755D 10F0110C 1DBD462F
    226CFDAB FBB04A8B CDEF9516 7D84AF64 128C0D71 F4D5B8C0
    EDFBBE3D F40448D2 D8E18081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Hash(counter||no_of_bits_to_return||input_string) is
                                          57B2CF00 B5429746
    0B087E52 75D7DD74 23B6E3B6 5E3516D2 481199A0 17B53A22


temp =
                                          57B2CF00 B5429746
    0B087E52 75D7DD74 23B6E3B6 5E3516D2 481199A0 17B53A22


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                          020000
    01B801AB 41CDE437 AB8B091C A7C5755D 10F0110C 1DBD462F
    226CFDAB FBB04A8B CDEF9516 7D84AF64 128C0D71 F4D5B8C0
    EDFBBE3D F40448D2 D8E18081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Hash(counter||no_of_bits_to_return||input_string) is
                                          2033FE68 A60BD0BD
    704026CD 5A3E7955 DB01DCB2 8448D1B1 21D18F19 55FEA723


temp =
                                            57B2CF 00B54297
    460B087E 5275D7DD 7423B6E3 B65E3516 D2481199 A017B53A
    222033FE 68A60BD0 BD704026 CD5A3E79 55DB01DC B28448D1
```

```
  V is
                                                  57B2CF 00B54297
        460B087E 5275D7DD 7423B6E3 B65E3516 D2481199 A017B53A
        222033FE 68A60BD0 BD704026 CD5A3E79 55DB01DC B28448D1


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                                0057B2CF 00B54297
        460B087E 5275D7DD 7423B6E3 B65E3516 D2481199 A017B53A
        222033FE 68A60BD0 BD704026 CD5A3E79 55DB01DC B28448D1


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 0057B2CF 00B54297
        460B087E 5275D7DD 7423B6E3 B65E3516 D2481199 A017B53A
        222033FE 68A60BD0 BD704026 CD5A3E79 55DB01DC B28448D1


    Hash(counter||no_of_bits_to_return||input_string) is
                                                5BC1C645 CC8D3215
        82AFBB00 16992B0F 3AFE0F54 7AE7A74C 9C05A144 02FBB1D5


    temp =
                                                5BC1C645 CC8D3215
        82AFBB00 16992B0F 3AFE0F54 7AE7A74C 9C05A144 02FBB1D5


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 0057B2CF 00B54297
```

```
        460B087E 5275D7DD 7423B6E3 B65E3516 D2481199 A017B53A
        222033FE 68A60BD0 BD704026 CD5A3E79 55DB01DC B28448D1


    Hash(counter||no_of_bits_to_return||input_string) is
                                              40E6809D 8BEEF599
        ED4C3916 4740EDA0 D9C3795D E552C5DF 0AC1CAC6 AE8C0116


    temp =
                                                5BC1C6 45CC8D32
        1582AFBB 0016992B 0F3AFE0F 547AE7A7 4C9C05A1 4402FBB1
        D540E680 9D8BEEF5 99ED4C39 164740ED A0D9C379 5DE552C5


  C is
                                                5BC1C6 45CC8D32
        1582AFBB 0016992B 0F3AFE0F 547AE7A7 4C9C05A1 4402FBB1
        D540E680 9D8BEEF5 99ED4C39 164740ED A0D9C379 5DE552C5


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1

    data is
                                                57B2CF 00B54297
        460B087E 5275D7DD 7423B6E3 B65E3516 D2481199 A017B53A
        222033FE 68A60BD0 BD704026 CD5A3E79 55DB01DC B28448D1


    w_i is
```

```
                                              11601B72 CA608973
        6B204744 B29DA1AA AFBACAA5 288F06BE 484569CC EDBECE03


    W is
                                              11601B72 CA608973
        6B204744 B29DA1AA AFBACAA5 288F06BE 484569CC EDBECE03


    ------------

    i = 2

    data is
                                                57B2CF 00B54297
        460B087E 5275D7DD 7423B6E3 B65E3516 D2481199 A017B53A
        222033FE 68A60BD0 BD704026 CD5A3E79 55DB01DC B28448D2


    w_i is
                                              E822EAA5 B14F0E04
        948C05CD 3CC2E288 9A89FA03 D65D4D74 AC50FF6B D856E579


    W is
                           11601B72 CA608973 6B204744 B29DA1AA
        AFBACAA5 288F06BE 484569CC EDBECE03 E822EAA5 B14F0E04
        948C05CD 3CC2E288 9A89FA03 D65D4D74 AC50FF6B D856E579


  returned_bits is
                           11601B72 CA608973 6B204744 B29DA1AA
        AFBACAA5 288F06BE 484569CC EDBECE03 E822EAA5 B14F0E04
        948C05CD 3CC2E288 9A89FA03 D65D4D74 AC50FF6B D856E579


--------------------------

  Update V

    0x03||V is
                                              0357B2CF 00B54297
        460B087E 5275D7DD 7423B6E3 B65E3516 D2481199 A017B53A
        222033FE 68A60BD0 BD704026 CD5A3E79 55DB01DC B28448D1
```

```
    H is
                                                7FBCBE0A E8E26727
        3390B8F7 891507B0 D40B893F 491EFFE1 7D69F05C A0B8758E


  Updated values

  V is
                                                  B37495 4681CFC9
        5B8DB839 528C7108 835EB4F3 0AD91CBE 9EA0D545 CCFD1813
        2AF1D376 8F470277 2B69159F 2CC07F48 741EB5B2 B1221125


  reseed_counter is
                                                     0000 00000002


rnd_val is
                          11601B72 CA608973 6B204744 B29DA1AA
        AFBACAA5 288F06BE 484569CC EDBECE03 E822EAA5 B14F0E04
        948C05CD 3CC2E288 9A89FA03 D65D4D74 AC50FF6B D856E579


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                  C0C1C2 C3C4C5C6
```

```
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  additional_input
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01B3 74954681 CFC95B8D B839528C 7108835E B4F30AD9
        1CBE9EA0 D545CCFD 18132AF1 D3768F47 02772B69 159F2CC0
        7F48741E B5B2B122 1125C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                      010000
        01B801B3 74954681 CFC95B8D B839528C 7108835E B4F30AD9
        1CBE9EA0 D545CCFD 18132AF1 D3768F47 02772B69 159F2CC0
        7F48741E B5B2B122 1125C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    Hash(counter||no_of_bits_to_return||input_string) is
                                             5DC1C5F4 B41150CE
        E0EFC129 B837B31C 84D791FF 2E7EDAC2 9C2C50CF 8A40709B
```

```
    temp =
                                                5DC1C5F4 B41150CE
        E0EFC129 B837B31C 84D791FF 2E7EDAC2 9C2C50CF 8A40709B


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                          020000
        01B801B3 74954681 CFC95B8D B839528C 7108835E B4F30AD9
        1CBE9EA0 D545CCFD 18132AF1 D3768F47 02772B69 159F2CC0
        7F48741E B5B2B122 1125C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                98640F7B BD32BCF0
        FCB613F9 6D55D160 56BB3CA6 A774059D EC8C65C6 853BDEFE


    temp =
                                                  5DC1C5 F4B41150
        CEE0EFC1 29B837B3 1C84D791 FF2E7EDA C29C2C50 CF8A4070
        9B98640F 7BBD32BC F0FCB613 F96D55D1 6056BB3C A6A77405


  V is
                                                  5DC1C5 F4B41150
        CEE0EFC1 29B837B3 1C84D791 FF2E7EDA C29C2C50 CF8A4070
        9B98640F 7BBD32BC F0FCB613 F96D55D1 6056BB3C A6A77405


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                                005DC1C5 F4B41150
        CEE0EFC1 29B837B3 1C84D791 FF2E7EDA C29C2C50 CF8A4070
        9B98640F 7BBD32BC F0FCB613 F96D55D1 6056BB3C A6A77405
```

```
  no_of_bits_to_return = 440

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                              01 000001B8 005DC1C5 F4B41150
      CEE0EFC1 29B837B3 1C84D791 FF2E7EDA C29C2C50 CF8A4070
      9B98640F 7BBD32BC F0FCB613 F96D55D1 6056BB3C A6A77405


  Hash(counter||no_of_bits_to_return||input_string) is
                                          6222108C EDFE6D6A
      229F8C3C BF4468C8 F5172286 4CC416A4 2926D99B A6F045C1


  temp =
                                          6222108C EDFE6D6A
      229F8C3C BF4468C8 F5172286 4CC416A4 2926D99B A6F045C1


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                              02 000001B8 005DC1C5 F4B41150
      CEE0EFC1 29B837B3 1C84D791 FF2E7EDA C29C2C50 CF8A4070
      9B98640F 7BBD32BC F0FCB613 F96D55D1 6056BB3C A6A77405


  Hash(counter||no_of_bits_to_return||input_string) is
                                          F6211156 946C6E79
      3729974E B4C5A607 8F9A1D4D 1CD749DE FE72459A 097C1198


  temp =
                                            622210 8CEDFE6D
      6A229F8C 3CBF4468 C8F51722 864CC416 A42926D9 9BA6F045
      C1F62111 56946C6E 79372997 4EB4C5A6 078F9A1D 4D1CD749


C is
                                            622210 8CEDFE6D
```

```
        6A229F8C 3CBF4468 C8F51722 864CC416 A42926D9 9BA6F045
        C1F62111 56946C6E 79372997 4EB4C5A6 078F9A1D 4D1CD749


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1

    data is
                                                 5DC1C5 F4B41150
        CEE0EFC1 29B837B3 1C84D791 FF2E7EDA C29C2C50 CF8A4070
        9B98640F 7BBD32BC F0FCB613 F96D55D1 6056BB3C A6A77405


    w_i is
                                               055BC128 CC2D0E25
        0F47E4E4 F582375D E3EE5E9F E8316874 97E5AF1E 7CB69EFD


    W is
                                               055BC128 CC2D0E25
        0F47E4E4 F582375D E3EE5E9F E8316874 97E5AF1E 7CB69EFD


    ------------

    i = 2

    data is
                                                 5DC1C5 F4B41150
        CEE0EFC1 29B837B3 1C84D791 FF2E7EDA C29C2C50 CF8A4070
        9B98640F 7BBD32BC F0FCB613 F96D55D1 6056BB3C A6A77406
```

```
    w_i is
                                                EBD2FD31 C7CE2BBA
        0DBC6C74 C8A20A7D 72F60E6D 9F63ED50 9E963E54 A69E9048


    W is
                           055BC128 CC2D0E25 0F47E4E4 F582375D
        E3EE5E9F E8316874 97E5AF1E 7CB69EFD EBD2FD31 C7CE2BBA
        0DBC6C74 C8A20A7D 72F60E6D 9F63ED50 9E963E54 A69E9048


  returned_bits is
                           055BC128 CC2D0E25 0F47E4E4 F582375D
        E3EE5E9F E8316874 97E5AF1E 7CB69EFD EBD2FD31 C7CE2BBA
        0DBC6C74 C8A20A7D 72F60E6D 9F63ED50 9E963E54 A69E9048


----------------------------

  Update V

    0x03||V is
                                                035DC1C5 F4B41150
        CEE0EFC1 29B837B3 1C84D791 FF2E7EDA C29C2C50 CF8A4070
        9B98640F 7BBD32BC F0FCB613 F96D55D1 6056BB3C A6A77405


    H is
                                                B57A0660 EE3186F3
        EA802045 2C991ED0 6C740D20 4DE0A5D4 924A9B9F 8DCBC181


  Updated values

  V is
                                                  BFE3D6 81A20FBE
        39038F4D 66777C1B E579EEB4 857B42F2 1C3F598B 5962B7AA
        480EA565 FEEABDFB D6A7ECCB 9602C14B FA30F0F9 81900CD0


  reseed_counter is
                                                    0000 00000002
```

```
rnd_val is
                          055BC128 CC2D0E25 0F47E4E4 F582375D
        E3EE5E9F E8316874 97E5AF1E 7CB69EFD EBD2FD31 C7CE2BBA
        0DBC6C74 C8A20A7D 72F60E6D 9F63ED50 9E963E54 A69E9048


##############################################################

Hash_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                 C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                               20212223 24252627


    PersonalizationString =
                                                 404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

##############################################################
```

```
************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                               20212223 24252627


    personal_str is
                                                 404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                       010000
        01B80001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
```

```
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                                              A3E94E39 26FDA169
        C303D664 383905E0 D79962D1 65446D63 BDA654D1 32F72DB4


    temp =
                                              A3E94E39 26FDA169
        C303D664 383905E0 D79962D1 65446D63 BDA654D1 32F72DB4


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                        020000
        01B80001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                                              71564B45 6FF2EEC8
        36422ACC 5A029935 A7992990 94A1CA74 1B916DC0 26A7E107


    temp =
                                                A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


  V is
                                                A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


--------------------------
```

```
Hash_df - Generate C - Step 4

  0x00||V is
                                          00A3E94E 3926FDA1
      69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
      B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


  no_of_bits_to_return = 440

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                              01 000001B8 00A3E94E 3926FDA1
      69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
      B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


  Hash(counter||no_of_bits_to_return||input_string) is
                                          44748A78 B16E7555
      9F881D51 C15DFE6C 52CFB0BB 71620169 C7933427 67E7F887


  temp =
                                          44748A78 B16E7555
      9F881D51 C15DFE6C 52CFB0BB 71620169 C7933427 67E7F887


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                              02 000001B8 00A3E94E 3926FDA1
      69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
      B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


  Hash(counter||no_of_bits_to_return||input_string) is
                                          5F42CB6A 20C89D7C
      6EF3DC61 0D8FF203 D6766CED 1919D094 ED485EF7 FADDB668


  temp =
```

```
                                                  44748A 78B16E75
        559F881D 51C15DFE 6C52CFB0 BB716201 69C79334 2767E7F8
        875F42CB 6A20C89D 7C6EF3DC 610D8FF2 03D6766C ED1919D0


  C is
                                                  44748A 78B16E75
        559F881D 51C15DFE 6C52CFB0 BB716201 69C79334 2767E7F8
        875F42CB 6A20C89D 7C6EF3DC 610D8FF2 03D6766C ED1919D0


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  additional_input <empty>

--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                            01A3E9 4E3926FD A169C303 D6643839
        05E0D799 62D16544 6D63BDA6 54D132F7 2DB47156 4B456FF2
        EEC83642 2ACC5A02 9935A799 299094A1 CA808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

```
no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
             01000001 B801A3E9 4E3926FD A169C303 D6643839
    05E0D799 62D16544 6D63BDA6 54D132F7 2DB47156 4B456FF2
    EEC83642 2ACC5A02 9935A799 299094A1 CA808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


Hash(counter||no_of_bits_to_return||input_string) is
                                        E026A5C2 E7623E62
    B71A2E04 C25F0B08 582BE216 3634C049 6D2B65DA 7EAA03B5


temp =
                                        E026A5C2 E7623E62
    B71A2E04 C25F0B08 582BE216 3634C049 6D2B65DA 7EAA03B5


------------

i = 2

counter||no_of_bits_to_return||input_string is
             02000001 B801A3E9 4E3926FD A169C303 D6643839
    05E0D799 62D16544 6D63BDA6 54D132F7 2DB47156 4B456FF2
    EEC83642 2ACC5A02 9935A799 299094A1 CA808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


Hash(counter||no_of_bits_to_return||input_string) is
                                        C3B6B510 BB3FE474
    34071F70 7AC7FE4C 396AAAEE 764C9068 F3A21A46 411C15BB


temp =
                                          E026A5 C2E7623E
    62B71A2E 04C25F0B 08582BE2 163634C0 496D2B65 DA7EAA03
```

```
        B5C3B6B5 10BB3FE4 7434071F 707AC7FE 4C396AAA EE764C90


  V is
                                                E026A5 C2E7623E
        62B71A2E 04C25F0B 08582BE2 163634C0 496D2B65 DA7EAA03
        B5C3B6B5 10BB3FE4 7434071F 707AC7FE 4C396AAA EE764C90


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              00E026A5 C2E7623E
        62B71A2E 04C25F0B 08582BE2 163634C0 496D2B65 DA7EAA03
        B5C3B6B5 10BB3FE4 7434071F 707AC7FE 4C396AAA EE764C90


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 00E026A5 C2E7623E
        62B71A2E 04C25F0B 08582BE2 163634C0 496D2B65 DA7EAA03
        B5C3B6B5 10BB3FE4 7434071F 707AC7FE 4C396AAA EE764C90


    Hash(counter||no_of_bits_to_return||input_string) is
                                              C9EA754B EE0AB644
        15CA7FE3 2EBBFB07 ED932E7C 957ECEAE F0CD2FA7 7A46F9E8


    temp =
                                              C9EA754B EE0AB644
        15CA7FE3 2EBBFB07 ED932E7C 957ECEAE F0CD2FA7 7A46F9E8


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
```

```
                              02 000001B8 00E026A5 C2E7623E
        62B71A2E 04C25F0B 08582BE2 163634C0 496D2B65 DA7EAA03
        B5C3B6B5 10BB3FE4 7434071F 707AC7FE 4C396AAA EE764C90


    Hash(counter||no_of_bits_to_return||input_string) is
                                             59627897 54C6D298
        F9B5E459 6B4E0E6D F4F4B823 60DA3388 F6702DBF 2836D573


    temp =
                                               C9EA75 4BEE0AB6
        4415CA7F E32EBBFB 07ED932E 7C957ECE AEF0CD2F A77A46F9
        E8596278 9754C6D2 98F9B5E4 596B4E0E 6DF4F4B8 2360DA33


  C is
                                               C9EA75 4BEE0AB6
        4415CA7F E32EBBFB 07ED932E 7C957ECE AEF0CD2F A77A46F9
        E8596278 9754C6D2 98F9B5E4 596B4E0E 6DF4F4B8 2360DA33


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1

    data is
                                               E026A5 C2E7623E
        62B71A2E 04C25F0B 08582BE2 163634C0 496D2B65 DA7EAA03
        B5C3B6B5 10BB3FE4 7434071F 707AC7FE 4C396AAA EE764C90
```

```
    w_i is
                                                7A33D390 33F86058
        9F375E73 35307552 9658BBED 99C8A0EF 5E28B351 B2DF3358


    W is
                                                7A33D390 33F86058
        9F375E73 35307552 9658BBED 99C8A0EF 5E28B351 B2DF3358


    ------------

    i = 2

    data is
                                                  E026A5 C2E7623E
        62B71A2E 04C25F0B 08582BE2 163634C0 496D2B65 DA7EAA03
        B5C3B6B5 10BB3FE4 7434071F 707AC7FE 4C396AAA EE764C91


    w_i is
                                                B3D89BAC 7225DF9E
        3BCD0836 B99B5DBF 363A170C 7BB9BE41 A4AA9744 5ECEE41E


    W is
                            7A33D390 33F86058 9F375E73 35307552
        9658BBED 99C8A0EF 5E28B351 B2DF3358 B3D89BAC 7225DF9E
        3BCD0836 B99B5DBF 363A170C 7BB9BE41 A4AA9744 5ECEE41E


  returned_bits is
                            7A33D390 33F86058 9F375E73 35307552
        9658BBED 99C8A0EF 5E28B351 B2DF3358 B3D89BAC 7225DF9E
        3BCD0836 B99B5DBF 363A170C 7BB9BE41 A4AA9744 5ECEE41E


---------------------------

  Update V

    0x03||V is
                                                03E026A5 C2E7623E
        62B71A2E 04C25F0B 08582BE2 163634C0 496D2B65 DA7EAA03
        B5C3B6B5 10BB3FE4 7434071F 707AC7FE 4C396AAA EE764C90
```

```
    H is
                                                FAC59D54 E0D97A2A
        2A697018 1D83B3B9 B656F0A9 7B910686 F66DC805 F57BAB14


  Updated values

  V is
                                                  AA111B 0ED56CF4
        A6CCE4AD E7F11B06 1045BF10 92CBB38F F32395EA 62D26B27
        C8868945 C593BA70 C384ADAD 45771C93 B09C2769 0752D1D8


  reseed_counter is
                                                    0000 00000002


rnd_val is
                          7A33D390 33F86058 9F375E73 35307552
        9658BBED 99C8A0EF 5E28B351 B2DF3358 B3D89BAC 7225DF9E
        3BCD0836 B99B5DBF 363A170C 7BB9BE41 A4AA9744 5ECEE41E


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
```

```
  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                            01AA11 1B0ED56C F4A6CCE4 ADE7F11B
        061045BF 1092CBB3 8FF32395 EA62D26B 27C88689 45C593BA
        70C384AD AD45771C 93B09C27 690752D1 D8C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                01000001 B801AA11 1B0ED56C F4A6CCE4 ADE7F11B
        061045BF 1092CBB3 8FF32395 EA62D26B 27C88689 45C593BA
        70C384AD AD45771C 93B09C27 690752D1 D8C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                                            FC5F5648 EDC4FC30
        7B5C5A53 D51289B5 0E73DCEC 4AA1CB47 A3BAD846 BB57C3C4


    temp =
                                            FC5F5648 EDC4FC30
        7B5C5A53 D51289B5 0E73DCEC 4AA1CB47 A3BAD846 BB57C3C4


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                02000001 B801AA11 1B0ED56C F4A6CCE4 ADE7F11B
        061045BF 1092CBB3 8FF32395 EA62D26B 27C88689 45C593BA
```

```
        70C384AD AD45771C 93B09C27 690752D1 D8C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                                              80491DF5 21C4669B
        FFF37A41 8BAF6E9B EAEC3496 D0F1A6DC 3210CCA3 071DD6B7


    temp =
                                                FC5F56 48EDC4FC
        307B5C5A 53D51289 B50E73DC EC4AA1CB 47A3BAD8 46BB57C3
        C480491D F521C466 9BFFF37A 418BAF6E 9BEAEC34 96D0F1A6


  V is
                                                FC5F56 48EDC4FC
        307B5C5A 53D51289 B50E73DC EC4AA1CB 47A3BAD8 46BB57C3
        C480491D F521C466 9BFFF37A 418BAF6E 9BEAEC34 96D0F1A6


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              00FC5F56 48EDC4FC
        307B5C5A 53D51289 B50E73DC EC4AA1CB 47A3BAD8 46BB57C3
        C480491D F521C466 9BFFF37A 418BAF6E 9BEAEC34 96D0F1A6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 00FC5F56 48EDC4FC
        307B5C5A 53D51289 B50E73DC EC4AA1CB 47A3BAD8 46BB57C3
        C480491D F521C466 9BFFF37A 418BAF6E 9BEAEC34 96D0F1A6


    Hash(counter||no_of_bits_to_return||input_string) is
                                              62B07DC3 9EBDF310
```

```
        87B85DDC ECFD4335 62E53BAE 9F721C5A FAB8F1CF 0161C88E


    temp =
                                              62B07DC3 9EBDF310
        87B85DDC ECFD4335 62E53BAE 9F721C5A FAB8F1CF 0161C88E


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00FC5F56 48EDC4FC
        307B5C5A 53D51289 B50E73DC EC4AA1CB 47A3BAD8 46BB57C3
        C480491D F521C466 9BFFF37A 418BAF6E 9BEAEC34 96D0F1A6


    Hash(counter||no_of_bits_to_return||input_string) is
                                              45503E15 B26E7B80
        D51DB0B9 2452362D C3DC570D FE6E1721 DB2A72BA 67BAE5E5


    temp =
                                                62B07D C39EBDF3
        1087B85D DCECFD43 3562E53B AE9F721C 5AFAB8F1 CF0161C8
        8E45503E 15B26E7B 80D51DB0 B9245236 2DC3DC57 0DFE6E17


  C is
                                                62B07D C39EBDF3
        1087B85D DCECFD43 3562E53B AE9F721C 5AFAB8F1 CF0161C8
        8E45503E 15B26E7B 80D51DB0 B9245236 2DC3DC57 0DFE6E17


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

---------------------------

  Hashgen
```

```
  requested_no_of_bits  = 512

  ------------

  i = 1

  data is
                                              FC5F56 48EDC4FC
      307B5C5A 53D51289 B50E73DC EC4AA1CB 47A3BAD8 46BB57C3
      C480491D F521C466 9BFFF37A 418BAF6E 9BEAEC34 96D0F1A6


  w_i is
                                            041ABD94 079A0571
      885F1665 944E0E7F 1BFACDEA EAE9D44E EDC11FAD D84C34C7


  W is
                                            041ABD94 079A0571
      885F1665 944E0E7F 1BFACDEA EAE9D44E EDC11FAD D84C34C7


  ------------

  i = 2

  data is
                                              FC5F56 48EDC4FC
      307B5C5A 53D51289 B50E73DC EC4AA1CB 47A3BAD8 46BB57C3
      C480491D F521C466 9BFFF37A 418BAF6E 9BEAEC34 96D0F1A7


  w_i is
                                            CAA73D09 A0193193
      FA40A19F 644F048D 2A541704 2553DF52 51741B40 EACFEB98


  W is
                        041ABD94 079A0571 885F1665 944E0E7F
      1BFACDEA EAE9D44E EDC11FAD D84C34C7 CAA73D09 A0193193
      FA40A19F 644F048D 2A541704 2553DF52 51741B40 EACFEB98


returned_bits is
                        041ABD94 079A0571 885F1665 944E0E7F
```

```
        1BFACDEA EAE9D44E EDC11FAD D84C34C7 CAA73D09 A0193193
        FA40A19F 644F048D 2A541704 2553DF52 51741B40 EACFEB98


---------------------------

  Update V

    0x03||V is
                                            03FC5F56 48EDC4FC
        307B5C5A 53D51289 B50E73DC EC4AA1CB 47A3BAD8 46BB57C3
        C480491D F521C466 9BFFF37A 418BAF6E 9BEAEC34 96D0F1A6


    H is
                                            A5D6F49E 03109586
        67190F26 4D427131 85C06133 B88E3214 E4501826 1D64AB22


  Updated values

  V is
                                              5F0FD4 0C8C82EF
        410314B8 30C20FCC EA715918 9AEA13E8 48756868 18CD4F12
        B9DEA882 5816A413 A295725E B33E33B9 ADFEE0B1 C2340AE0


  reseed_counter is
                                                0000 00000002


rnd_val is
                         041ABD94 079A0571 885F1665 944E0E7F
        1BFACDEA EAE9D44E EDC11FAD D84C34C7 CAA73D09 A0193193
        FA40A19F 644F048D 2A541704 2553DF52 51741B40 EACFEB98


################################################################

Hash_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
```

```
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                20212223 24252627


    PersonalizationString =
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

Hash_DRBG_Instantiate_algorithm
```

```
    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                              20212223 24252627


    personal_str is
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                          010000
        01B80001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
                                                A3E94E39 26FDA169
        C303D664 383905E0 D79962D1 65446D63 BDA654D1 32F72DB4


    temp =
                                                A3E94E39 26FDA169
        C303D664 383905E0 D79962D1 65446D63 BDA654D1 32F72DB4


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                              020000
        01B80001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                                                71564B45 6FF2EEC8
        36422ACC 5A029935 A7992990 94A1CA74 1B916DC0 26A7E107


    temp =
                                                  A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


  V is
                                                  A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                                00A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
```

```
    B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                            01 000001B8 00A3E94E 3926FDA1
    69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
    B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


Hash(counter||no_of_bits_to_return||input_string) is
                                        44748A78 B16E7555
    9F881D51 C15DFE6C 52CFB0BB 71620169 C7933427 67E7F887


temp =
                                        44748A78 B16E7555
    9F881D51 C15DFE6C 52CFB0BB 71620169 C7933427 67E7F887


------------

i = 2

counter||no_of_bits_to_return||input_string is
                            02 000001B8 00A3E94E 3926FDA1
    69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
    B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


Hash(counter||no_of_bits_to_return||input_string) is
                                        5F42CB6A 20C89D7C
    6EF3DC61 0D8FF203 D6766CED 1919D094 ED485EF7 FADDB668


temp =
                                          44748A 78B16E75
    559F881D 51C15DFE 6C52CFB0 BB716201 69C79334 2767E7F8
    875F42CB 6A20C89D 7C6EF3DC 610D8FF2 03D6766C ED1919D0
```

```
  C is
                                                  44748A 78B16E75
        559F881D 51C15DFE 6C52CFB0 BB716201 69C79334 2767E7F8
        875F42CB 6A20C89D 7C6EF3DC 610D8FF2 03D6766C ED1919D0


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  additional_input
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01A3 E94E3926 FDA169C3 03D66438 3905E0D7 9962D165
        446D63BD A654D132 F72DB471 564B456F F2EEC836 422ACC5A
```

```
    029935A7 99299094 A1CA8081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                                      010000
    01B801A3 E94E3926 FDA169C3 03D66438 3905E0D7 9962D165
    446D63BD A654D132 F72DB471 564B456F F2EEC836 422ACC5A
    029935A7 99299094 A1CA8081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Hash(counter||no_of_bits_to_return||input_string) is
                                          9875BB7C 7A0B236B
    F46F4EA6 6F67C7B4 4F80EF70 614BEFE8 B085CCAF 5589A76F


temp =
                                          9875BB7C 7A0B236B
    F46F4EA6 6F67C7B4 4F80EF70 614BEFE8 B085CCAF 5589A76F


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
    01B801A3 E94E3926 FDA169C3 03D66438 3905E0D7 9962D165
    446D63BD A654D132 F72DB471 564B456F F2EEC836 422ACC5A
    029935A7 99299094 A1CA8081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
```

```
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    Hash(counter||no_of_bits_to_return||input_string) is
                                                85FD9669 53E20A55
        D2F35BA5 81EF5111 BFBF0565 3AF7E73F 13E35ACD 3D548B70


    temp =
                                                  9875BB 7C7A0B23
        6BF46F4E A66F67C7 B44F80EF 70614BEF E8B085CC AF5589A7
        6F85FD96 6953E20A 55D2F35B A581EF51 11BFBF05 653AF7E7


  V is
                                                  9875BB 7C7A0B23
        6BF46F4E A66F67C7 B44F80EF 70614BEF E8B085CC AF5589A7
        6F85FD96 6953E20A 55D2F35B A581EF51 11BFBF05 653AF7E7


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                                009875BB 7C7A0B23
        6BF46F4E A66F67C7 B44F80EF 70614BEF E8B085CC AF5589A7
        6F85FD96 6953E20A 55D2F35B A581EF51 11BFBF05 653AF7E7


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 009875BB 7C7A0B23
        6BF46F4E A66F67C7 B44F80EF 70614BEF E8B085CC AF5589A7
        6F85FD96 6953E20A 55D2F35B A581EF51 11BFBF05 653AF7E7


    Hash(counter||no_of_bits_to_return||input_string) is
                                                1280FE1F 05798CCA
        ED5D6DF6 E7D26F04 6E538CC5 2A6A030D A826B2B4 7982D6EE
```

```
    temp =
                                                1280FE1F 05798CCA
        ED5D6DF6 E7D26F04 6E538CC5 2A6A030D A826B2B4 7982D6EE


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 009875BB 7C7A0B23
        6BF46F4E A66F67C7 B44F80EF 70614BEF E8B085CC AF5589A7
        6F85FD96 6953E20A 55D2F35B A581EF51 11BFBF05 653AF7E7


    Hash(counter||no_of_bits_to_return||input_string) is
                                                8A686758 0706939E
        CC03FC11 B0059FE2 AEADEA0A 46985C64 0E0BF8E2 C4A6A026


    temp =
                                                  1280FE 1F05798C
        CAED5D6D F6E7D26F 046E538C C52A6A03 0DA826B2 B47982D6
        EE8A6867 58070693 9ECC03FC 11B0059F E2AEADEA 0A46985C


  C is
                                                  1280FE 1F05798C
        CAED5D6D F6E7D26F 046E538C C52A6A03 0DA826B2 B47982D6
        EE8A6867 58070693 9ECC03FC 11B0059F E2AEADEA 0A46985C


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 512
```

```
  ------------

  i = 1

  data is
                                                 9875BB 7C7A0B23
      6BF46F4E A66F67C7 B44F80EF 70614BEF E8B085CC AF5589A7
      6F85FD96 6953E20A 55D2F35B A581EF51 11BFBF05 653AF7E7


  w_i is
                                               88973297 5B36E8E2
      E7B74050 AEA17139 DA2B8634 DCE2133B 0634743F 477557AB


  W is
                                               88973297 5B36E8E2
      E7B74050 AEA17139 DA2B8634 DCE2133B 0634743F 477557AB


  ------------

  i = 2

  data is
                                                 9875BB 7C7A0B23
      6BF46F4E A66F67C7 B44F80EF 70614BEF E8B085CC AF5589A7
      6F85FD96 6953E20A 55D2F35B A581EF51 11BFBF05 653AF7E8


  w_i is
                                               7B844ED3 F2A46CC6
      3EB23286 464C51D5 D76971C4 7BC5B55F ED72A804 3CBF664F


  W is
                         88973297 5B36E8E2 E7B74050 AEA17139
      DA2B8634 DCE2133B 0634743F 477557AB 7B844ED3 F2A46CC6
      3EB23286 464C51D5 D76971C4 7BC5B55F ED72A804 3CBF664F


returned_bits is
                         88973297 5B36E8E2 E7B74050 AEA17139
      DA2B8634 DCE2133B 0634743F 477557AB 7B844ED3 F2A46CC6
      3EB23286 464C51D5 D76971C4 7BC5B55F ED72A804 3CBF664F
```

```
---------------------------

  Update V

    0x03||V is
                                                039875BB 7C7A0B23
        6BF46F4E A66F67C7 B44F80EF 70614BEF E8B085CC AF5589A7
        6F85FD96 6953E20A 55D2F35B A581EF51 11BFBF05 653AF7E7


    H is
                                                CB7E3B10 D6DB1D73
        6A6A8068 F72BAB20 FFCD5A6A 9515CA0D 56C7085E 5C788E39


  Updated values

  V is
                                                  AAF6B9 9B7F84B0
        36E1CCBC 9D573A36 B8BDD47C 358BB5F3 C1D6E790 3AAA29F1
        C87AE666 B88693BE F46C51C2 4C47BEFE 4B35754D CBFA1E7D


  reseed_counter is
                                                    0000 00000002


rnd_val is
                          88973297 5B36E8E2 E7B74050 AEA17139
        DA2B8634 DCE2133B 0634743F 477557AB 7B844ED3 F2A46CC6
        3EB23286 464C51D5 D76971C4 7BC5B55F ED72A804 3CBF664F


-------------------------------------------------------------

Second call to Generate

*************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input
```

```
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
-------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  additional_input
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01AA F6B99B7F 84B036E1 CCBC9D57 3A36B8BD D47C358B
        B5F3C1D6 E7903AAA 29F1C87A E666B886 93BEF46C 51C24C47
        BEFE4B35 754DCBFA 1E7DC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                        010000
        01B801AA F6B99B7F 84B036E1 CCBC9D57 3A36B8BD D47C358B
        B5F3C1D6 E7903AAA 29F1C87A E666B886 93BEF46C 51C24C47
```

```
    BEFE4B35 754DCBFA 1E7DC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Hash(counter||no_of_bits_to_return||input_string) is
                                          B06DBFB1 4E7F4E01
    2562942F E4F2A960 1707559D 7DD19089 8BC80624 E5C8C1BB


  temp =
                                          B06DBFB1 4E7F4E01
    2562942F E4F2A960 1707559D 7DD19089 8BC80624 E5C8C1BB


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                                                    020000
    01B801AA F6B99B7F 84B036E1 CCBC9D57 3A36B8BD D47C358B
    B5F3C1D6 E7903AAA 29F1C87A E666B886 93BEF46C 51C24C47
    BEFE4B35 754DCBFA 1E7DC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Hash(counter||no_of_bits_to_return||input_string) is
                                          9B90FB2E EF12ED24
    BEBD8DF7 1EF65C70 FA4E9186 3A31BE73 7AF120FF 4E66AD23


  temp =
                                            B06DBF B14E7F4E
    01256294 2FE4F2A9 60170755 9D7DD190 898BC806 24E5C8C1
    BB9B90FB 2EEF12ED 24BEBD8D F71EF65C 70FA4E91 863A31BE


V is
                                            B06DBF B14E7F4E
    01256294 2FE4F2A9 60170755 9D7DD190 898BC806 24E5C8C1
```

```
        BB9B90FB 2EEF12ED 24BEBD8D F71EF65C 70FA4E91 863A31BE


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            00B06DBF B14E7F4E
        01256294 2FE4F2A9 60170755 9D7DD190 898BC806 24E5C8C1
        BB9B90FB 2EEF12ED 24BEBD8D F71EF65C 70FA4E91 863A31BE


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 00B06DBF B14E7F4E
        01256294 2FE4F2A9 60170755 9D7DD190 898BC806 24E5C8C1
        BB9B90FB 2EEF12ED 24BEBD8D F71EF65C 70FA4E91 863A31BE


    Hash(counter||no_of_bits_to_return||input_string) is
                                            5C07B79C 12831BAC
        3652178B 2F907A69 619839D8 A7FAA2B6 95EFB310 82380135


    temp =
                                            5C07B79C 12831BAC
        3652178B 2F907A69 619839D8 A7FAA2B6 95EFB310 82380135


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                               02 000001B8 00B06DBF B14E7F4E
        01256294 2FE4F2A9 60170755 9D7DD190 898BC806 24E5C8C1
        BB9B90FB 2EEF12ED 24BEBD8D F71EF65C 70FA4E91 863A31BE


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
                                                85191F59 9C9907C7
        2192ED25 7E9F6CD3 77DD6BAC 337C19E4 9348D426 B2A13C96


    temp =
                                                  5C07B7 9C12831B
        AC365217 8B2F907A 69619839 D8A7FAA2 B695EFB3 10823801
        3585191F 599C9907 C72192ED 257E9F6C D377DD6B AC337C19


  C is
                                                  5C07B7 9C12831B
        AC365217 8B2F907A 69619839 D8A7FAA2 B695EFB3 10823801
        3585191F 599C9907 C72192ED 257E9F6C D377DD6B AC337C19


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1

    data is
                                                  B06DBF B14E7F4E
        01256294 2FE4F2A9 60170755 9D7DD190 898BC806 24E5C8C1
        BB9B90FB 2EEF12ED 24BEBD8D F71EF65C 70FA4E91 863A31BE


    w_i is
                                                BF49B889 BA984D34
        6387E864 7E98BB99 CD41A32F BEC1FCB3 B6A1B7D9 932BA7E1


    W is
```

```
                                                BF49B889 BA984D34
        6387E864 7E98BB99 CD41A32F BEC1FCB3 B6A1B7D9 932BA7E1


    ------------

    i = 2

    data is
                                                  B06DBF B14E7F4E
        01256294 2FE4F2A9 60170755 9D7DD190 898BC806 24E5C8C1
        BB9B90FB 2EEF12ED 24BEBD8D F71EF65C 70FA4E91 863A31BF


    w_i is
                                                1EE6BBD9 24405A2C
        7FCA890A 5E9A8DEA 66AC0CAC A0CA7BC1 8D74FBC0 2A11E453


    W is
                            BF49B889 BA984D34 6387E864 7E98BB99
        CD41A32F BEC1FCB3 B6A1B7D9 932BA7E1 1EE6BBD9 24405A2C
        7FCA890A 5E9A8DEA 66AC0CAC A0CA7BC1 8D74FBC0 2A11E453


  returned_bits is
                            BF49B889 BA984D34 6387E864 7E98BB99
        CD41A32F BEC1FCB3 B6A1B7D9 932BA7E1 1EE6BBD9 24405A2C
        7FCA890A 5E9A8DEA 66AC0CAC A0CA7BC1 8D74FBC0 2A11E453


--------------------------

  Update V

    0x03||V is
                                                03B06DBF B14E7F4E
        01256294 2FE4F2A9 60170755 9D7DD190 898BC806 24E5C8C1
        BB9B90FB 2EEF12ED 24BEBD8D F71EF65C 70FA4E91 863A31BE


    H is
                                                F35A4B8D F8320B8C
        BB1014B8 5552B8C3 8E4C1FEC 362484F6 CCB5175B F9E2318F
```

Updated values

V is

0C7577 4D610269
AD5BB4AB BB148323 C9789F8F 7625CC34 337C0347 2D9A0C4F
AC30BED2 DDDE64B8 7A2C7067 52C21AC0 11274359 2C4FDF67

reseed_counter is

0000 00000002

rnd_val is

BF49B889 BA984D34 6387E864 7E98BB99
CD41A32F BEC1FCB3 B6A1B7D9 932BA7E1 1EE6BBD9 24405A2C
7FCA890A 5E9A8DEA 66AC0CAC A0CA7BC1 8D74FBC0 2A11E453

```
###############################################################

Hash_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                    20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

Hash_DRBG_Instantiate_algorithm
```

```
    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                   20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

----------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                          000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
        63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                               01000003 78000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
        63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
    703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
    FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4


temp =
    703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
    FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                        02000003 78000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


Hash(counter||no_of_bits_to_return||input_string) is
    31487080 FDE0B521 DEBCFC5A AB9D39DA D9466C24 D4498964
    E4E318D4 DC777C22 A0EEE9B5 79B281AE 6AEB18B0 28D5C99A


temp =
    703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
    FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4
    31487080 FDE0B521 DEBCFC5A AB9D39DA D9466C24 D4498964
    E4E318D4 DC777C22 A0EEE9B5 79B281AE 6AEB18B0 28D5C99A


------------

i = 3

counter||no_of_bits_to_return||input_string is
                                        03000003 78000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
        9B71197A 30150000 F1E5B6AD 1EB81AB2 7B8E19BE 185E4F70
        61F1D3CA 9B3A0DF4 FD597962 C2070B7E B064B31F 4F3E10BD


    temp =
                            703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


  V is
                            703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A
```

```
Hash(counter||no_of_bits_to_return||input_string) is
    805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
    DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009


temp =
    805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
    DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 00703AEC B83762E8 855BF167 2A52FAEF
    5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
    FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
    DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
    AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


Hash(counter||no_of_bits_to_return||input_string) is
    424E5B0A BDF33FBB 5C02CA64 3A5753A2 4ED17561 9251B4E0
    89DACFDA C1CD8989 CF0F87B9 197E7BEF D8550312 538A89B9


temp =
    805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
    DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009
    424E5B0A BDF33FBB 5C02CA64 3A5753A2 4ED17561 9251B4E0
    89DACFDA C1CD8989 CF0F87B9 197E7BEF D8550312 538A89B9


------------

i = 3

counter||no_of_bits_to_return||input_string is
          03 00000378 00703AEC B83762E8 855BF167 2A52FAEF
    5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
    FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
    DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
    AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
        55F0BF84 2C6BF212 18612101 CB0E1A06 0E2E9C66 5E87E1BA
        9632F01B 4CF80D08 C9645BD1 830112EA 6EBFED69 A48CA9C9


    temp =
                            805F3E 8A9A40AA EE585729 8729B9CF
        5187C6DD BB443A05 D3DFF4C7 F2053B3C BE34E9B1 9763329E
        7CCE8806 8B1DD2C0 09424E5B 0ABDF33F BB5C02CA 643A5753
        A24ED175 619251B4 E089DACF DAC1CD89 89CF0F87 B9197E7B
        EFD85503 12538A89 B955F0BF 842C6BF2 12186121 01CB0E1A


  C is
                            805F3E 8A9A40AA EE585729 8729B9CF
        5187C6DD BB443A05 D3DFF4C7 F2053B3C BE34E9B1 9763329E
        7CCE8806 8B1DD2C0 09424E5B 0ABDF33F BB5C02CA 643A5753
        A24ED175 619251B4 E089DACF DAC1CD89 89CF0F87 B9197E7B
        EFD85503 12538A89 B955F0BF 842C6BF2 12186121 01CB0E1A


----------------------------------------------------------------

First call to Generate

****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
```

```
                          703AEC B83762E8 855BF167 2A52FAEF
      5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
      FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
      DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
      AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


  w_i is
      04FF23AD 15E78790 ADD36B43 8BBC097C 7A11747C C2CCEEDE
      2C978B23 B3DC63B7 32C95306 1D776499 0ABFEFC4 7A581B92


  W is
      04FF23AD 15E78790 ADD36B43 8BBC097C 7A11747C C2CCEEDE
      2C978B23 B3DC63B7 32C95306 1D776499 0ABFEFC4 7A581B92


  ------------

  i = 2

  data is
                          703AEC B83762E8 855BF167 2A52FAEF
      5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
      FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
      DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
      AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81B


  w_i is
      1BC0428C 4F122124 60E406A0 F0651E7F 0CB9A90A BFDB07B5
      25565C74 F0AA0850 82F6CF21 3AAFAD0C 06468950 78F1E1FE


  W is
      04FF23AD 15E78790 ADD36B43 8BBC097C 7A11747C C2CCEEDE
      2C978B23 B3DC63B7 32C95306 1D776499 0ABFEFC4 7A581B92
      1BC0428C 4F122124 60E406A0 F0651E7F 0CB9A90A BFDB07B5
      25565C74 F0AA0850 82F6CF21 3AAFAD0C 06468950 78F1E1FE


returned_bits is
      04FF23AD 15E78790 ADD36B43 8BBC097C 7A11747C C2CCEEDE
      2C978B23 B3DC63B7 32C95306 1D776499 0ABFEFC4 7A581B92
      1BC0428C 4F122124 60E406A0 F0651E7F 0CB9A90A BFDB07B5
      25565C74 F0AA0850 82F6CF21 3AAFAD0C 06468950 78F1E1FE
```

```
---------------------------

  Update V

    0x03||V is
                           03703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


    H is
        DAFD91E4 4FB509DF 5AFC7DA7 9B82820D 28A7153C C258E03A
        2400E763 3648DD95 B68BF28C 7DC37D68 854DADDB BB1A3D54


  Updated values

  V is
                             F09A2B 42D1A393 73B44890 B17CB4BE
        AE032361 A3D80A07 04DEBB04 8CCB307B E157F70E 65D99FA8
        7CBF62CA A2E65BEF CD7396CB 8BBBD3F4 DD3ABFC6 BEE5F48E
        5825A9C5 D61BA51D A06B3B90 4B20C712 D51713AE 30EC1137
        C244277E F8C53DE9 0A7D5465 7C1FFE5A 9857F4B3 6A040389


  reseed_counter is
                                                 0000 00000002


rnd_val is
        04FF23AD 15E78790 ADD36B43 8BBC097C 7A11747C C2CCEEDE
        2C978B23 B3DC63B7 32C95306 1D776499 0ABFEFC4 7A581B92
        1BC0428C 4F122124 60E406A0 F0651E7F 0CB9A90A BFDB07B5
        25565C74 F0AA0850 82F6CF21 3AAFAD0C 06468950 78F1E1FE


---------------------------------------------------------------

Second call to Generate

***************************************************************
```

```
Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                           F09A2B 42D1A393 73B44890 B17CB4BE
        AE032361 A3D80A07 04DEBB04 8CCB307B E157F70E 65D99FA8
        7CBF62CA A2E65BEF CD7396CB 8BBBD3F4 DD3ABFC6 BEE5F48E
        5825A9C5 D61BA51D A06B3B90 4B20C712 D51713AE 30EC1137
        C244277E F8C53DE9 0A7D5465 7C1FFE5A 9857F4B3 6A040389


    w_i is
        4F35B85F 95DEE3E8 73054905 CFD02341 653E18F5 29930CBE
        14D909F3 7FEAF2C7 90D22FAE 7516B459 0BE35D53 E2FE1A35


    W is
        4F35B85F 95DEE3E8 73054905 CFD02341 653E18F5 29930CBE
        14D909F3 7FEAF2C7 90D22FAE 7516B459 0BE35D53 E2FE1A35


    ------------

    i = 2

    data is
                           F09A2B 42D1A393 73B44890 B17CB4BE
        AE032361 A3D80A07 04DEBB04 8CCB307B E157F70E 65D99FA8
        7CBF62CA A2E65BEF CD7396CB 8BBBD3F4 DD3ABFC6 BEE5F48E
        5825A9C5 D61BA51D A06B3B90 4B20C712 D51713AE 30EC1137
        C244277E F8C53DE9 0A7D5465 7C1FFE5A 9857F4B3 6A04038A
```

```
    w_i is
        AFE4B660 7CB35858 9C3B4D09 4A1D81FE 0717F1DF 5BDDEB3E
        114F130B B781E66C 22B5B770 E8AE115F F39F8ADA F66DEEDF


    W is
        4F35B85F 95DEE3E8 73054905 CFD02341 653E18F5 29930CBE
        14D909F3 7FEAF2C7 90D22FAE 7516B459 0BE35D53 E2FE1A35
        AFE4B660 7CB35858 9C3B4D09 4A1D81FE 0717F1DF 5BDDEB3E
        114F130B B781E66C 22B5B770 E8AE115F F39F8ADA F66DEEDF


  returned_bits is
        4F35B85F 95DEE3E8 73054905 CFD02341 653E18F5 29930CBE
        14D909F3 7FEAF2C7 90D22FAE 7516B459 0BE35D53 E2FE1A35
        AFE4B660 7CB35858 9C3B4D09 4A1D81FE 0717F1DF 5BDDEB3E
        114F130B B781E66C 22B5B770 E8AE115F F39F8ADA F66DEEDF


---------------------------

  Update V

    0x03||V is
                          03F09A2B 42D1A393 73B44890 B17CB4BE
        AE032361 A3D80A07 04DEBB04 8CCB307B E157F70E 65D99FA8
        7CBF62CA A2E65BEF CD7396CB 8BBBD3F4 DD3ABFC6 BEE5F48E
        5825A9C5 D61BA51D A06B3B90 4B20C712 D51713AE 30EC1137
        C244277E F8C53DE9 0A7D5465 7C1FFE5A 9857F4B3 6A040389


    H is
        DFE8790D F7153FE5 E634CDD6 48943BAC 36AED716 064DEAED
        97954957 CD97E5CD CB2F723B 27823018 D414D93F 7EF82599


  Updated values

  V is
                            70F969 CD6BE43E 620C9FBA 38A66E8D
        FF8AEA3F 5F1C440C D8BEAFCC 7ED06BB8 9F8CE0BF FD3CD246
        F98DEAD1 2E042EAF D6B5E526 9679C734 9896C291 23204BE2
        DA5CF449 2EC336B8 6729E436 6E76D048 9594FA4B F0537AA1
        49B1C5D9 D8B0AE40 8F02B760 27CE9A65 7E852F13 EAC7373E
```

```
  reseed_counter is
                                                  0000 00000003


rnd_val is
        4F35B85F 95DEE3E8 73054905 CFD02341 653E18F5 29930CBE
        14D909F3 7FEAF2C7 90D22FAE 7516B459 0BE35D53 E2FE1A35
        AFE4B660 7CB35858 9C3B4D09 4A1D81FE 0717F1DF 5BDDEB3E
        114F130B B781E66C 22B5B770 E8AE115F F39F8ADA F66DEEDF


################################################################

Hash_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                    20212223 24252627 28292A2B
```

```
    PersonalizationString = <empty>

    AdditionalInput1 =
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    AdditionalInput2 =
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


###############################################################

***************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                    20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

--------------------------

  Hash_df - Generate seed(which is V) - Step 2
```

```
seed_material is
                                                          000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                          01000003 78000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


Hash(counter||no_of_bits_to_return||input_string) is
    703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
    FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4


temp =
    703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
    FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                          02000003 78000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B
```

```
  Hash(counter||no_of_bits_to_return||input_string) is
      31487080 FDE0B521 DEBCFC5A AB9D39DA D9466C24 D4498964
      E4E318D4 DC777C22 A0EEE9B5 79B281AE 6AEB18B0 28D5C99A


  temp =
      703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
      FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4
      31487080 FDE0B521 DEBCFC5A AB9D39DA D9466C24 D4498964
      E4E318D4 DC777C22 A0EEE9B5 79B281AE 6AEB18B0 28D5C99A


  ------------

  i = 3

  counter||no_of_bits_to_return||input_string is
                                          03000003 78000102
      03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
      1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
      33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
      4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
      63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


  Hash(counter||no_of_bits_to_return||input_string) is
      9B71197A 30150000 F1E5B6AD 1EB81AB2 7B8E19BE 185E4F70
      61F1D3CA 9B3A0DF4 FD597962 C2070B7E B064B31F 4F3E10BD


  temp =
                          703AEC B83762E8 855BF167 2A52FAEF
      5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
      FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
      DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
      AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


V is
                          703AEC B83762E8 855BF167 2A52FAEF
      5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
      FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
      DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
      AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A
```

```
---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


    Hash(counter||no_of_bits_to_return||input_string) is
        805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
        DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009


    temp =
        805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
        DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
              02 00000378 00703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
```

```
    AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


  Hash(counter||no_of_bits_to_return||input_string) is
    424E5B0A BDF33FBB 5C02CA64 3A5753A2 4ED17561 9251B4E0
    89DACFDA C1CD8989 CF0F87B9 197E7BEF D8550312 538A89B9


  temp =
    805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
    DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009
    424E5B0A BDF33FBB 5C02CA64 3A5753A2 4ED17561 9251B4E0
    89DACFDA C1CD8989 CF0F87B9 197E7BEF D8550312 538A89B9


  ------------

  i = 3

  counter||no_of_bits_to_return||input_string is
           03 00000378 00703AEC B83762E8 855BF167 2A52FAEF
    5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
    FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
    DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
    AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


  Hash(counter||no_of_bits_to_return||input_string) is
    55F0BF84 2C6BF212 18612101 CB0E1A06 0E2E9C66 5E87E1BA
    9632F01B 4CF80D08 C9645BD1 830112EA 6EBFED69 A48CA9C9


  temp =
                       805F3E 8A9A40AA EE585729 8729B9CF
    5187C6DD BB443A05 D3DFF4C7 F2053B3C BE34E9B1 9763329E
    7CCE8806 8B1DD2C0 09424E5B 0ABDF33F BB5C02CA 643A5753
    A24ED175 619251B4 E089DACF DAC1CD89 89CF0F87 B9197E7B
    EFD85503 12538A89 B955F0BF 842C6BF2 12186121 01CB0E1A


C is
                       805F3E 8A9A40AA EE585729 8729B9CF
    5187C6DD BB443A05 D3DFF4C7 F2053B3C BE34E9B1 9763329E
    7CCE8806 8B1DD2C0 09424E5B 0ABDF33F BB5C02CA 643A5753
    A24ED175 619251B4 E089DACF DAC1CD89 89CF0F87 B9197E7B
    EFD85503 12538A89 B955F0BF 842C6BF2 12186121 01CB0E1A
```

```
---------------------------------------------------------------

First call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


---------------------------

  Process additional_input

    0x02||V||additional_input is
                                                02703A ECB83762
        E8855BF1 672A52FA EF5C7B5C 83E893D0 0130FEC6 3C9AC5F5
        3F23230D 5CCE766D 09FFF0DA C417C889 2FC43148 7080FDE0
        B521DEBC FC5AAB9D 39DAD946 6C24D449 8964E4E3 18D4DC77
        7C22A0EE E9B579B2 81AE6AEB 18B028D5 C99A9B71 197A3015
        0000F1E5 B6AD1EB8 1A606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    w=Hash(0x02||V||additional_input) is
        EE4375B2 9D2DB6EA 2FEBDE64 3BE768BB 5728BDCD 3CC2E9C7
        8DD9E04A 3B21D222 B5255FAD ADDAA214 FCEBFCBA 774E4C1F


    V is
                            703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D3A
```

```
        C91CBC1E C2020073 94D0C17D 10C3E037 79C9ACB6 F23C9C49
        3C44CB62 EB4AA7EC 4FC0D0C7 280AB714 FDDDE271 246D0439


----------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                           703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D3A
        C91CBC1E C2020073 94D0C17D 10C3E037 79C9ACB6 F23C9C49
        3C44CB62 EB4AA7EC 4FC0D0C7 280AB714 FDDDE271 246D0439


    w_i is
        03D1294E 33F12491 597CF23D B8DF118F 9AD2BA71 D84B3C67
        60A43C58 39A3F449 ADE2B0F3 E02A13D2 2E1119C7 B95C207E


    W is
        03D1294E 33F12491 597CF23D B8DF118F 9AD2BA71 D84B3C67
        60A43C58 39A3F449 ADE2B0F3 E02A13D2 2E1119C7 B95C207E


    ------------

    i = 2

    data is
                           703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D3A
        C91CBC1E C2020073 94D0C17D 10C3E037 79C9ACB6 F23C9C49
        3C44CB62 EB4AA7EC 4FC0D0C7 280AB714 FDDDE271 246D043A


    w_i is
        0844A8BF E837C229 0BE251C8 DCC4D8CC 04B1CEF6 B42931CB
```

```
        54248C52 975CB5F7 5E2867B5 4C139B4C 0072E6EC 8A4EA49B


    W is
        03D1294E 33F12491 597CF23D B8DF118F 9AD2BA71 D84B3C67
        60A43C58 39A3F449 ADE2B0F3 E02A13D2 2E1119C7 B95C207E
        0844A8BF E837C229 0BE251C8 DCC4D8CC 04B1CEF6 B42931CB
        54248C52 975CB5F7 5E2867B5 4C139B4C 0072E6EC 8A4EA49B


  returned_bits is
        03D1294E 33F12491 597CF23D B8DF118F 9AD2BA71 D84B3C67
        60A43C58 39A3F449 ADE2B0F3 E02A13D2 2E1119C7 B95C207E
        0844A8BF E837C229 0BE251C8 DCC4D8CC 04B1CEF6 B42931CB
        54248C52 975CB5F7 5E2867B5 4C139B4C 0072E6EC 8A4EA49B


---------------------------

  Update V

    0x03||V is
                          03703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D3A
        C91CBC1E C2020073 94D0C17D 10C3E037 79C9ACB6 F23C9C49
        3C44CB62 EB4AA7EC 4FC0D0C7 280AB714 FDDDE271 246D0439


    H is
        EC6876DB 88ECA9C7 BC5F8875 B8D684F7 CDFA2747 D76628B5
        57AECAB4 07852B30 83E26D7F 9972C3F7 F1155371 5996C1C6


  Updated values

  V is
                            F09A2B 42D1A393 73B44890 B17CB4BE
        AE032361 A3D80A07 04DEBB04 8CCB307B E157F70E 65D99FA8
        7CBF62CA A2E65BEF CD7396CB 8BBBD3F4 DD3ABFC6 BEE5F48F
        57D4046F AC80FBF0 31BA24C2 A45C32B8 D192E386 82BC437A
        83CBEB1A 05235DA6 8CF92F06 45A9E6FF 010B9703 7FCED41A


  reseed_counter is
                                                0000 00000002
```

```
rnd_val is
        03D1294E 33F12491 597CF23D B8DF118F 9AD2BA71 D84B3C67
        60A43C58 39A3F449 ADE2B0F3 E02A13D2 2E1119C7 B95C207E
        0844A8BF E837C229 0BE251C8 DCC4D8CC 04B1CEF6 B42931CB
        54248C52 975CB5F7 5E2867B5 4C139B4C 0072E6EC 8A4EA49B


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
       AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
       C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
       DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
       F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


--------------------------

  Process additional_input

    0x02||V||additional_input is
                                                 02F09A 2B42D1A3
        9373B448 90B17CB4 BEAE0323 61A3D80A 0704DEBB 048CCB30
        7BE157F7 0E65D99F A87CBF62 CAA2E65B EFCD7396 CB8BBBD3
        F4DD3ABF C6BEE5F4 8F57D404 6FAC80FB F031BA24 C2A45C32
        B8D192E3 8682BC43 7A83CBEB 1A05235D A68CF92F 0645A9E6
        FF010B97 037FCED4 1AA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    w=Hash(0x02||V||additional_input) is
        D7D8B279 6E9806AC 119CBC1C 927B6B0E 4A22F083 2C0A53EF
```

```
        848D7133 30AE8B68 3625E0E3 4A8E4A72 0947CE2A F46128B8


    V is
                            F09A2B 42D1A393 73B44890 B17CB4BE
        AE032361 A3D80A07 04DEBB04 8CCB307B E157F70E 65D99FA8
        7CBF62CA A2E65BEF CD7396CB 8BBBD3F4 DD3ABFC6 BEE5F490
        2FACB6E9 1B19029C 4356E0DF 36D79DC7 1BB5D409 AEC6976A
        08595C4D 35D1E90E C31F0FE9 90383171 0A53652E 742FFCD2


----------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                            F09A2B 42D1A393 73B44890 B17CB4BE
        AE032361 A3D80A07 04DEBB04 8CCB307B E157F70E 65D99FA8
        7CBF62CA A2E65BEF CD7396CB 8BBBD3F4 DD3ABFC6 BEE5F490
        2FACB6E9 1B19029C 4356E0DF 36D79DC7 1BB5D409 AEC6976A
        08595C4D 35D1E90E C31F0FE9 90383171 0A53652E 742FFCD2


    w_i is
        D5398518 F8087E2F 155B3C56 47AF609C 8820D5F5 4B787490
        2934FB10 97C89440 A47A71E3 6A9A32A2 242F3799 66CD3F5D


    W is
        D5398518 F8087E2F 155B3C56 47AF609C 8820D5F5 4B787490
        2934FB10 97C89440 A47A71E3 6A9A32A2 242F3799 66CD3F5D


    ------------

    i = 2

    data is
                            F09A2B 42D1A393 73B44890 B17CB4BE
        AE032361 A3D80A07 04DEBB04 8CCB307B E157F70E 65D99FA8
```

```
        7CBF62CA A2E65BEF CD7396CB 8BBBD3F4 DD3ABFC6 BEE5F490
        2FACB6E9 1B19029C 4356E0DF 36D79DC7 1BB5D409 AEC6976A
        08595C4D 35D1E90E C31F0FE9 90383171 0A53652E 742FFCD3


    w_i is
        BBEF623B D6117BDE 441D2A94 815FD5C1 3638DE99 D50CFE0E
        390A2A6B 137B55A4 2452F182 8060DB3C 68AF5C86 A83AF833


    W is
        D5398518 F8087E2F 155B3C56 47AF609C 8820D5F5 4B787490
        2934FB10 97C89440 A47A71E3 6A9A32A2 242F3799 66CD3F5D
        BBEF623B D6117BDE 441D2A94 815FD5C1 3638DE99 D50CFE0E
        390A2A6B 137B55A4 2452F182 8060DB3C 68AF5C86 A83AF833


  returned_bits is
        D5398518 F8087E2F 155B3C56 47AF609C 8820D5F5 4B787490
        2934FB10 97C89440 A47A71E3 6A9A32A2 242F3799 66CD3F5D
        BBEF623B D6117BDE 441D2A94 815FD5C1 3638DE99 D50CFE0E
        390A2A6B 137B55A4 2452F182 8060DB3C 68AF5C86 A83AF833


--------------------------

  Update V

    0x03||V is
                          03F09A2B 42D1A393 73B44890 B17CB4BE
        AE032361 A3D80A07 04DEBB04 8CCB307B E157F70E 65D99FA8
        7CBF62CA A2E65BEF CD7396CB 8BBBD3F4 DD3ABFC6 BEE5F490
        2FACB6E9 1B19029C 4356E0DF 36D79DC7 1BB5D409 AEC6976A
        08595C4D 35D1E90E C31F0FE9 90383171 0A53652E 742FFCD2


    H is
        833DD309 055891D9 1B580F44 646C8AD9 B2839216 292FFC8F
        E13FA67E 2A56AC10 648A6E1C 5F810898 62581F7D 32829D4F


  Updated values

  V is
                            70F969 CD6BE43E 620C9FBA 38A66E8D
        FF8AEA3F 5F1C440C D8BEAFCC 7ED06BB8 9F8CE0BF FD3CD246
```

```
        F98DEAD1 2E042EAF D6B5E526 9679C734 9896C291 23204BE4
        55395B67 8203E62A 3F38CAF3 7605F62A 580875A7 91101275
        D97157CE 727C1FA8 E0FF6EC5 73E5A5FB 7EC3E5CC A87DA83D


  reseed_counter is
                                                0000 00000003


rnd_val is
        D5398518 F8087E2F 155B3C56 47AF609C 8820D5F5 4B787490
        2934FB10 97C89440 A47A71E3 6A9A32A2 242F3799 66CD3F5D
        BBEF623B D6117BDE 441D2A94 815FD5C1 3638DE99 D50CFE0E
        390A2A6B 137B55A4 2452F182 8060DB3C 68AF5C86 A83AF833


##############################################################

Hash_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
```

```
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                20212223 24252627 28292A2B


    PersonalizationString =
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    AdditionalInput = <empty>

###############################################################

***************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                20212223 24252627 28292A2B


    personal_str is
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "No PredictionResistance"

---------------------------
```

```
Hash_df - Generate seed(which is V) - Step 2

  seed_material is
                  0001 02030405 06070809 0A0B0C0D 0E0F1011
      12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
      2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
      42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
      5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
      23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
      4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
      9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  no_of_bits_to_return = 888

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
        010000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
      12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
      2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
      42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
      5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
      23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
      4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
      9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  Hash(counter||no_of_bits_to_return||input_string) is
      A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
      EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964


  temp =
      A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
      EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964


  ------------
```

```
i = 2

counter||no_of_bits_to_return||input_string is
      020000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
    C74754B6 A1E77C6C 0DE0245E 3BC81E15 85F2F379 F4489643
    5F61C23D B552DB8B 3190F5F3 7B966F3D D000CEB5 373CA2BD


temp =
    A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
    EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964
    C74754B6 A1E77C6C 0DE0245E 3BC81E15 85F2F379 F4489643
    5F61C23D B552DB8B 3190F5F3 7B966F3D D000CEB5 373CA2BD


------------

i = 3

counter||no_of_bits_to_return||input_string is
      030000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
```

```
        A8989587 CED14C8E 80790CD7 146F3328 3D84860A 708750EA
        1FDCD1DA D814E76A CA6E310F 12AA0BBA 611A8E86 FC0EAE47


    temp =
                            A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


  V is
                            A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           00A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33
```

```
Hash(counter||no_of_bits_to_return||input_string) is
    DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
    273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D


temp =
    DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
    273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 00A028F8 43783D77 21E32AC5 FD923031
    884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
    C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
    1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
    3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


Hash(counter||no_of_bits_to_return||input_string) is
    7B72F966 9A700AF1 C7E3466A 5E89A0DC A45282E7 1A39E4AA
    24585736 11785015 85B95258 C40A2016 2D1F62CA 988BBEC7


temp =
    DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
    273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D
    7B72F966 9A700AF1 C7E3466A 5E89A0DC A45282E7 1A39E4AA
    24585736 11785015 85B95258 C40A2016 2D1F62CA 988BBEC7


------------

i = 3

counter||no_of_bits_to_return||input_string is
          03 00000378 00A028F8 43783D77 21E32AC5 FD923031
    884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
    C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
    1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
    3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
        FD2CAD8E 501A9FA7 18212A41 9FA2251F 01E46C40 DDBF4D85
        223B6E11 48351858 CC99BE10 6D1A4301 A307DBAF DE079ADA


    temp =
                            DE0424 3D3BB302 329A9112 4D780ADC
        F3672DDD 2CE78196 3E273BB2 49F6EC13 B16A903F 40D01C2D
        FF1464BF A6AFD698 7D7B72F9 669A700A F1C7E346 6A5E89A0
        DCA45282 E71A39E4 AA245857 36117850 1585B952 58C40A20
        162D1F62 CA988BBE C7FD2CAD 8E501A9F A718212A 419FA225


  C is
                            DE0424 3D3BB302 329A9112 4D780ADC
        F3672DDD 2CE78196 3E273BB2 49F6EC13 B16A903F 40D01C2D
        FF1464BF A6AFD698 7D7B72F9 669A700A F1C7E346 6A5E89A0
        DCA45282 E71A39E4 AA245857 36117850 1585B952 58C40A20
        162D1F62 CA988BBE C7FD2CAD 8E501A9F A718212A 419FA225


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                            A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
```

```
      C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
      1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
      3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


  w_i is
      CB339E74 95C3645C 5961FF07 871F47ED F9D33B0A B471282F
      0E8FADD0 74661AEE 4D4F47C1 E39CE4FF 381A8BC4 DE0AA260


  W is
      CB339E74 95C3645C 5961FF07 871F47ED F9D33B0A B471282F
      0E8FADD0 74661AEE 4D4F47C1 E39CE4FF 381A8BC4 DE0AA260


  ------------

  i = 2

  data is
                          A028F8 43783D77 21E32AC5 FD923031
      884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
      C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
      1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
      3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F34


  w_i is
      ABD20471 17E89ED4 70829892 FC806CA1 33FC8435 340BE2EC
      8278AFC5 DF48595D 1D205F7F 835E2549 B9068A85 16FB1496


  W is
      CB339E74 95C3645C 5961FF07 871F47ED F9D33B0A B471282F
      0E8FADD0 74661AEE 4D4F47C1 E39CE4FF 381A8BC4 DE0AA260
      ABD20471 17E89ED4 70829892 FC806CA1 33FC8435 340BE2EC
      8278AFC5 DF48595D 1D205F7F 835E2549 B9068A85 16FB1496


returned_bits is
      CB339E74 95C3645C 5961FF07 871F47ED F9D33B0A B471282F
      0E8FADD0 74661AEE 4D4F47C1 E39CE4FF 381A8BC4 DE0AA260
      ABD20471 17E89ED4 70829892 FC806CA1 33FC8435 340BE2EC
      8278AFC5 DF48595D 1D205F7F 835E2549 B9068A85 16FB1496
```

```
--------------------------

  Update V

    0x03||V is
                          03A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


    H is
        C51C82A3 D8EF332A 9C797699 F9E02289 F64D4850 CA0B186F
        BA66C32F 3971156C CA591193 6567EA3A 8EAEA908 EF1F29AE


  Updated values

  V is
                            7E2D1C 80B3F079 547DBBD8 4B0A3B0E
        7BB427B1 1D472454 4812A635 1179A233 ED93C886 FA5EE0E7
        BFDCCC0D 91907551 E242BA4E 1D3C5787 5DD5C36A C89A51BF
        B746C81A 39FDB5A5 89FD30B3 6DA6EDB5 97049299 164AB8FF
        0E63E360 B940DDCE 4FFED6D6 7B86D626 C4474340 07D33B07


  reseed_counter is
                                                0000 00000002


rnd_val is
        CB339E74 95C3645C 5961FF07 871F47ED F9D33B0A B471282F
        0E8FADD0 74661AEE 4D4F47C1 E39CE4FF 381A8BC4 DE0AA260
        ABD20471 17E89ED4 70829892 FC806CA1 33FC8435 340BE2EC
        8278AFC5 DF48595D 1D205F7F 835E2549 B9068A85 16FB1496


-------------------------------------------------------------

Second call to Generate

*************************************************************

Hash_DRBG_Generate_algorithm
```

```
  requested_number_of_bits = 768

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                            7E2D1C 80B3F079 547DBBD8 4B0A3B0E
        7BB427B1 1D472454 4812A635 1179A233 ED93C886 FA5EE0E7
        BFDCCC0D 91907551 E242BA4E 1D3C5787 5DD5C36A C89A51BF
        B746C81A 39FDB5A5 89FD30B3 6DA6EDB5 97049299 164AB8FF
        0E63E360 B940DDCE 4FFED6D6 7B86D626 C4474340 07D33B07


    w_i is
        938BAB9C 357B9023 92AEFA66 8DFDB88C 9C671FC0 220ED319
        7F852B3B 9C27AD33 D99403E6 56510F77 E964130B 284759A0


    W is
        938BAB9C 357B9023 92AEFA66 8DFDB88C 9C671FC0 220ED319
        7F852B3B 9C27AD33 D99403E6 56510F77 E964130B 284759A0


    ------------

    i = 2

    data is
                            7E2D1C 80B3F079 547DBBD8 4B0A3B0E
        7BB427B1 1D472454 4812A635 1179A233 ED93C886 FA5EE0E7
        BFDCCC0D 91907551 E242BA4E 1D3C5787 5DD5C36A C89A51BF
        B746C81A 39FDB5A5 89FD30B3 6DA6EDB5 97049299 164AB8FF
        0E63E360 B940DDCE 4FFED6D6 7B86D626 C4474340 07D33B08


    w_i is
        EB42F933 E6B2D170 99744089 402ED23B C8C0CAD5 9BA485A9
```

```
        04B5456E 4EFEFC22 9415778F 50957FDD B559C053 FB97CE79


    W is
        938BAB9C 357B9023 92AEFA66 8DFDB88C 9C671FC0 220ED319
        7F852B3B 9C27AD33 D99403E6 56510F77 E964130B 284759A0
        EB42F933 E6B2D170 99744089 402ED23B C8C0CAD5 9BA485A9
        04B5456E 4EFEFC22 9415778F 50957FDD B559C053 FB97CE79


  returned_bits is
        938BAB9C 357B9023 92AEFA66 8DFDB88C 9C671FC0 220ED319
        7F852B3B 9C27AD33 D99403E6 56510F77 E964130B 284759A0
        EB42F933 E6B2D170 99744089 402ED23B C8C0CAD5 9BA485A9
        04B5456E 4EFEFC22 9415778F 50957FDD B559C053 FB97CE79


---------------------------

  Update V

    0x03||V is
                           037E2D1C 80B3F079 547DBBD8 4B0A3B0E
        7BB427B1 1D472454 4812A635 1179A233 ED93C886 FA5EE0E7
        BFDCCC0D 91907551 E242BA4E 1D3C5787 5DD5C36A C89A51BF
        B746C81A 39FDB5A5 89FD30B3 6DA6EDB5 97049299 164AB8FF
        0E63E360 B940DDCE 4FFED6D6 7B86D626 C4474340 07D33B07


    H is
        6A7CBF9C FBFDBBFB A6105685 736B5949 231723D9 902E60CB
        289AA32B 0B06A6FF D00F7F0A 29DFD1EF 461D8806 4F8A4AD5


  Updated values

  V is
                             5C3140 BDEFA37B 87184CEA 988245EB
        6F1B558E 4A2EA5EA 8639E1E7 5B708E47 9EFE58C6 3B2EFD15
        BEF130CD 38404BEA 5FBE2D47 83D6C792 4F9DA6B1 32F8DB60
        FE67DA3A 1D15AB85 DA31DF90 1723BF4E CFA16FC4 FF3D23EA
        4D2BA5EE 8EE0108C E80B828E 33B6C2B5 B17CEC70 98FD2803


  reseed_counter is
                                                 0000 00000003
```

```
rnd_val is
        938BAB9C 357B9023 92AEFA66 8DFDB88C 9C671FC0 220ED319
        7F852B3B 9C27AD33 D99403E6 56510F77 E964130B 284759A0
        EB42F933 E6B2D170 99744089 402ED23B C8C0CAD5 9BA485A9
        04B5456E 4EFEFC22 9415778F 50957FDD B559C053 FB97CE79


################################################################

Hash_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                  20212223 24252627 28292A2B
```

PersonalizationString =
404142 43444546 4748494A 4B4C4D4E
4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE

AdditionalInput1 =
606162 63646566 6768696A 6B6C6D6E
6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE

AdditionalInput2 =
A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E

##

****

Hash_DRBG_Instantiate_algorithm

entropy_input is
000102 03040506 0708090A 0B0C0D0E
0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E

nonce is
20212223 24252627 28292A2B

personal_str is
404142 43444546 4748494A 4B4C4D4E
4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E

```
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "No PredictionResistance"

--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                    0001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
          010000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    Hash(counter||no_of_bits_to_return||input_string) is
        A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
        EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964
```

```
temp =
    A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
    EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964


------------

i = 2

counter||no_of_bits_to_return||input_string is
      020000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
    C74754B6 A1E77C6C 0DE0245E 3BC81E15 85F2F379 F4489643
    5F61C23D B552DB8B 3190F5F3 7B966F3D D000CEB5 373CA2BD


temp =
    A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
    EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964
    C74754B6 A1E77C6C 0DE0245E 3BC81E15 85F2F379 F4489643
    5F61C23D B552DB8B 3190F5F3 7B966F3D D000CEB5 373CA2BD


------------

i = 3

counter||no_of_bits_to_return||input_string is
      030000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
```

```
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    Hash(counter||no_of_bits_to_return||input_string) is
        A8989587 CED14C8E 80790CD7 146F3328 3D84860A 708750EA
        1FDCD1DA D814E76A CA6E310F 12AA0BBA 611A8E86 FC0EAE47


    temp =
                            A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


  V is
                            A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
```

```
          01 00000378 00A028F8 43783D77 21E32AC5 FD923031
    884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
    C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
    1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
    3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


Hash(counter||no_of_bits_to_return||input_string) is
    DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
    273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D


temp =
    DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
    273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 00A028F8 43783D77 21E32AC5 FD923031
    884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
    C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
    1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
    3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


Hash(counter||no_of_bits_to_return||input_string) is
    7B72F966 9A700AF1 C7E3466A 5E89A0DC A45282E7 1A39E4AA
    24585736 11785015 85B95258 C40A2016 2D1F62CA 988BBEC7


temp =
    DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
    273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D
    7B72F966 9A700AF1 C7E3466A 5E89A0DC A45282E7 1A39E4AA
    24585736 11785015 85B95258 C40A2016 2D1F62CA 988BBEC7


------------

i = 3

counter||no_of_bits_to_return||input_string is
```

```
              03 00000378 00A028F8 43783D77 21E32AC5 FD923031
         884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
         C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
         1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
         3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


    Hash(counter||no_of_bits_to_return||input_string) is
         FD2CAD8E 501A9FA7 18212A41 9FA2251F 01E46C40 DDBF4D85
         223B6E11 48351858 CC99BE10 6D1A4301 A307DBAF DE079ADA


    temp =
                             DE0424 3D3BB302 329A9112 4D780ADC
         F3672DDD 2CE78196 3E273BB2 49F6EC13 B16A903F 40D01C2D
         FF1464BF A6AFD698 7D7B72F9 669A700A F1C7E346 6A5E89A0
         DCA45282 E71A39E4 AA245857 36117850 1585B952 58C40A20
         162D1F62 CA988BBE C7FD2CAD 8E501A9F A718212A 419FA225


  C is
                             DE0424 3D3BB302 329A9112 4D780ADC
         F3672DDD 2CE78196 3E273BB2 49F6EC13 B16A903F 40D01C2D
         FF1464BF A6AFD698 7D7B72F9 669A700A F1C7E346 6A5E89A0
         DCA45282 E71A39E4 AA245857 36117850 1585B952 58C40A20
         162D1F62 CA988BBE C7FD2CAD 8E501A9F A718212A 419FA225


----------------------------------------------------------------

First call to Generate

****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input
                             606162 63646566 6768696A 6B6C6D6E
         6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
         8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
         9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
         B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

```
---------------------------

  Process additional_input

    0x02||V||additional_input is
                                                 02A028 F843783D
        7721E32A C5FD9230 31884CF9 D3F05FA2 BE09EB6A 82C782B6
        203C2938 47B98EC4 B9C0C867 4DEAE09E B964C747 54B6A1E7
        7C6C0DE0 245E3BC8 1E1585F2 F379F448 96435F61 C23DB552
        DB8B3190 F5F37B96 6F3DD000 CEB5373C A2BDA898 9587CED1
        4C8E8079 0CD7146F 33606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    w=Hash(0x02||V||additional_input) is
        89F101CF 9C3005E9 178BAD96 C069CF25 6FBB31FE A611220F
        860F6C0F CB4FE568 467A6238 53376C6D E4820FAE 06692A95


    V is
                            A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        9F76F4C3 16244E7F 5AEB0F58 FE1F2200 FAECC2F4 998CB87E
        C3DF6CDE 8087220B 0422FACD DB063DBA 730288BA DD7D99C8


---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                            A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        9F76F4C3 16244E7F 5AEB0F58 FE1F2200 FAECC2F4 998CB87E
        C3DF6CDE 8087220B 0422FACD DB063DBA 730288BA DD7D99C8
```

```
    w_i is
        5C0EDEEE 4E8060FE D022020C 83882E71 61F16100 9CCBC827
        E557091D 3FA172D8 E6EDFFB1 B4315D94 2448C8C5 42314E5C


    W is
        5C0EDEEE 4E8060FE D022020C 83882E71 61F16100 9CCBC827
        E557091D 3FA172D8 E6EDFFB1 B4315D94 2448C8C5 42314E5C


    ------------

    i = 2

    data is
                            A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        9F76F4C3 16244E7F 5AEB0F58 FE1F2200 FAECC2F4 998CB87E
        C3DF6CDE 8087220B 0422FACD DB063DBA 730288BA DD7D99C9


    w_i is
        F64BF9EE 10033D70 6BE38685 D3CA639A 14D54D3F 2877472E
        90794E29 BCD6E5EC A890E217 C7CA56A0 58113C6C 6483E455


    W is
        5C0EDEEE 4E8060FE D022020C 83882E71 61F16100 9CCBC827
        E557091D 3FA172D8 E6EDFFB1 B4315D94 2448C8C5 42314E5C
        F64BF9EE 10033D70 6BE38685 D3CA639A 14D54D3F 2877472E
        90794E29 BCD6E5EC A890E217 C7CA56A0 58113C6C 6483E455


  returned_bits is
        5C0EDEEE 4E8060FE D022020C 83882E71 61F16100 9CCBC827
        E557091D 3FA172D8 E6EDFFB1 B4315D94 2448C8C5 42314E5C
        F64BF9EE 10033D70 6BE38685 D3CA639A 14D54D3F 2877472E
        90794E29 BCD6E5EC A890E217 C7CA56A0 58113C6C 6483E455


--------------------------

  Update V
```

```
    0x03||V is
                          03A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        9F76F4C3 16244E7F 5AEB0F58 FE1F2200 FAECC2F4 998CB87E
        C3DF6CDE 8087220B 0422FACD DB063DBA 730288BA DD7D99C8


    H is
        3A9852A9 482B8F08 D0AA4A59 8938647C 53958EDE D90D362B
        29AABCC3 0CFE18A1 82DB77D5 35BC98E7 CE6132F1 6A11FBE2


  Updated values

  V is
                            7E2D1C 80B3F079 547DBBD8 4B0A3B0E
        7BB427B1 1D472454 4812A635 1179A233 ED93C886 FA5EE0E7
        BFDCCC0D 91907551 E242BA4E 1D3C5787 5DD5C36A C89A51BF
        B6B399EF 456A176C D5B9B209 BD68FECD 64080B25 CB5DF8CA
        03B74904 581DC66B 4EFB9F50 9F12F141 E87BDCD6 892F37D0


  reseed_counter is
                                                0000 00000002


rnd_val is
        5C0EDEEE 4E8060FE D022020C 83882E71 61F16100 9CCBC827
        E557091D 3FA172D8 E6EDFFB1 B4315D94 2448C8C5 42314E5C
        F64BF9EE 10033D70 6BE38685 D3CA639A 14D54D3F 2877472E
        90794E29 BCD6E5EC A890E217 C7CA56A0 58113C6C 6483E455


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number__of_bits = 768

  additional_input
```

```
                          A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


---------------------------

  Process additional_input

    0x02||V||additional_input is
                                              027E2D 1C80B3F0
        79547DBB D84B0A3B 0E7BB427 B11D4724 544812A6 351179A2
        33ED93C8 86FA5EE0 E7BFDCCC 0D919075 51E242BA 4E1D3C57
        875DD5C3 6AC89A51 BFB6B399 EF456A17 6CD5B9B2 09BD68FE
        CD64080B 25CB5DF8 CA03B749 04581DC6 6B4EFB9F 509F12F1
        41E87BDC D6892F37 D0A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    w=Hash(0x02||V||additional_input) is
        F8B39FAA C0A147A4 FB8A4344 6EA54F62 1417A1E4 06A73BF5
        6BAF2965 1A4278CD 051C2AA4 5ED0E030 01481C22 8EC4D71F


    V is
                          7E2D1C 80B3F079 547DBBD8 4B0A3B0E
        7BB427B1 1D472454 4812A635 1179A233 ED93C886 FA5EE0E7
        BFDCCC0D 91907551 E242BA4E 1D3C5787 5DD5C36A C89A51C0
        AF67399A 060B5F11 D143F54E 2C0E4E2F 781FAD09 D20534BF
        6F667269 72603F38 5417C9F4 FDE3D171 E9C3F8F9 17F40EEF


---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1
```

```
  data is
                          7E2D1C 80B3F079 547DBBD8 4B0A3B0E
      7BB427B1 1D472454 4812A635 1179A233 ED93C886 FA5EE0E7
      BFDCCC0D 91907551 E242BA4E 1D3C5787 5DD5C36A C89A51C0
      AF67399A 060B5F11 D143F54E 2C0E4E2F 781FAD09 D20534BF
      6F667269 72603F38 5417C9F4 FDE3D171 E9C3F8F9 17F40EEF


  w_i is
      C80CAED7 81EF9B2A 31E2138F C4461243 6D992B6B EDFBBC82
      EEA943ED 49209F36 E0AE25F4 ED5FBA96 BE0357F1 64964D32


  W is
      C80CAED7 81EF9B2A 31E2138F C4461243 6D992B6B EDFBBC82
      EEA943ED 49209F36 E0AE25F4 ED5FBA96 BE0357F1 64964D32


  ------------

  i = 2

  data is
                          7E2D1C 80B3F079 547DBBD8 4B0A3B0E
      7BB427B1 1D472454 4812A635 1179A233 ED93C886 FA5EE0E7
      BFDCCC0D 91907551 E242BA4E 1D3C5787 5DD5C36A C89A51C0
      AF67399A 060B5F11 D143F54E 2C0E4E2F 781FAD09 D20534BF
      6F667269 72603F38 5417C9F4 FDE3D171 E9C3F8F9 17F40EF0


  w_i is
      267F5736 6C89A1B0 CFE86D02 5CA1E21D 14F0B4C0 998DADF4
      684BFB21 18F82241 3D87693C B99AC0B5 9D5E0494 BF74293B


  W is
      C80CAED7 81EF9B2A 31E2138F C4461243 6D992B6B EDFBBC82
      EEA943ED 49209F36 E0AE25F4 ED5FBA96 BE0357F1 64964D32
      267F5736 6C89A1B0 CFE86D02 5CA1E21D 14F0B4C0 998DADF4
      684BFB21 18F82241 3D87693C B99AC0B5 9D5E0494 BF74293B


returned_bits is
      C80CAED7 81EF9B2A 31E2138F C4461243 6D992B6B EDFBBC82
      EEA943ED 49209F36 E0AE25F4 ED5FBA96 BE0357F1 64964D32
```

```
        267F5736 6C89A1B0 CFE86D02 5CA1E21D 14F0B4C0 998DADF4
        684BFB21 18F82241 3D87693C B99AC0B5 9D5E0494 BF74293B


---------------------------

  Update V

    0x03||V is
                         037E2D1C 80B3F079 547DBBD8 4B0A3B0E
        7BB427B1 1D472454 4812A635 1179A233 ED93C886 FA5EE0E7
        BFDCCC0D 91907551 E242BA4E 1D3C5787 5DD5C36A C89A51C0
        AF67399A 060B5F11 D143F54E 2C0E4E2F 781FAD09 D20534BF
        6F667269 72603F38 5417C9F4 FDE3D171 E9C3F8F9 17F40EEF


    H is
        A9EE2234 CE80829B C041F6C6 6767C640 A755BC7E 1448E311
        BE81C684 5FD345ED FD46BBFB 374CBCCC E2CB1C30 A03D0E44


  Updated values

  V is
                           5C3140 BDEFA37B 87184CEA 988245EB
        6F1B558E 4A2EA5EA 8639E1E7 5B708E47 9EFE58C6 3B2EFD15
        BEF130CD 38404BEA 5FBE2D47 83D6C792 4F9DA6B1 32F8DB62
        35F9AE51 BBA61B92 3BAA446B C9878CC0 34FB22DA 3F1221F1
        44155850 9CCC10E5 195BB29D C380A8DE 73A73653 F9D0BF5A


  reseed_counter is
                                                0000 00000003


rnd_val is
        C80CAED7 81EF9B2A 31E2138F C4461243 6D992B6B EDFBBC82
        EEA943ED 49209F36 E0AE25F4 ED5FBA96 BE0357F1 64964D32
        267F5736 6C89A1B0 CFE86D02 5CA1E21D 14F0B4C0 998DADF4
        684BFB21 18F82241 3D87693C B99AC0B5 9D5E0494 BF74293B


##############################################################

Hash_DRBG
```

```
    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                   20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
```

```
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                   20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                          000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
        63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                               01000003 78000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
        63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


    Hash(counter||no_of_bits_to_return||input_string) is
        703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
        FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4
```

```
temp =
    703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
    FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                          02000003 78000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


Hash(counter||no_of_bits_to_return||input_string) is
    31487080 FDE0B521 DEBCFC5A AB9D39DA D9466C24 D4498964
    E4E318D4 DC777C22 A0EEE9B5 79B281AE 6AEB18B0 28D5C99A


temp =
    703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
    FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4
    31487080 FDE0B521 DEBCFC5A AB9D39DA D9466C24 D4498964
    E4E318D4 DC777C22 A0EEE9B5 79B281AE 6AEB18B0 28D5C99A


------------

i = 3

counter||no_of_bits_to_return||input_string is
                                          03000003 78000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


Hash(counter||no_of_bits_to_return||input_string) is
    9B71197A 30150000 F1E5B6AD 1EB81AB2 7B8E19BE 185E4F70
    61F1D3CA 9B3A0DF4 FD597962 C2070B7E B064B31F 4F3E10BD
```

```
    temp =
                            703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


  V is
                            703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           00703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


    Hash(counter||no_of_bits_to_return||input_string) is
        805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
```

```
    DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009


temp =
    805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
    DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 00703AEC B83762E8 855BF167 2A52FAEF
    5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
    FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
    DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
    AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


Hash(counter||no_of_bits_to_return||input_string) is
    424E5B0A BDF33FBB 5C02CA64 3A5753A2 4ED17561 9251B4E0
    89DACFDA C1CD8989 CF0F87B9 197E7BEF D8550312 538A89B9


temp =
    805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
    DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009
    424E5B0A BDF33FBB 5C02CA64 3A5753A2 4ED17561 9251B4E0
    89DACFDA C1CD8989 CF0F87B9 197E7BEF D8550312 538A89B9


------------

i = 3

counter||no_of_bits_to_return||input_string is
          03 00000378 00703AEC B83762E8 855BF167 2A52FAEF
    5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
    FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
    DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
    AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


Hash(counter||no_of_bits_to_return||input_string) is
    55F0BF84 2C6BF212 18612101 CB0E1A06 0E2E9C66 5E87E1BA
```

```
        9632F01B 4CF80D08 C9645BD1 830112EA 6EBFED69 A48CA9C9


    temp =
                            805F3E 8A9A40AA EE585729 8729B9CF
        5187C6DD BB443A05 D3DFF4C7 F2053B3C BE34E9B1 9763329E
        7CCE8806 8B1DD2C0 09424E5B 0ABDF33F BB5C02CA 643A5753
        A24ED175 619251B4 E089DACF DAC1CD89 89CF0F87 B9197E7B
        EFD85503 12538A89 B955F0BF 842C6BF2 12186121 01CB0E1A


  C is
                            805F3E 8A9A40AA EE585729 8729B9CF
        5187C6DD BB443A05 D3DFF4C7 F2053B3C BE34E9B1 9763329E
        7CCE8806 8B1DD2C0 09424E5B 0ABDF33F BB5C02CA 643A5753
        A24ED175 619251B4 E089DACF DAC1CD89 89CF0F87 B9197E7B
        EFD85503 12538A89 B955F0BF 842C6BF2 12186121 01CB0E1A


---------------------------------------------------------------

First call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

Generate FAILED: Reseed is required
---------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  additional_input <empty>
```

```
--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                 01703A ECB83762
        E8855BF1 672A52FA EF5C7B5C 83E893D0 0130FEC6 3C9AC5F5
        3F23230D 5CCE766D 09FFF0DA C417C889 2FC43148 7080FDE0
        B521DEBC FC5AAB9D 39DAD946 6C24D449 8964E4E3 18D4DC77
        7C22A0EE E9B579B2 81AE6AEB 18B028D5 C99A9B71 197A3015
        0000F1E5 B6AD1EB8 1A808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                  01000003 7801703A ECB83762
        E8855BF1 672A52FA EF5C7B5C 83E893D0 0130FEC6 3C9AC5F5
        3F23230D 5CCE766D 09FFF0DA C417C889 2FC43148 7080FDE0
        B521DEBC FC5AAB9D 39DAD946 6C24D449 8964E4E3 18D4DC77
        7C22A0EE E9B579B2 81AE6AEB 18B028D5 C99A9B71 197A3015
        0000F1E5 B6AD1EB8 1A808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    Hash(counter||no_of_bits_to_return||input_string) is
        7E5DAD76 6ACF7AAF B519AACA 20DDE991 7C71518B 26AA4D22
        59D74355 01D36678 FAC6ED03 02D6CB58 19B41DE1 BE37D52F


    temp =
        7E5DAD76 6ACF7AAF B519AACA 20DDE991 7C71518B 26AA4D22
        59D74355 01D36678 FAC6ED03 02D6CB58 19B41DE1 BE37D52F
```

```
------------

i = 2

counter||no_of_bits_to_return||input_string is
                                02000003 7801703A ECB83762
    E8855BF1 672A52FA EF5C7B5C 83E893D0 0130FEC6 3C9AC5F5
    3F23230D 5CCE766D 09FFF0DA C417C889 2FC43148 7080FDE0
    B521DEBC FC5AAB9D 39DAD946 6C24D449 8964E4E3 18D4DC77
    7C22A0EE E9B579B2 81AE6AEB 18B028D5 C99A9B71 197A3015
    0000F1E5 B6AD1EB8 1A808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


Hash(counter||no_of_bits_to_return||input_string) is
    4CF663DE 1206F3E7 155A77DE CCD25928 52C5ABC0 5E965EEF
    D9A037B8 0F543BDE 841A2995 17DD59E4 D2B94266 688FCAE8


temp =
    7E5DAD76 6ACF7AAF B519AACA 20DDE991 7C71518B 26AA4D22
    59D74355 01D36678 FAC6ED03 02D6CB58 19B41DE1 BE37D52F
    4CF663DE 1206F3E7 155A77DE CCD25928 52C5ABC0 5E965EEF
    D9A037B8 0F543BDE 841A2995 17DD59E4 D2B94266 688FCAE8


------------

i = 3

counter||no_of_bits_to_return||input_string is
                                03000003 7801703A ECB83762
    E8855BF1 672A52FA EF5C7B5C 83E893D0 0130FEC6 3C9AC5F5
    3F23230D 5CCE766D 09FFF0DA C417C889 2FC43148 7080FDE0
    B521DEBC FC5AAB9D 39DAD946 6C24D449 8964E4E3 18D4DC77
    7C22A0EE E9B579B2 81AE6AEB 18B028D5 C99A9B71 197A3015
    0000F1E5 B6AD1EB8 1A808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
        0FE80879 F630AC0C 8AD29B88 CE04BA06 1205867D E4370C70
        8EA1D26A AA5404A5 BDEC5A21 D4C67A06 0E1EEC9B 3DAE4D5A


    temp =
                            7E5DAD 766ACF7A AFB519AA CA20DDE9
        917C7151 8B26AA4D 2259D743 5501D366 78FAC6ED 0302D6CB
        5819B41D E1BE37D5 2F4CF663 DE1206F3 E7155A77 DECCD259
        2852C5AB C05E965E EFD9A037 B80F543B DE841A29 9517DD59
        E4D2B942 66688FCA E80FE808 79F630AC 0C8AD29B 88CE04BA


  V is
                            7E5DAD 766ACF7A AFB519AA CA20DDE9
        917C7151 8B26AA4D 2259D743 5501D366 78FAC6ED 0302D6CB
        5819B41D E1BE37D5 2F4CF663 DE1206F3 E7155A77 DECCD259
        2852C5AB C05E965E EFD9A037 B80F543B DE841A29 9517DD59
        E4D2B942 66688FCA E80FE808 79F630AC 0C8AD29B 88CE04BA


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           007E5DAD 766ACF7A AFB519AA CA20DDE9
        917C7151 8B26AA4D 2259D743 5501D366 78FAC6ED 0302D6CB
        5819B41D E1BE37D5 2F4CF663 DE1206F3 E7155A77 DECCD259
        2852C5AB C05E965E EFD9A037 B80F543B DE841A29 9517DD59
        E4D2B942 66688FCA E80FE808 79F630AC 0C8AD29B 88CE04BA


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 007E5DAD 766ACF7A AFB519AA CA20DDE9
        917C7151 8B26AA4D 2259D743 5501D366 78FAC6ED 0302D6CB
        5819B41D E1BE37D5 2F4CF663 DE1206F3 E7155A77 DECCD259
        2852C5AB C05E965E EFD9A037 B80F543B DE841A29 9517DD59
        E4D2B942 66688FCA E80FE808 79F630AC 0C8AD29B 88CE04BA
```

```
Hash(counter||no_of_bits_to_return||input_string) is
    0FAEFA23 5A4B132C 0E1FE14C DFBF3B74 CB7AA766 5ADE588A
    A944BD29 0A544B1A 51D131B6 FE18970F ED180A8A 6F20FEB1


temp =
    0FAEFA23 5A4B132C 0E1FE14C DFBF3B74 CB7AA766 5ADE588A
    A944BD29 0A544B1A 51D131B6 FE18970F ED180A8A 6F20FEB1


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 007E5DAD 766ACF7A AFB519AA CA20DDE9
    917C7151 8B26AA4D 2259D743 5501D366 78FAC6ED 0302D6CB
    5819B41D E1BE37D5 2F4CF663 DE1206F3 E7155A77 DECCD259
    2852C5AB C05E965E EFD9A037 B80F543B DE841A29 9517DD59
    E4D2B942 66688FCA E80FE808 79F630AC 0C8AD29B 88CE04BA


Hash(counter||no_of_bits_to_return||input_string) is
    DC4E2903 A842F51D 513F106E D4C52B41 5C888415 720628B2
    BE042776 1EC657E4 A5732C05 F47EBEF6 9942E47D E7387959


temp =
    0FAEFA23 5A4B132C 0E1FE14C DFBF3B74 CB7AA766 5ADE588A
    A944BD29 0A544B1A 51D131B6 FE18970F ED180A8A 6F20FEB1
    DC4E2903 A842F51D 513F106E D4C52B41 5C888415 720628B2
    BE042776 1EC657E4 A5732C05 F47EBEF6 9942E47D E7387959


------------

i = 3

counter||no_of_bits_to_return||input_string is
          03 00000378 007E5DAD 766ACF7A AFB519AA CA20DDE9
    917C7151 8B26AA4D 2259D743 5501D366 78FAC6ED 0302D6CB
    5819B41D E1BE37D5 2F4CF663 DE1206F3 E7155A77 DECCD259
    2852C5AB C05E965E EFD9A037 B80F543B DE841A29 9517DD59
    E4D2B942 66688FCA E80FE808 79F630AC 0C8AD29B 88CE04BA
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
        DBA8857F B0CCCB33 CDC1F142 FB0E0826 309E9715 1671A68D
        A86CADA4 55F42B5F D57762B9 43CCDEF3 856B0F59 CE548570


    temp =
                            0FAEFA 235A4B13 2C0E1FE1 4CDFBF3B
        74CB7AA7 665ADE58 8AA944BD 290A544B 1A51D131 B6FE1897
        0FED180A 8A6F20FE B1DC4E29 03A842F5 1D513F10 6ED4C52B
        415C8884 15720628 B2BE0427 761EC657 E4A5732C 05F47EBE
        F69942E4 7DE73879 59DBA885 7FB0CCCB 33CDC1F1 42FB0E08


  C is
                            0FAEFA 235A4B13 2C0E1FE1 4CDFBF3B
        74CB7AA7 665ADE58 8AA944BD 290A544B 1A51D131 B6FE1897
        0FED180A 8A6F20FE B1DC4E29 03A842F5 1D513F10 6ED4C52B
        415C8884 15720628 B2BE0427 761EC657 E4A5732C 05F47EBE
        F69942E4 7DE73879 59DBA885 7FB0CCCB 33CDC1F1 42FB0E08


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                            7E5DAD 766ACF7A AFB519AA CA20DDE9
        917C7151 8B26AA4D 2259D743 5501D366 78FAC6ED 0302D6CB
        5819B41D E1BE37D5 2F4CF663 DE1206F3 E7155A77 DECCD259
        2852C5AB C05E965E EFD9A037 B80F543B DE841A29 9517DD59
        E4D2B942 66688FCA E80FE808 79F630AC 0C8AD29B 88CE04BA
```

```
    w_i is
        97993B78 F7C31C0E 876DC92E B7D6C408 E09D608A D6B99D0E
        A2229B05 A578C426 334FCC8A 1C7E676E D2D89A5B 4CDF5B3F


    W is
        97993B78 F7C31C0E 876DC92E B7D6C408 E09D608A D6B99D0E
        A2229B05 A578C426 334FCC8A 1C7E676E D2D89A5B 4CDF5B3F


    ------------

    i = 2

    data is
                            7E5DAD 766ACF7A AFB519AA CA20DDE9
        917C7151 8B26AA4D 2259D743 5501D366 78FAC6ED 0302D6CB
        5819B41D E1BE37D5 2F4CF663 DE1206F3 E7155A77 DECCD259
        2852C5AB C05E965E EFD9A037 B80F543B DE841A29 9517DD59
        E4D2B942 66688FCA E80FE808 79F630AC 0C8AD29B 88CE04BB


    w_i is
        4ADF1193 6BF14F4E 10909DBA 9C24F4FD FFDE7235 1DA8E2CC
        3B135A39 5373899E 5F1A5955 B880CA9B 9E9DD4C9 CA7FA4D4


    W is
        97993B78 F7C31C0E 876DC92E B7D6C408 E09D608A D6B99D0E
        A2229B05 A578C426 334FCC8A 1C7E676E D2D89A5B 4CDF5B3F
        4ADF1193 6BF14F4E 10909DBA 9C24F4FD FFDE7235 1DA8E2CC
        3B135A39 5373899E 5F1A5955 B880CA9B 9E9DD4C9 CA7FA4D4


  returned_bits is
        97993B78 F7C31C0E 876DC92E B7D6C408 E09D608A D6B99D0E
        A2229B05 A578C426 334FCC8A 1C7E676E D2D89A5B 4CDF5B3F
        4ADF1193 6BF14F4E 10909DBA 9C24F4FD FFDE7235 1DA8E2CC
        3B135A39 5373899E 5F1A5955 B880CA9B 9E9DD4C9 CA7FA4D4


--------------------------

  Update V
```

```
    0x03||V is
                          037E5DAD 766ACF7A AFB519AA CA20DDE9
        917C7151 8B26AA4D 2259D743 5501D366 78FAC6ED 0302D6CB
        5819B41D E1BE37D5 2F4CF663 DE1206F3 E7155A77 DECCD259
        2852C5AB C05E965E EFD9A037 B80F543B DE841A29 9517DD59
        E4D2B942 66688FCA E80FE808 79F630AC 0C8AD29B 88CE04BA


    H is
        2470C998 B8CD701E 9BE7C781 35CD4AE1 16A1A45F B5201E46
        44F1EDA5 21397674 22F94411 88315066 971E8650 94367968


  Updated values

  V is
                            8E0CA7 99C51A8D DBC3398C 17009D25
        0647EBF8 F18188A5 AD031C00 7E0C27B1 934C981E BA00EF62
        6806CC28 6C2D58D3 E129448C E1BA49E9 04669988 4DA19784
        8E2017C8 8E9E0CA6 3E7F6BE0 63FB6574 D9CB31B5 502C7A5F
        205DE9CC 05893EB8 64E4D49F 81D84DDD D7771ADD 5FFF8C2B


  reseed_counter is
                                                0000 00000002


rnd_val is
        97993B78 F7C31C0E 876DC92E B7D6C408 E09D608A D6B99D0E
        A2229B05 A578C426 334FCC8A 1C7E676E D2D89A5B 4CDF5B3F
        4ADF1193 6BF14F4E 10909DBA 9C24F4FD FFDE7235 1DA8E2CC
        3B135A39 5373899E 5F1A5955 B880CA9B 9E9DD4C9 CA7FA4D4


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>
```

```
Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                              018E0C A799C51A
        8DDBC339 8C17009D 250647EB F8F18188 A5AD031C 007E0C27
        B1934C98 1EBA00EF 626806CC 286C2D58 D3E12944 8CE1BA49
        E9046699 884DA197 848E2017 C88E9E0C A63E7F6B E063FB65
        74D9CB31 B5502C7A 5F205DE9 CC05893E B864E4D4 9F81D84D
        DDD7771A DD5FFF8C 2BC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                   01000003 78018E0C A799C51A
        8DDBC339 8C17009D 250647EB F8F18188 A5AD031C 007E0C27
        B1934C98 1EBA00EF 626806CC 286C2D58 D3E12944 8CE1BA49
        E9046699 884DA197 848E2017 C88E9E0C A63E7F6B E063FB65
        74D9CB31 B5502C7A 5F205DE9 CC05893E B864E4D4 9F81D84D
        DDD7771A DD5FFF8C 2BC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

```
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Hash(counter||no_of_bits_to_return||input_string) is
    3B501497 7E9BEF76 896882A3 74700D0F 005EC2B8 1A3DDC55
    40ACD3E9 F977A973 EEA7CFFB 39723992 3A1AA7B0 46237084


temp =
    3B501497 7E9BEF76 896882A3 74700D0F 005EC2B8 1A3DDC55
    40ACD3E9 F977A973 EEA7CFFB 39723992 3A1AA7B0 46237084


------------

i = 2

counter||no_of_bits_to_return||input_string is
                              02000003 78018E0C A799C51A
    8DDBC339 8C17009D 250647EB F8F18188 A5AD031C 007E0C27
    B1934C98 1EBA00EF 626806CC 286C2D58 D3E12944 8CE1BA49
    E9046699 884DA197 848E2017 C88E9E0C A63E7F6B E063FB65
    74D9CB31 B5502C7A 5F205DE9 CC05893E B864E4D4 9F81D84D
    DDD7771A DD5FFF8C 2BC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Hash(counter||no_of_bits_to_return||input_string) is
    E969AA92 E830907F F9539E22 3F819AB5 9BF925D9 29F358E0
    BD65668D B0D6435F 36231B96 24DC29B9 6E5F31AE 187179FF


temp =
    3B501497 7E9BEF76 896882A3 74700D0F 005EC2B8 1A3DDC55
    40ACD3E9 F977A973 EEA7CFFB 39723992 3A1AA7B0 46237084
    E969AA92 E830907F F9539E22 3F819AB5 9BF925D9 29F358E0
    BD65668D B0D6435F 36231B96 24DC29B9 6E5F31AE 187179FF


------------
```

```
    i = 3

    counter||no_of_bits_to_return||input_string is
                                    03000003 78018E0C A799C51A
        8DDBC339 8C17009D 250647EB F8F18188 A5AD031C 007E0C27
        B1934C98 1EBA00EF 626806CC 286C2D58 D3E12944 8CE1BA49
        E9046699 884DA197 848E2017 C88E9E0C A63E7F6B E063FB65
        74D9CB31 B5502C7A 5F205DE9 CC05893E B864E4D4 9F81D84D
        DDD7771A DD5FFF8C 2BC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Hash(counter||no_of_bits_to_return||input_string) is
        C683593C 29EAC84F FA3A7080 00F693AE 7D74F667 BFE35F02
        5339D960 956FD38D 73940468 762FF5D2 DA586BF0 7E493167


    temp =
                            3B5014 977E9BEF 76896882 A374700D
        0F005EC2 B81A3DDC 5540ACD3 E9F977A9 73EEA7CF FB397239
        923A1AA7 B0462370 84E969AA 92E83090 7FF9539E 223F819A
        B59BF925 D929F358 E0BD6566 8DB0D643 5F36231B 9624DC29
        B96E5F31 AE187179 FFC68359 3C29EAC8 4FFA3A70 8000F693


  V is
                            3B5014 977E9BEF 76896882 A374700D
        0F005EC2 B81A3DDC 5540ACD3 E9F977A9 73EEA7CF FB397239
        923A1AA7 B0462370 84E969AA 92E83090 7FF9539E 223F819A
        B59BF925 D929F358 E0BD6566 8DB0D643 5F36231B 9624DC29
        B96E5F31 AE187179 FFC68359 3C29EAC8 4FFA3A70 8000F693


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           003B5014 977E9BEF 76896882 A374700D
        0F005EC2 B81A3DDC 5540ACD3 E9F977A9 73EEA7CF FB397239
        923A1AA7 B0462370 84E969AA 92E83090 7FF9539E 223F819A
        B59BF925 D929F358 E0BD6566 8DB0D643 5F36231B 9624DC29
```

```
    B96E5F31 AE187179 FFC68359 3C29EAC8 4FFA3A70 8000F693


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
          01 00000378 003B5014 977E9BEF 76896882 A374700D
    0F005EC2 B81A3DDC 5540ACD3 E9F977A9 73EEA7CF FB397239
    923A1AA7 B0462370 84E969AA 92E83090 7FF9539E 223F819A
    B59BF925 D929F358 E0BD6566 8DB0D643 5F36231B 9624DC29
    B96E5F31 AE187179 FFC68359 3C29EAC8 4FFA3A70 8000F693


Hash(counter||no_of_bits_to_return||input_string) is
    8D07901B B7A8BF92 96741892 EC320FD3 25277543 ADA4C852
    E958037A D711C4D9 5F27E87C CAB1CB05 BE2EDFF3 8D929EDC


temp =
    8D07901B B7A8BF92 96741892 EC320FD3 25277543 ADA4C852
    E958037A D711C4D9 5F27E87C CAB1CB05 BE2EDFF3 8D929EDC


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 003B5014 977E9BEF 76896882 A374700D
    0F005EC2 B81A3DDC 5540ACD3 E9F977A9 73EEA7CF FB397239
    923A1AA7 B0462370 84E969AA 92E83090 7FF9539E 223F819A
    B59BF925 D929F358 E0BD6566 8DB0D643 5F36231B 9624DC29
    B96E5F31 AE187179 FFC68359 3C29EAC8 4FFA3A70 8000F693


Hash(counter||no_of_bits_to_return||input_string) is
    5E81C2BB 672FB37F F264402F A005D14E D6A38D76 491E9A82
    EEB01A7B 24138027 EC192B21 B111323C 5AD635D8 A291F3CA


temp =
    8D07901B B7A8BF92 96741892 EC320FD3 25277543 ADA4C852
```

E958037A D711C4D9 5F27E87C CAB1CB05 BE2EDFF3 8D929EDC
E81C2BB 672FB37F F264402F A005D14E D6A38D76 491E9A82
EEB01A7B 24138027 EC192B21 B111323C 5AD635D8 A291F3CA

---

i = 3

counter||no_of_bits_to_return||input_string is
03 00000378 003B5014 977E9BEF 76896882 A374700D
0F005EC2 B81A3DDC 5540ACD3 E9F977A9 73EEA7CF FB397239
923A1AA7 B0462370 84E969AA 92E83090 7FF9539E 223F819A
B59BF925 D929F358 E0BD6566 8DB0D643 5F36231B 9624DC29
B96E5F31 AE187179 FFC68359 3C29EAC8 4FFA3A70 8000F693

Hash(counter||no_of_bits_to_return||input_string) is
EA30D4CA 4A632217 75764E63 C166E12B 110EA234 149CA55C
2691229B E6BBB238 FACF8924 ACB5F9F8 96FD5264 A2F46BE2

temp =
8D0790 1BB7A8BF 92967418 92EC320F
D3252775 43ADA4C8 52E95803 7AD711C4 D95F27E8 7CCAB1CB
05BE2EDF F38D929E DC5E81C2 BB672FB3 7FF26440 2FA005D1
4ED6A38D 76491E9A 82EEB01A 7B241380 27EC192B 21B11132
3C5AD635 D8A291F3 CAEA30D4 CA4A6322 1775764E 63C166E1

C is
8D0790 1BB7A8BF 92967418 92EC320F
D3252775 43ADA4C8 52E95803 7AD711C4 D95F27E8 7CCAB1CB
05BE2EDF F38D929E DC5E81C2 BB672FB3 7FF26440 2FA005D1
4ED6A38D 76491E9A 82EEB01A 7B241380 27EC192B 21B11132
3C5AD635 D8A291F3 CAEA30D4 CA4A6322 1775764E 63C166E1

****

Hash_DRBG_Generate_algorithm

requested_number_of_bits = 768

additional_input <empty>

```
---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                            3B5014 977E9BEF 76896882 A374700D
        0F005EC2 B81A3DDC 5540ACD3 E9F977A9 73EEA7CF FB397239
        923A1AA7 B0462370 84E969AA 92E83090 7FF9539E 223F819A
        B59BF925 D929F358 E0BD6566 8DB0D643 5F36231B 9624DC29
        B96E5F31 AE187179 FFC68359 3C29EAC8 4FFA3A70 8000F693


    w_i is
        F5983946 320E36C6 4EF283CA 1F65D197 CF81624E C6778E77
        0E78949D 84EF21A4 5CDD62D1 DB76920D 4C2836FC 6AE5299F


    W is
        F5983946 320E36C6 4EF283CA 1F65D197 CF81624E C6778E77
        0E78949D 84EF21A4 5CDD62D1 DB76920D 4C2836FC 6AE5299F


    ------------

    i = 2

    data is
                            3B5014 977E9BEF 76896882 A374700D
        0F005EC2 B81A3DDC 5540ACD3 E9F977A9 73EEA7CF FB397239
        923A1AA7 B0462370 84E969AA 92E83090 7FF9539E 223F819A
        B59BF925 D929F358 E0BD6566 8DB0D643 5F36231B 9624DC29
        B96E5F31 AE187179 FFC68359 3C29EAC8 4FFA3A70 8000F694


    w_i is
        AF1357D9 701FAD10 FBD88D1E 28322394 36D76EB2 71BDC3CA
        04425EC8 8BC0E89A 4D5C37FF CE7C6C3A BDE9C413 AE6D3FEA


    W is
```

```
        F5983946 320E36C6 4EF283CA 1F65D197 CF81624E C6778E77
        0E78949D 84EF21A4 5CDD62D1 DB76920D 4C2836FC 6AE5299F
        AF1357D9 701FAD10 FBD88D1E 28322394 36D76EB2 71BDC3CA
        04425EC8 8BC0E89A 4D5C37FF CE7C6C3A BDE9C413 AE6D3FEA


  returned_bits is
        F5983946 320E36C6 4EF283CA 1F65D197 CF81624E C6778E77
        0E78949D 84EF21A4 5CDD62D1 DB76920D 4C2836FC 6AE5299F
        AF1357D9 701FAD10 FBD88D1E 28322394 36D76EB2 71BDC3CA
        04425EC8 8BC0E89A 4D5C37FF CE7C6C3A BDE9C413 AE6D3FEA


---------------------------

  Update V

    0x03||V is
                          033B5014 977E9BEF 76896882 A374700D
        0F005EC2 B81A3DDC 5540ACD3 E9F977A9 73EEA7CF FB397239
        923A1AA7 B0462370 84E969AA 92E83090 7FF9539E 223F819A
        B59BF925 D929F358 E0BD6566 8DB0D643 5F36231B 9624DC29
        B96E5F31 AE187179 FFC68359 3C29EAC8 4FFA3A70 8000F693


    H is
        2EE3D634 22DF47F0 9117EB31 793BFD6D 3FA27D8A E9DD51CE
        5EF32DBA 5B099597 423B310B E0292C29 9FD141FC 91A9FC11


  Updated values

  V is
                            C857A4 B33644AF 091FDC9B 3660A21C
        E2258637 FBC7E2A4 A82A04D7 64D0896E 4D4DCFB8 78042404
        97F84987 A3D3B60F 6147EB6D 4E4F6043 FFEBB7DE 51DF876C
        335672E7 725259E3 F4C400B2 8210E730 C6C4B9D1 A1B33F2A
        54BC6321 E1C49905 0CEBE539 E69D7A14 0740F2BB 756C5986


  reseed_counter is
                                                0000 00000002


rnd_val is
        F5983946 320E36C6 4EF283CA 1F65D197 CF81624E C6778E77
```

0E78949D 84EF21A4 5CDD62D1 DB76920D 4C2836FC 6AE5299F
AF1357D9 701FAD10 FBD88D1E 28322394 36D76EB2 71BDC3CA
04425EC8 8BC0E89A 4D5C37FF CE7C6C3A BDE9C413 AE6D3FEA

##

Hash_DRBG

Requested Security Strength = 192

Requested Hash Algorithm = SHA-384

prediction_resistance_flag = "ENABLED"
EntropyInput =
000102 03040506 0708090A 0B0C0D0E
0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E

EntropyInput1 (for Reseed1) =
808182 83848586 8788898A 8B8C8D8E
8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE

EntropyInput2 (for Reseed2) =
C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E

Nonce =
20212223 24252627 28292A2B

PersonalizationString = <empty>

AdditionalInput1 =
606162 63646566 6768696A 6B6C6D6E

```
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    AdditionalInput2 =
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


##############################################################

**************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                    20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                          000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
```

```
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                        01000003 78000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


Hash(counter||no_of_bits_to_return||input_string) is
    703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
    FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4


temp =
    703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
    FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                        02000003 78000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


Hash(counter||no_of_bits_to_return||input_string) is
    31487080 FDE0B521 DEBCFC5A AB9D39DA D9466C24 D4498964
    E4E318D4 DC777C22 A0EEE9B5 79B281AE 6AEB18B0 28D5C99A
```

```
    temp =
        703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
        FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4
        31487080 FDE0B521 DEBCFC5A AB9D39DA D9466C24 D4498964
        E4E318D4 DC777C22 A0EEE9B5 79B281AE 6AEB18B0 28D5C99A


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                                              03000003 78000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
        63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


    Hash(counter||no_of_bits_to_return||input_string) is
        9B71197A 30150000 F1E5B6AD 1EB81AB2 7B8E19BE 185E4F70
        61F1D3CA 9B3A0DF4 FD597962 C2070B7E B064B31F 4F3E10BD


    temp =
                            703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


  V is
                            703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
```

```
                    00703AEC B83762E8 855BF167 2A52FAEF
    5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
    FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
    DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
    AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
          01 00000378 00703AEC B83762E8 855BF167 2A52FAEF
    5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
    FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
    DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
    AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


Hash(counter||no_of_bits_to_return||input_string) is
    805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
    DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009


temp =
    805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
    DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 00703AEC B83762E8 855BF167 2A52FAEF
    5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
    FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
    DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
    AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


Hash(counter||no_of_bits_to_return||input_string) is
    424E5B0A BDF33FBB 5C02CA64 3A5753A2 4ED17561 9251B4E0
    89DACFDA C1CD8989 CF0F87B9 197E7BEF D8550312 538A89B9
```

```
    temp =
        805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
        DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009
        424E5B0A BDF33FBB 5C02CA64 3A5753A2 4ED17561 9251B4E0
        89DACFDA C1CD8989 CF0F87B9 197E7BEF D8550312 538A89B9


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
              03 00000378 00703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


    Hash(counter||no_of_bits_to_return||input_string) is
        55F0BF84 2C6BF212 18612101 CB0E1A06 0E2E9C66 5E87E1BA
        9632F01B 4CF80D08 C9645BD1 830112EA 6EBFED69 A48CA9C9


    temp =
                            805F3E 8A9A40AA EE585729 8729B9CF
        5187C6DD BB443A05 D3DFF4C7 F2053B3C BE34E9B1 9763329E
        7CCE8806 8B1DD2C0 09424E5B 0ABDF33F BB5C02CA 643A5753
        A24ED175 619251B4 E089DACF DAC1CD89 89CF0F87 B9197E7B
        EFD85503 12538A89 B955F0BF 842C6BF2 12186121 01CB0E1A


  C is
                            805F3E 8A9A40AA EE585729 8729B9CF
        5187C6DD BB443A05 D3DFF4C7 F2053B3C BE34E9B1 9763329E
        7CCE8806 8B1DD2C0 09424E5B 0ABDF33F BB5C02CA 643A5753
        A24ED175 619251B4 E089DACF DAC1CD89 89CF0F87 B9197E7B
        EFD85503 12538A89 B955F0BF 842C6BF2 12186121 01CB0E1A


------------------------------------------------------------

First call to Generate
```

```
**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Generate FAILED: Reseed is required
--------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  additional_input
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0170 3AECB837 62E8855B F1672A52 FAEF5C7B 5C83E893
        D00130FE C63C9AC5 F53F2323 0D5CCE76 6D09FFF0 DAC417C8
        892FC431 487080FD E0B521DE BCFC5AAB 9D39DAD9 466C24D4
        498964E4 E318D4DC 777C22A0 EEE9B579 B281AE6A EB18B028
        D5C99A9B 71197A30 150000F1 E5B6AD1E B81A8081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
```

```
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                                      010000
    03780170 3AECB837 62E8855B F1672A52 FAEF5C7B 5C83E893
    D00130FE C63C9AC5 F53F2323 0D5CCE76 6D09FFF0 DAC417C8
    892FC431 487080FD E0B521DE BCFC5AAB 9D39DAD9 466C24D4
    498964E4 E318D4DC 777C22A0 EEE9B579 B281AE6A EB18B028
    D5C99A9B 71197A30 150000F1 E5B6AD1E B81A8081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Hash(counter||no_of_bits_to_return||input_string) is
    2EC68512 4C44A241 41B27CE0 A667988B 1862B83B 74885C0F
    ED758F3D 214F663E 3487B2C0 08FF214C 1FB7B815 7E0B45E9


temp =
    2EC68512 4C44A241 41B27CE0 A667988B 1862B83B 74885C0F
    ED758F3D 214F663E 3487B2C0 08FF214C 1FB7B815 7E0B45E9


------------
```

```
i = 2

counter||no_of_bits_to_return||input_string is
                                                        020000
    03780170 3AECB837 62E8855B F1672A52 FAEF5C7B 5C83E893
    D00130FE C63C9AC5 F53F2323 0D5CCE76 6D09FFF0 DAC417C8
    892FC431 487080FD E0B521DE BCFC5AAB 9D39DAD9 466C24D4
    498964E4 E318D4DC 777C22A0 EEE9B579 B281AE6A EB18B028
    D5C99A9B 71197A30 150000F1 E5B6AD1E B81A8081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Hash(counter||no_of_bits_to_return||input_string) is
    D3F65CB3 AF39B4BF 15E6DA8A BC9902E2 CE5B297F 01E89E31
    0A6515C0 8F42FAB2 91F08335 3EDF23DB 76584ABF 527837C6


temp =
    2EC68512 4C44A241 41B27CE0 A667988B 1862B83B 74885C0F
    ED758F3D 214F663E 3487B2C0 08FF214C 1FB7B815 7E0B45E9
    D3F65CB3 AF39B4BF 15E6DA8A BC9902E2 CE5B297F 01E89E31
    0A6515C0 8F42FAB2 91F08335 3EDF23DB 76584ABF 527837C6


------------

i = 3

counter||no_of_bits_to_return||input_string is
                                                        030000
    03780170 3AECB837 62E8855B F1672A52 FAEF5C7B 5C83E893
    D00130FE C63C9AC5 F53F2323 0D5CCE76 6D09FFF0 DAC417C8
    892FC431 487080FD E0B521DE BCFC5AAB 9D39DAD9 466C24D4
    498964E4 E318D4DC 777C22A0 EEE9B579 B281AE6A EB18B028
    D5C99A9B 71197A30 150000F1 E5B6AD1E B81A8081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
```

```
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    Hash(counter||no_of_bits_to_return||input_string) is
        04C46773 69F62CB5 0C897A5D 438FDBC0 408F1139 53ED6641
        E119F9A1 724830AA A78D3C51 CC430F24 19BAE40B A6151252


    temp =
                            2EC685 124C44A2 4141B27C E0A66798
        8B1862B8 3B74885C 0FED758F 3D214F66 3E3487B2 C008FF21
        4C1FB7B8 157E0B45 E9D3F65C B3AF39B4 BF15E6DA 8ABC9902
        E2CE5B29 7F01E89E 310A6515 C08F42FA B291F083 353EDF23
        DB76584A BF527837 C604C467 7369F62C B50C897A 5D438FDB


  V is
                            2EC685 124C44A2 4141B27C E0A66798
        8B1862B8 3B74885C 0FED758F 3D214F66 3E3487B2 C008FF21
        4C1FB7B8 157E0B45 E9D3F65C B3AF39B4 BF15E6DA 8ABC9902
        E2CE5B29 7F01E89E 310A6515 C08F42FA B291F083 353EDF23
        DB76584A BF527837 C604C467 7369F62C B50C897A 5D438FDB


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           002EC685 124C44A2 4141B27C E0A66798
        8B1862B8 3B74885C 0FED758F 3D214F66 3E3487B2 C008FF21
        4C1FB7B8 157E0B45 E9D3F65C B3AF39B4 BF15E6DA 8ABC9902
        E2CE5B29 7F01E89E 310A6515 C08F42FA B291F083 353EDF23
        DB76584A BF527837 C604C467 7369F62C B50C897A 5D438FDB


    no_of_bits_to_return = 888

    ------------

    i = 1
```

```
counter||no_of_bits_to_return||input_string is
          01 00000378 002EC685 124C44A2 4141B27C E0A66798
    8B1862B8 3B74885C 0FED758F 3D214F66 3E3487B2 C008FF21
    4C1FB7B8 157E0B45 E9D3F65C B3AF39B4 BF15E6DA 8ABC9902
    E2CE5B29 7F01E89E 310A6515 C08F42FA B291F083 353EDF23
    DB76584A BF527837 C604C467 7369F62C B50C897A 5D438FDB


Hash(counter||no_of_bits_to_return||input_string) is
    CFF74C15 F913106A 8D4C3201 1866ECE3 48203068 66A53E0B
    D56E68A4 E61A9D62 A73233E6 7D5BDB9C FFDA6063 0AD61EE9


temp =
    CFF74C15 F913106A 8D4C3201 1866ECE3 48203068 66A53E0B
    D56E68A4 E61A9D62 A73233E6 7D5BDB9C FFDA6063 0AD61EE9


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 002EC685 124C44A2 4141B27C E0A66798
    8B1862B8 3B74885C 0FED758F 3D214F66 3E3487B2 C008FF21
    4C1FB7B8 157E0B45 E9D3F65C B3AF39B4 BF15E6DA 8ABC9902
    E2CE5B29 7F01E89E 310A6515 C08F42FA B291F083 353EDF23
    DB76584A BF527837 C604C467 7369F62C B50C897A 5D438FDB


Hash(counter||no_of_bits_to_return||input_string) is
    1DCE24C8 0C295386 9DF89D86 2AC5080E E7000A4F 68B878D2
    D62437F1 E0C84C5D 2E0F1C55 21E5EF75 905ECF95 C5471A15


temp =
    CFF74C15 F913106A 8D4C3201 1866ECE3 48203068 66A53E0B
    D56E68A4 E61A9D62 A73233E6 7D5BDB9C FFDA6063 0AD61EE9
    1DCE24C8 0C295386 9DF89D86 2AC5080E E7000A4F 68B878D2
    D62437F1 E0C84C5D 2E0F1C55 21E5EF75 905ECF95 C5471A15


------------

i = 3
```

```
    counter||no_of_bits_to_return||input_string is
              03 00000378 002EC685 124C44A2 4141B27C E0A66798
        8B1862B8 3B74885C 0FED758F 3D214F66 3E3487B2 C008FF21
        4C1FB7B8 157E0B45 E9D3F65C B3AF39B4 BF15E6DA 8ABC9902
        E2CE5B29 7F01E89E 310A6515 C08F42FA B291F083 353EDF23
        DB76584A BF527837 C604C467 7369F62C B50C897A 5D438FDB


    Hash(counter||no_of_bits_to_return||input_string) is
        F671096A 2C471C7D 586DB04A FDB4F459 DA6FC12F BAD53E8F
        8E7DF27E BD701D43 6A82C950 5FBA3AC0 23967BD9 55C95899


    temp =
                            CFF74C 15F91310 6A8D4C32 011866EC
        E3482030 6866A53E 0BD56E68 A4E61A9D 62A73233 E67D5BDB
        9CFFDA60 630AD61E E91DCE24 C80C2953 869DF89D 862AC508
        0EE7000A 4F68B878 D2D62437 F1E0C84C 5D2E0F1C 5521E5EF
        75905ECF 95C5471A 15F67109 6A2C471C 7D586DB0 4AFDB4F4


  C is
                            CFF74C 15F91310 6A8D4C32 011866EC
        E3482030 6866A53E 0BD56E68 A4E61A9D 62A73233 E67D5BDB
        9CFFDA60 630AD61E E91DCE24 C80C2953 869DF89D 862AC508
        0EE7000A 4F68B878 D2D62437 F1E0C84C 5D2E0F1C 5521E5EF
        75905ECF 95C5471A 15F67109 6A2C471C 7D586DB0 4AFDB4F4


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------
```

```
  i = 1

  data is
                          2EC685 124C44A2 4141B27C E0A66798
      8B1862B8 3B74885C 0FED758F 3D214F66 3E3487B2 C008FF21
      4C1FB7B8 157E0B45 E9D3F65C B3AF39B4 BF15E6DA 8ABC9902
      E2CE5B29 7F01E89E 310A6515 C08F42FA B291F083 353EDF23
      DB76584A BF527837 C604C467 7369F62C B50C897A 5D438FDB


  w_i is
      1D332DE2 79BD8828 3A8FB9E9 C595227C 870F77D1 80FC743F
      758FEEC7 CD372472 26A35B6E BC073529 AED940B3 4829143E


  W is
      1D332DE2 79BD8828 3A8FB9E9 C595227C 870F77D1 80FC743F
      758FEEC7 CD372472 26A35B6E BC073529 AED940B3 4829143E


  ------------

  i = 2

  data is
                          2EC685 124C44A2 4141B27C E0A66798
      8B1862B8 3B74885C 0FED758F 3D214F66 3E3487B2 C008FF21
      4C1FB7B8 157E0B45 E9D3F65C B3AF39B4 BF15E6DA 8ABC9902
      E2CE5B29 7F01E89E 310A6515 C08F42FA B291F083 353EDF23
      DB76584A BF527837 C604C467 7369F62C B50C897A 5D438FDC


  w_i is
      587E175A D24D3D41 6C57F1C6 90D82C69 DB4C96AC 04ADAD2F
      8BA5A651 B1D7476A 4ED3B683 324685AB 8DB9F811 F79B1BA7


  W is
      1D332DE2 79BD8828 3A8FB9E9 C595227C 870F77D1 80FC743F
      758FEEC7 CD372472 26A35B6E BC073529 AED940B3 4829143E
      587E175A D24D3D41 6C57F1C6 90D82C69 DB4C96AC 04ADAD2F
      8BA5A651 B1D7476A 4ED3B683 324685AB 8DB9F811 F79B1BA7


returned_bits is
      1D332DE2 79BD8828 3A8FB9E9 C595227C 870F77D1 80FC743F
```

```
        758FEEC7 CD372472 26A35B6E BC073529 AED940B3 4829143E
        587E175A D24D3D41 6C57F1C6 90D82C69 DB4C96AC 04ADAD2F
        8BA5A651 B1D7476A 4ED3B683 324685AB 8DB9F811 F79B1BA7


---------------------------

  Update V

    0x03||V is
                          032EC685 124C44A2 4141B27C E0A66798
        8B1862B8 3B74885C 0FED758F 3D214F66 3E3487B2 C008FF21
        4C1FB7B8 157E0B45 E9D3F65C B3AF39B4 BF15E6DA 8ABC9902
        E2CE5B29 7F01E89E 310A6515 C08F42FA B291F083 353EDF23
        DB76584A BF527837 C604C467 7369F62C B50C897A 5D438FDB


    H is
        7A17B8BD 2EA72A06 BB316EE2 959B48F9 BA59C3E8 987B6744
        2B6F8027 4EEFF4A4 CD391467 BA5B0F3D 61AA24EB 715284C8


  Updated values

  V is
                            FEBDD1 284557B2 ABCEFEAE E1BECE85
        6E6082E8 A3DB2D9A 1BC2E3F7 E2076A03 A0DBB9E6 A6865AFC
        E91F9218 7888E164 D2F1C481 7BBB6308 45B3DF78 10E75E0B
        6BCD13F0 FD11CB1D BF11F830 480B5440 CA19C388 22DC2C57
        7C763741 A407B3F6 A93449D8 97F14C86 940F1C16 1993C998


  reseed_counter is
                                                0000 00000002


rnd_val is
        1D332DE2 79BD8828 3A8FB9E9 C595227C 870F77D1 80FC743F
        758FEEC7 CD372472 26A35B6E BC073529 AED940B3 4829143E
        587E175A D24D3D41 6C57F1C6 90D82C69 DB4C96AC 04ADAD2F
        8BA5A651 B1D7476A 4ED3B683 324685AB 8DB9F811 F79B1BA7


-------------------------------------------------------------

Second call to Generate
```

```
************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                           C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  additional_input
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01FE BDD12845 57B2ABCE FEAEE1BE CE856E60 82E8A3DB
        2D9A1BC2 E3F7E207 6A03A0DB B9E6A686 5AFCE91F 92187888
        E164D2F1 C4817BBB 630845B3 DF7810E7 5E0B6BCD 13F0FD11
        CB1DBF11 F830480B 5440CA19 C38822DC 2C577C76 3741A407
        B3F6A934 49D897F1 4C86940F 1C161993 C998C0C1 C2C3C4C5
```

```
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                                      010000
    037801FE BDD12845 57B2ABCE FEAEE1BE CE856E60 82E8A3DB
    2D9A1BC2 E3F7E207 6A03A0DB B9E6A686 5AFCE91F 92187888
    E164D2F1 C4817BBB 630845B3 DF7810E7 5E0B6BCD 13F0FD11
    CB1DBF11 F830480B 5440CA19 C38822DC 2C577C76 3741A407
    B3F6A934 49D897F1 4C86940F 1C161993 C998C0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Hash(counter||no_of_bits_to_return||input_string) is
    0CBC7C85 938D2C85 24D4FA7F 75CD7868 AE192376 E0912491
    D0E72C2B AFE33204 0400AF3E F3543A92 ABA503E9 226CE0E0


temp =
    0CBC7C85 938D2C85 24D4FA7F 75CD7868 AE192376 E0912491
    D0E72C2B AFE33204 0400AF3E F3543A92 ABA503E9 226CE0E0


------------
```

```
i = 2

counter||no_of_bits_to_return||input_string is
                                                        020000
    037801FE BDD12845 57B2ABCE FEAEE1BE CE856E60 82E8A3DB
    2D9A1BC2 E3F7E207 6A03A0DB B9E6A686 5AFCE91F 92187888
    E164D2F1 C4817BBB 630845B3 DF7810E7 5E0B6BCD 13F0FD11
    CB1DBF11 F830480B 5440CA19 C38822DC 2C577C76 3741A407
    B3F6A934 49D897F1 4C86940F 1C161993 C998C0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Hash(counter||no_of_bits_to_return||input_string) is
    8A938880 74BC3D00 7303A5EE 0874F8ED 82064F30 F2472D8E
    7B966403 CBDC23E4 A0523F2E 3E11F6ED B1ADF5C6 C469A377


temp =
    0CBC7C85 938D2C85 24D4FA7F 75CD7868 AE192376 E0912491
    D0E72C2B AFE33204 0400AF3E F3543A92 ABA503E9 226CE0E0
    8A938880 74BC3D00 7303A5EE 0874F8ED 82064F30 F2472D8E
    7B966403 CBDC23E4 A0523F2E 3E11F6ED B1ADF5C6 C469A377


------------

i = 3

counter||no_of_bits_to_return||input_string is
                                                        030000
    037801FE BDD12845 57B2ABCE FEAEE1BE CE856E60 82E8A3DB
    2D9A1BC2 E3F7E207 6A03A0DB B9E6A686 5AFCE91F 92187888
    E164D2F1 C4817BBB 630845B3 DF7810E7 5E0B6BCD 13F0FD11
    CB1DBF11 F830480B 5440CA19 C38822DC 2C577C76 3741A407
    B3F6A934 49D897F1 4C86940F 1C161993 C998C0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
```

```
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    Hash(counter||no_of_bits_to_return||input_string) is
        91A0A74D 14AE0597 DDE0D324 6219D784 2C2CB510 093EBAE1
        38C579CB 623BFCDE B9E9CC6E 05F351BF A2C17770 667CB1F1


    temp =
                            0CBC7C 85938D2C 8524D4FA 7F75CD78
        68AE1923 76E09124 91D0E72C 2BAFE332 040400AF 3EF3543A
        92ABA503 E9226CE0 E08A9388 8074BC3D 007303A5 EE0874F8
        ED82064F 30F2472D 8E7B9664 03CBDC23 E4A0523F 2E3E11F6
        EDB1ADF5 C6C469A3 7791A0A7 4D14AE05 97DDE0D3 246219D7


  V is
                            0CBC7C 85938D2C 8524D4FA 7F75CD78
        68AE1923 76E09124 91D0E72C 2BAFE332 040400AF 3EF3543A
        92ABA503 E9226CE0 E08A9388 8074BC3D 007303A5 EE0874F8
        ED82064F 30F2472D 8E7B9664 03CBDC23 E4A0523F 2E3E11F6
        EDB1ADF5 C6C469A3 7791A0A7 4D14AE05 97DDE0D3 246219D7


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           000CBC7C 85938D2C 8524D4FA 7F75CD78
        68AE1923 76E09124 91D0E72C 2BAFE332 040400AF 3EF3543A
        92ABA503 E9226CE0 E08A9388 8074BC3D 007303A5 EE0874F8
        ED82064F 30F2472D 8E7B9664 03CBDC23 E4A0523F 2E3E11F6
        EDB1ADF5 C6C469A3 7791A0A7 4D14AE05 97DDE0D3 246219D7


    no_of_bits_to_return = 888

    ------------
```

```
i = 1

counter||no_of_bits_to_return||input_string is
          01 00000378 000CBC7C 85938D2C 8524D4FA 7F75CD78
    68AE1923 76E09124 91D0E72C 2BAFE332 040400AF 3EF3543A
    92ABA503 E9226CE0 E08A9388 8074BC3D 007303A5 EE0874F8
    ED82064F 30F2472D 8E7B9664 03CBDC23 E4A0523F 2E3E11F6
    EDB1ADF5 C6C469A3 7791A0A7 4D14AE05 97DDE0D3 246219D7


Hash(counter||no_of_bits_to_return||input_string) is
    6957C0B9 A4E6023B 9429FD5E 97B7D15A F22EAE23 C4D97282
    43737CF7 388CC109 44671C90 B5CC8332 AE225A1A A6F90D6A


temp =
    6957C0B9 A4E6023B 9429FD5E 97B7D15A F22EAE23 C4D97282
    43737CF7 388CC109 44671C90 B5CC8332 AE225A1A A6F90D6A


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 000CBC7C 85938D2C 8524D4FA 7F75CD78
    68AE1923 76E09124 91D0E72C 2BAFE332 040400AF 3EF3543A
    92ABA503 E9226CE0 E08A9388 8074BC3D 007303A5 EE0874F8
    ED82064F 30F2472D 8E7B9664 03CBDC23 E4A0523F 2E3E11F6
    EDB1ADF5 C6C469A3 7791A0A7 4D14AE05 97DDE0D3 246219D7


Hash(counter||no_of_bits_to_return||input_string) is
    74B0B25C 0064E888 36146F27 D908F901 62BD1B97 7803E346
    90DA2225 E2999EEA BF842516 0A3BED3B 3571AD12 BE4E2E69


temp =
    6957C0B9 A4E6023B 9429FD5E 97B7D15A F22EAE23 C4D97282
    43737CF7 388CC109 44671C90 B5CC8332 AE225A1A A6F90D6A
    74B0B25C 0064E888 36146F27 D908F901 62BD1B97 7803E346
    90DA2225 E2999EEA BF842516 0A3BED3B 3571AD12 BE4E2E69


------------
```

```
    i = 3

    counter||no_of_bits_to_return||input_string is
              03 00000378 000CBC7C 85938D2C 8524D4FA 7F75CD78
        68AE1923 76E09124 91D0E72C 2BAFE332 040400AF 3EF3543A
        92ABA503 E9226CE0 E08A9388 8074BC3D 007303A5 EE0874F8
        ED82064F 30F2472D 8E7B9664 03CBDC23 E4A0523F 2E3E11F6
        EDB1ADF5 C6C469A3 7791A0A7 4D14AE05 97DDE0D3 246219D7


    Hash(counter||no_of_bits_to_return||input_string) is
        95E73825 F6DF0B03 09180685 A51C43F8 6D268199 75F63082
        E9FAE867 6876B8E2 BEF09A87 26B8B8C9 1B1DA259 625B81F9


    temp =
                            6957C0 B9A4E602 3B9429FD 5E97B7D1
        5AF22EAE 23C4D972 8243737C F7388CC1 0944671C 90B5CC83
        32AE225A 1AA6F90D 6A74B0B2 5C0064E8 8836146F 27D908F9
        0162BD1B 977803E3 4690DA22 25E2999E EABF8425 160A3BED
        3B3571AD 12BE4E2E 6995E738 25F6DF0B 03091806 85A51C43


  C is
                            6957C0 B9A4E602 3B9429FD 5E97B7D1
        5AF22EAE 23C4D972 8243737C F7388CC1 0944671C 90B5CC83
        32AE225A 1AA6F90D 6A74B0B2 5C0064E8 8836146F 27D908F9
        0162BD1B 977803E3 4690DA22 25E2999E EABF8425 160A3BED
        3B3571AD 12BE4E2E 6995E738 25F6DF0B 03091806 85A51C43


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------
```

```
  i = 1

  data is
                          0CBC7C 85938D2C 8524D4FA 7F75CD78
      68AE1923 76E09124 91D0E72C 2BAFE332 040400AF 3EF3543A
      92ABA503 E9226CE0 E08A9388 8074BC3D 007303A5 EE0874F8
      ED82064F 30F2472D 8E7B9664 03CBDC23 E4A0523F 2E3E11F6
      EDB1ADF5 C6C469A3 7791A0A7 4D14AE05 97DDE0D3 246219D7


  w_i is
      4B7FF453 EB17F58C 49041450 8ABCCA50 E760FB71 13308E29
      F4E8A9B7 A67AC594 2ADBB6AC 445077EB B8D47B8C 92A7161B


  W is
      4B7FF453 EB17F58C 49041450 8ABCCA50 E760FB71 13308E29
      F4E8A9B7 A67AC594 2ADBB6AC 445077EB B8D47B8C 92A7161B


  ------------

  i = 2

  data is
                          0CBC7C 85938D2C 8524D4FA 7F75CD78
      68AE1923 76E09124 91D0E72C 2BAFE332 040400AF 3EF3543A
      92ABA503 E9226CE0 E08A9388 8074BC3D 007303A5 EE0874F8
      ED82064F 30F2472D 8E7B9664 03CBDC23 E4A0523F 2E3E11F6
      EDB1ADF5 C6C469A3 7791A0A7 4D14AE05 97DDE0D3 246219D8


  w_i is
      E9020087 F87DAAD6 7E8F0BEE B5E53BCD 806243C8 E6362CB3
      5BACE034 00B5CDC9 5EFF9DE4 135A398F F50FC0F5 903B8073


  W is
      4B7FF453 EB17F58C 49041450 8ABCCA50 E760FB71 13308E29
      F4E8A9B7 A67AC594 2ADBB6AC 445077EB B8D47B8C 92A7161B
      E9020087 F87DAAD6 7E8F0BEE B5E53BCD 806243C8 E6362CB3
      5BACE034 00B5CDC9 5EFF9DE4 135A398F F50FC0F5 903B8073


returned_bits is
```

```
        4B7FF453 EB17F58C 49041450 8ABCCA50 E760FB71 13308E29
        F4E8A9B7 A67AC594 2ADBB6AC 445077EB B8D47B8C 92A7161B
        E9020087 F87DAAD6 7E8F0BEE B5E53BCD 806243C8 E6362CB3
        5BACE034 00B5CDC9 5EFF9DE4 135A398F F50FC0F5 903B8073


--------------------------

  Update V

    0x03||V is
                          030CBC7C 85938D2C 8524D4FA 7F75CD78
        68AE1923 76E09124 91D0E72C 2BAFE332 040400AF 3EF3543A
        92ABA503 E9226CE0 E08A9388 8074BC3D 007303A5 EE0874F8
        ED82064F 30F2472D 8E7B9664 03CBDC23 E4A0523F 2E3E11F6
        EDB1ADF5 C6C469A3 7791A0A7 4D14AE05 97DDE0D3 246219D7


    H is
        3EB6BAA9 3ADF6560 38CF1960 7D08A3E0 8D04D674 28FFEFEA
        C6DFC2EE 869DBC36 9F26D852 8FDCBD23 5ED55CEC 83AA2005


  Updated values

  V is
                            76143D 3F38732E C0B8FEF7 DE0D8549
        C3A047D1 9AA56A97 14145AA9 22E86FF3 0D4867CB CFA920BD
        C559C75E 03C965EE 4AFF443A DC752125 88A91815 15E17DF2
        2D9B7E14 0349B071 0DDB89E6 A6B719A3 5C64ACD8 6D483DCE
        EFC6E291 60207408 804E6032 02E84A33 F9BC55C6 2DB15620


  reseed_counter is
                                                0000 00000002


rnd_val is
        4B7FF453 EB17F58C 49041450 8ABCCA50 E760FB71 13308E29
        F4E8A9B7 A67AC594 2ADBB6AC 445077EB B8D47B8C 92A7161B
        E9020087 F87DAAD6 7E8F0BEE B5E53BCD 806243C8 E6362CB3
        5BACE034 00B5CDC9 5EFF9DE4 135A398F F50FC0F5 903B8073


################################################################
```

```
Hash_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                    20212223 24252627 28292A2B


    PersonalizationString =
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    AdditionalInput = <empty>

################################################################
```

```
************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                  20212223 24252627 28292A2B


    personal_str is
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                     0001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    no_of_bits_to_return = 888
```

```
------------

i = 1

counter||no_of_bits_to_return||input_string is
      010000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
    A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
    EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964


temp =
    A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
    EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964


------------

i = 2

counter||no_of_bits_to_return||input_string is
      020000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
    C74754B6 A1E77C6C 0DE0245E 3BC81E15 85F2F379 F4489643
```

```
        5F61C23D B552DB8B 3190F5F3 7B966F3D D000CEB5 373CA2BD


    temp =
        A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
        EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964
        C74754B6 A1E77C6C 0DE0245E 3BC81E15 85F2F379 F4489643
        5F61C23D B552DB8B 3190F5F3 7B966F3D D000CEB5 373CA2BD


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
          030000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    Hash(counter||no_of_bits_to_return||input_string) is
        A8989587 CED14C8E 80790CD7 146F3328 3D84860A 708750EA
        1FDCD1DA D814E76A CA6E310F 12AA0BBA 611A8E86 FC0EAE47


    temp =
                            A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


V is
                            A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33
```

```
---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


    Hash(counter||no_of_bits_to_return||input_string) is
        DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
        273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D


    temp =
        DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
        273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
              02 00000378 00A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
```

```
    1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
    3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


Hash(counter||no_of_bits_to_return||input_string) is
    7B72F966 9A700AF1 C7E3466A 5E89A0DC A45282E7 1A39E4AA
    24585736 11785015 85B95258 C40A2016 2D1F62CA 988BBEC7


temp =
    DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
    273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D
    7B72F966 9A700AF1 C7E3466A 5E89A0DC A45282E7 1A39E4AA
    24585736 11785015 85B95258 C40A2016 2D1F62CA 988BBEC7


------------

i = 3

counter||no_of_bits_to_return||input_string is
          03 00000378 00A028F8 43783D77 21E32AC5 FD923031
    884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
    C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
    1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
    3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


Hash(counter||no_of_bits_to_return||input_string) is
    FD2CAD8E 501A9FA7 18212A41 9FA2251F 01E46C40 DDBF4D85
    223B6E11 48351858 CC99BE10 6D1A4301 A307DBAF DE079ADA


temp =
                        DE0424 3D3BB302 329A9112 4D780ADC
    F3672DDD 2CE78196 3E273BB2 49F6EC13 B16A903F 40D01C2D
    FF1464BF A6AFD698 7D7B72F9 669A700A F1C7E346 6A5E89A0
    DCA45282 E71A39E4 AA245857 36117850 1585B952 58C40A20
    162D1F62 CA988BBE C7FD2CAD 8E501A9F A718212A 419FA225


C is
                        DE0424 3D3BB302 329A9112 4D780ADC
    F3672DDD 2CE78196 3E273BB2 49F6EC13 B16A903F 40D01C2D
    FF1464BF A6AFD698 7D7B72F9 669A700A F1C7E346 6A5E89A0
    DCA45282 E71A39E4 AA245857 36117850 1585B952 58C40A20
```

```
        162D1F62 CA988BBE C7FD2CAD 8E501A9F A718212A 419FA225


-------------------------------------------------------------

First call to Generate

*************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

Generate FAILED: Reseed is required
-------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                           808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                01A028 F843783D
        7721E32A C5FD9230 31884CF9 D3F05FA2 BE09EB6A 82C782B6
        203C2938 47B98EC4 B9C0C867 4DEAE09E B964C747 54B6A1E7
        7C6C0DE0 245E3BC8 1E1585F2 F379F448 96435F61 C23DB552
        DB8B3190 F5F37B96 6F3DD000 CEB5373C A2BDA898 9587CED1
        4C8E8079 0CD7146F 33808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE
```

```
no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                01000003 7801A028 F843783D
    7721E32A C5FD9230 31884CF9 D3F05FA2 BE09EB6A 82C782B6
    203C2938 47B98EC4 B9C0C867 4DEAE09E B964C747 54B6A1E7
    7C6C0DE0 245E3BC8 1E1585F2 F379F448 96435F61 C23DB552
    DB8B3190 F5F37B96 6F3DD000 CEB5373C A2BDA898 9587CED1
    4C8E8079 0CD7146F 33808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


Hash(counter||no_of_bits_to_return||input_string) is
    B8FB4017 52EA402B 40088B38 B9E21FAF B07F86D2 EEFA0281
    2177C28A 76ABD2EA F0B450B6 7ED4F746 50EAF2DB 8F9C720A


temp =
    B8FB4017 52EA402B 40088B38 B9E21FAF B07F86D2 EEFA0281
    2177C28A 76ABD2EA F0B450B6 7ED4F746 50EAF2DB 8F9C720A


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                02000003 7801A028 F843783D
    7721E32A C5FD9230 31884CF9 D3F05FA2 BE09EB6A 82C782B6
    203C2938 47B98EC4 B9C0C867 4DEAE09E B964C747 54B6A1E7
    7C6C0DE0 245E3BC8 1E1585F2 F379F448 96435F61 C23DB552
    DB8B3190 F5F37B96 6F3DD000 CEB5373C A2BDA898 9587CED1
    4C8E8079 0CD7146F 33808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE
```

```
  Hash(counter||no_of_bits_to_return||input_string) is
      81AEAEC8 4BB298FE 4D5974CE E9FD5218 B50B6CCB C77DAF80
      9FB549BB 18974D0C 8B93B38E E6CE54C7 6EEB3D08 DEF2817D


  temp =
      B8FB4017 52EA402B 40088B38 B9E21FAF B07F86D2 EEFA0281
      2177C28A 76ABD2EA F0B450B6 7ED4F746 50EAF2DB 8F9C720A
      81AEAEC8 4BB298FE 4D5974CE E9FD5218 B50B6CCB C77DAF80
      9FB549BB 18974D0C 8B93B38E E6CE54C7 6EEB3D08 DEF2817D


  ------------

  i = 3

  counter||no_of_bits_to_return||input_string is
                                03000003 7801A028 F843783D
      7721E32A C5FD9230 31884CF9 D3F05FA2 BE09EB6A 82C782B6
      203C2938 47B98EC4 B9C0C867 4DEAE09E B964C747 54B6A1E7
      7C6C0DE0 245E3BC8 1E1585F2 F379F448 96435F61 C23DB552
      DB8B3190 F5F37B96 6F3DD000 CEB5373C A2BDA898 9587CED1
      4C8E8079 0CD7146F 33808182 83848586 8788898A 8B8C8D8E
      8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
      A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
      BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
      D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  Hash(counter||no_of_bits_to_return||input_string) is
      72E347E6 D5CB535C 70672C3A BDF0EFA4 6C9A7825 B88095E6
      5A8C9D11 3A31E537 ADB6C58D E33365EA 1E6A964C 98246E96


  temp =
                          B8FB40 1752EA40 2B40088B 38B9E21F
      AFB07F86 D2EEFA02 812177C2 8A76ABD2 EAF0B450 B67ED4F7
      4650EAF2 DB8F9C72 0A81AEAE C84BB298 FE4D5974 CEE9FD52
      18B50B6C CBC77DAF 809FB549 BB18974D 0C8B93B3 8EE6CE54
      C76EEB3D 08DEF281 7D72E347 E6D5CB53 5C70672C 3ABDF0EF


V is
                          B8FB40 1752EA40 2B40088B 38B9E21F
      AFB07F86 D2EEFA02 812177C2 8A76ABD2 EAF0B450 B67ED4F7
```

```
        4650EAF2 DB8F9C72 0A81AEAE C84BB298 FE4D5974 CEE9FD52
        18B50B6C CBC77DAF 809FB549 BB18974D 0C8B93B3 8EE6CE54
        C76EEB3D 08DEF281 7D72E347 E6D5CB53 5C70672C 3ABDF0EF


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00B8FB40 1752EA40 2B40088B 38B9E21F
        AFB07F86 D2EEFA02 812177C2 8A76ABD2 EAF0B450 B67ED4F7
        4650EAF2 DB8F9C72 0A81AEAE C84BB298 FE4D5974 CEE9FD52
        18B50B6C CBC77DAF 809FB549 BB18974D 0C8B93B3 8EE6CE54
        C76EEB3D 08DEF281 7D72E347 E6D5CB53 5C70672C 3ABDF0EF


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00B8FB40 1752EA40 2B40088B 38B9E21F
        AFB07F86 D2EEFA02 812177C2 8A76ABD2 EAF0B450 B67ED4F7
        4650EAF2 DB8F9C72 0A81AEAE C84BB298 FE4D5974 CEE9FD52
        18B50B6C CBC77DAF 809FB549 BB18974D 0C8B93B3 8EE6CE54
        C76EEB3D 08DEF281 7D72E347 E6D5CB53 5C70672C 3ABDF0EF


    Hash(counter||no_of_bits_to_return||input_string) is
        A00A98C1 82E4603D A4DEA867 148EBB96 693D9023 2B5369D0
        8B42EC27 146D80C5 BF9703DB D40E8BA5 80F6E695 8A8B99D9


    temp =
        A00A98C1 82E4603D A4DEA867 148EBB96 693D9023 2B5369D0
        8B42EC27 146D80C5 BF9703DB D40E8BA5 80F6E695 8A8B99D9


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
```

```
          02 00000378 00B8FB40 1752EA40 2B40088B 38B9E21F
      AFB07F86 D2EEFA02 812177C2 8A76ABD2 EAF0B450 B67ED4F7
      4650EAF2 DB8F9C72 0A81AEAE C84BB298 FE4D5974 CEE9FD52
      18B50B6C CBC77DAF 809FB549 BB18974D 0C8B93B3 8EE6CE54
      C76EEB3D 08DEF281 7D72E347 E6D5CB53 5C70672C 3ABDF0EF


  Hash(counter||no_of_bits_to_return||input_string) is
      7487DB59 E24C9E95 4E3AF35C F2BD6FB4 2D65D637 51DF2849
      85C28A78 97BBA5D9 F0CD57CE F2D510F0 B5B301ED 9DBC6D3F


  temp =
      A00A98C1 82E4603D A4DEA867 148EBB96 693D9023 2B5369D0
      8B42EC27 146D80C5 BF9703DB D40E8BA5 80F6E695 8A8B99D9
      7487DB59 E24C9E95 4E3AF35C F2BD6FB4 2D65D637 51DF2849
      85C28A78 97BBA5D9 F0CD57CE F2D510F0 B5B301ED 9DBC6D3F


  ------------

  i = 3

  counter||no_of_bits_to_return||input_string is
          03 00000378 00B8FB40 1752EA40 2B40088B 38B9E21F
      AFB07F86 D2EEFA02 812177C2 8A76ABD2 EAF0B450 B67ED4F7
      4650EAF2 DB8F9C72 0A81AEAE C84BB298 FE4D5974 CEE9FD52
      18B50B6C CBC77DAF 809FB549 BB18974D 0C8B93B3 8EE6CE54
      C76EEB3D 08DEF281 7D72E347 E6D5CB53 5C70672C 3ABDF0EF


  Hash(counter||no_of_bits_to_return||input_string) is
      CDF6BD79 4CBDFA51 F81D20A2 5BA13FFB 26B1CA0F 18161497
      9170A047 60F93748 01FC5EAF 8648F5F1 66CB4ED5 771C15BD


  temp =
                          A00A98 C182E460 3DA4DEA8 67148EBB
      96693D90 232B5369 D08B42EC 27146D80 C5BF9703 DBD40E8B
      A580F6E6 958A8B99 D97487DB 59E24C9E 954E3AF3 5CF2BD6F
      B42D65D6 3751DF28 4985C28A 7897BBA5 D9F0CD57 CEF2D510
      F0B5B301 ED9DBC6D 3FCDF6BD 794CBDFA 51F81D20 A25BA13F


C is
                          A00A98 C182E460 3DA4DEA8 67148EBB
```

```
        96693D90 232B5369 D08B42EC 27146D80 C5BF9703 DBD40E8B
        A580F6E6 958A8B99 D97487DB 59E24C9E 954E3AF3 5CF2BD6F
        B42D65D6 3751DF28 4985C28A 7897BBA5 D9F0CD57 CEF2D510
        F0B5B301 ED9DBC6D 3FCDF6BD 794CBDFA 51F81D20 A25BA13F


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                            B8FB40 1752EA40 2B40088B 38B9E21F
        AFB07F86 D2EEFA02 812177C2 8A76ABD2 EAF0B450 B67ED4F7
        4650EAF2 DB8F9C72 0A81AEAE C84BB298 FE4D5974 CEE9FD52
        18B50B6C CBC77DAF 809FB549 BB18974D 0C8B93B3 8EE6CE54
        C76EEB3D 08DEF281 7D72E347 E6D5CB53 5C70672C 3ABDF0EF


    w_i is
        8D77F997 4D6EFCAF 503E24DB 4BC0E0F8 1E5E4931 60D3FFF8
        02F5AE66 4088B9C7 8381E88C CB992BF6 BCD72CDC 85CBDFCB


    W is
        8D77F997 4D6EFCAF 503E24DB 4BC0E0F8 1E5E4931 60D3FFF8
        02F5AE66 4088B9C7 8381E88C CB992BF6 BCD72CDC 85CBDFCB


    ------------

    i = 2
```

```
    data is
                             B8FB40 1752EA40 2B40088B 38B9E21F
        AFB07F86 D2EEFA02 812177C2 8A76ABD2 EAF0B450 B67ED4F7
        4650EAF2 DB8F9C72 0A81AEAE C84BB298 FE4D5974 CEE9FD52
        18B50B6C CBC77DAF 809FB549 BB18974D 0C8B93B3 8EE6CE54
        C76EEB3D 08DEF281 7D72E347 E6D5CB53 5C70672C 3ABDF0F0


    w_i is
        D7A34759 D30CBB66 A97768F7 84654B25 98CF3814 8EEF1421
        0F2DC1A7 7479CE26 548BF86F B86AC16D 00064255 1F2BF597


    W is
        8D77F997 4D6EFCAF 503E24DB 4BC0E0F8 1E5E4931 60D3FFF8
        02F5AE66 4088B9C7 8381E88C CB992BF6 BCD72CDC 85CBDFCB
        D7A34759 D30CBB66 A97768F7 84654B25 98CF3814 8EEF1421
        0F2DC1A7 7479CE26 548BF86F B86AC16D 00064255 1F2BF597


  returned_bits is
        8D77F997 4D6EFCAF 503E24DB 4BC0E0F8 1E5E4931 60D3FFF8
        02F5AE66 4088B9C7 8381E88C CB992BF6 BCD72CDC 85CBDFCB
        D7A34759 D30CBB66 A97768F7 84654B25 98CF3814 8EEF1421
        0F2DC1A7 7479CE26 548BF86F B86AC16D 00064255 1F2BF597


--------------------------

  Update V

    0x03||V is
                           03B8FB40 1752EA40 2B40088B 38B9E21F
        AFB07F86 D2EEFA02 812177C2 8A76ABD2 EAF0B450 B67ED4F7
        4650EAF2 DB8F9C72 0A81AEAE C84BB298 FE4D5974 CEE9FD52
        18B50B6C CBC77DAF 809FB549 BB18974D 0C8B93B3 8EE6CE54
        C76EEB3D 08DEF281 7D72E347 E6D5CB53 5C70672C 3ABDF0EF


    H is
        4BC7D597 C62A8AB9 DF7D575B 36600197 989C10B4 7DBD39A7
        3A34661B 75FD5697 B1A503B8 62697571 D235D54B ECF1B172


  Updated values
```

```
  V is
                            5905D8 D8D5CEA0 68E4E733 9FCE70DB
        4619BD16 F61A4D6C 51ACBAAE B18B1953 B0B04B54 9252E382
        EBD1E1D9 711A280B E3F6368A 222DFF37 939B9468 2BDCBAC2
        18AA46DA C943E791 A9A2CF2F 6A10548A 7F1871BF DB96DD0C
        F259045A 6C7A0586 6EE5DDBD C28BFEBF 809E5998 CA0B43A1


  reseed_counter is
                                                 0000 00000002


rnd_val is
        8D77F997 4D6EFCAF 503E24DB 4BC0E0F8 1E5E4931 60D3FFF8
        02F5AE66 4088B9C7 8381E88C CB992BF6 BCD72CDC 85CBDFCB
        D7A34759 D30CBB66 A97768F7 84654B25 98CF3814 8EEF1421
        0F2DC1A7 7479CE26 548BF86F B86AC16D 00064255 1F2BF597


----------------------------------------------------------------

Second call to Generate

****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

Generate FAILED: Reseed is required
----------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  additional_input <empty>
```

```
--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                 015905 D8D8D5CE
        A068E4E7 339FCE70 DB4619BD 16F61A4D 6C51ACBA AEB18B19
        53B0B04B 549252E3 82EBD1E1 D9711A28 0BE3F636 8A222DFF
        37939B94 682BDCBA C218AA46 DAC943E7 91A9A2CF 2F6A1054
        8A7F1871 BFDB96DD 0CF25904 5A6C7A05 866EE5DD BDC28BFE
        BF809E59 98CA0B43 A1C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                 01000003 78015905 D8D8D5CE
        A068E4E7 339FCE70 DB4619BD 16F61A4D 6C51ACBA AEB18B19
        53B0B04B 549252E3 82EBD1E1 D9711A28 0BE3F636 8A222DFF
        37939B94 682BDCBA C218AA46 DAC943E7 91A9A2CF 2F6A1054
        8A7F1871 BFDB96DD 0CF25904 5A6C7A05 866EE5DD BDC28BFE
        BF809E59 98CA0B43 A1C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Hash(counter||no_of_bits_to_return||input_string) is
        E0E8FA8A 274E1C52 EC32FF2D B7B20DE3 11A687FE DCCE16BA
        2174D649 79CBC4EE 88E38C50 41CC1449 D9025CD7 CA8CDB4B


    temp =
        E0E8FA8A 274E1C52 EC32FF2D B7B20DE3 11A687FE DCCE16BA
        2174D649 79CBC4EE 88E38C50 41CC1449 D9025CD7 CA8CDB4B
```

```
------------

i = 2

counter||no_of_bits_to_return||input_string is
                                02000003 78015905 D8D8D5CE
    A068E4E7 339FCE70 DB4619BD 16F61A4D 6C51ACBA AEB18B19
    53B0B04B 549252E3 82EBD1E1 D9711A28 0BE3F636 8A222DFF
    37939B94 682BDCBA C218AA46 DAC943E7 91A9A2CF 2F6A1054
    8A7F1871 BFDB96DD 0CF25904 5A6C7A05 866EE5DD BDC28BFE
    BF809E59 98CA0B43 A1C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Hash(counter||no_of_bits_to_return||input_string) is
    D4AB3A72 3B82DDFA E3726CDF 44448476 95254A09 27E159EA
    84D51C35 8B1E09F6 3C33CDB7 60C7CF2F 0BC717E1 A7C79F88


temp =
    E0E8FA8A 274E1C52 EC32FF2D B7B20DE3 11A687FE DCCE16BA
    2174D649 79CBC4EE 88E38C50 41CC1449 D9025CD7 CA8CDB4B
    D4AB3A72 3B82DDFA E3726CDF 44448476 95254A09 27E159EA
    84D51C35 8B1E09F6 3C33CDB7 60C7CF2F 0BC717E1 A7C79F88


------------

i = 3

counter||no_of_bits_to_return||input_string is
                                03000003 78015905 D8D8D5CE
    A068E4E7 339FCE70 DB4619BD 16F61A4D 6C51ACBA AEB18B19
    53B0B04B 549252E3 82EBD1E1 D9711A28 0BE3F636 8A222DFF
    37939B94 682BDCBA C218AA46 DAC943E7 91A9A2CF 2F6A1054
    8A7F1871 BFDB96DD 0CF25904 5A6C7A05 866EE5DD BDC28BFE
    BF809E59 98CA0B43 A1C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
        0522B3EB 10EF6620 3FDFB8BD 78A4C9AA 3928F7C8 BF1D3B9C
        174C4BC2 6740B28B E351D4B1 A15100FF A92658D4 FBAB23A4


    temp =
                            E0E8FA 8A274E1C 52EC32FF 2DB7B20D
        E311A687 FEDCCE16 BA2174D6 4979CBC4 EE88E38C 5041CC14
        49D9025C D7CA8CDB 4BD4AB3A 723B82DD FAE3726C DF444484
        7695254A 0927E159 EA84D51C 358B1E09 F63C33CD B760C7CF
        2F0BC717 E1A7C79F 880522B3 EB10EF66 203FDFB8 BD78A4C9


  V is
                            E0E8FA 8A274E1C 52EC32FF 2DB7B20D
        E311A687 FEDCCE16 BA2174D6 4979CBC4 EE88E38C 5041CC14
        49D9025C D7CA8CDB 4BD4AB3A 723B82DD FAE3726C DF444484
        7695254A 0927E159 EA84D51C 358B1E09 F63C33CD B760C7CF
        2F0BC717 E1A7C79F 880522B3 EB10EF66 203FDFB8 BD78A4C9


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00E0E8FA 8A274E1C 52EC32FF 2DB7B20D
        E311A687 FEDCCE16 BA2174D6 4979CBC4 EE88E38C 5041CC14
        49D9025C D7CA8CDB 4BD4AB3A 723B82DD FAE3726C DF444484
        7695254A 0927E159 EA84D51C 358B1E09 F63C33CD B760C7CF
        2F0BC717 E1A7C79F 880522B3 EB10EF66 203FDFB8 BD78A4C9


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00E0E8FA 8A274E1C 52EC32FF 2DB7B20D
        E311A687 FEDCCE16 BA2174D6 4979CBC4 EE88E38C 5041CC14
        49D9025C D7CA8CDB 4BD4AB3A 723B82DD FAE3726C DF444484
        7695254A 0927E159 EA84D51C 358B1E09 F63C33CD B760C7CF
        2F0BC717 E1A7C79F 880522B3 EB10EF66 203FDFB8 BD78A4C9
```

```
Hash(counter||no_of_bits_to_return||input_string) is
    EF628007 43C7CB83 2F07C89A 2C83B2B7 DFA75554 51B5ED66
    8AFA1BCE 3A515971 78045783 4A80E93E 56148083 734E6A8A


temp =
    EF628007 43C7CB83 2F07C89A 2C83B2B7 DFA75554 51B5ED66
    8AFA1BCE 3A515971 78045783 4A80E93E 56148083 734E6A8A


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 00E0E8FA 8A274E1C 52EC32FF 2DB7B20D
    E311A687 FEDCCE16 BA2174D6 4979CBC4 EE88E38C 5041CC14
    49D9025C D7CA8CDB 4BD4AB3A 723B82DD FAE3726C DF444484
    7695254A 0927E159 EA84D51C 358B1E09 F63C33CD B760C7CF
    2F0BC717 E1A7C79F 880522B3 EB10EF66 203FDFB8 BD78A4C9


Hash(counter||no_of_bits_to_return||input_string) is
    C09EAEFF 50386CEF C43FD862 A87AD414 8300FA72 B4D95F8D
    EC98BDB8 594237B3 B9226818 36323998 A07CDECE D262579F


temp =
    EF628007 43C7CB83 2F07C89A 2C83B2B7 DFA75554 51B5ED66
    8AFA1BCE 3A515971 78045783 4A80E93E 56148083 734E6A8A
    C09EAEFF 50386CEF C43FD862 A87AD414 8300FA72 B4D95F8D
    EC98BDB8 594237B3 B9226818 36323998 A07CDECE D262579F


------------

i = 3

counter||no_of_bits_to_return||input_string is
          03 00000378 00E0E8FA 8A274E1C 52EC32FF 2DB7B20D
    E311A687 FEDCCE16 BA2174D6 4979CBC4 EE88E38C 5041CC14
    49D9025C D7CA8CDB 4BD4AB3A 723B82DD FAE3726C DF444484
    7695254A 0927E159 EA84D51C 358B1E09 F63C33CD B760C7CF
    2F0BC717 E1A7C79F 880522B3 EB10EF66 203FDFB8 BD78A4C9
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
        C0E1040B 9FC9BD97 78F36A8B 145C5088 345FFC14 B02B3136
        3401857D 89571268 366A5B46 090E2B1C A276EA7F FFA9AB38


    temp =
                            EF6280 0743C7CB 832F07C8 9A2C83B2
        B7DFA755 5451B5ED 668AFA1B CE3A5159 71780457 834A80E9
        3E561480 83734E6A 8AC09EAE FF50386C EFC43FD8 62A87AD4
        148300FA 72B4D95F 8DEC98BD B8594237 B3B92268 18363239
        98A07CDE CED26257 9FC0E104 0B9FC9BD 9778F36A 8B145C50


  C is
                            EF6280 0743C7CB 832F07C8 9A2C83B2
        B7DFA755 5451B5ED 668AFA1B CE3A5159 71780457 834A80E9
        3E561480 83734E6A 8AC09EAE FF50386C EFC43FD8 62A87AD4
        148300FA 72B4D95F 8DEC98BD B8594237 B3B92268 18363239
        98A07CDE CED26257 9FC0E104 0B9FC9BD 9778F36A 8B145C50


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                            E0E8FA 8A274E1C 52EC32FF 2DB7B20D
        E311A687 FEDCCE16 BA2174D6 4979CBC4 EE88E38C 5041CC14
        49D9025C D7CA8CDB 4BD4AB3A 723B82DD FAE3726C DF444484
        7695254A 0927E159 EA84D51C 358B1E09 F63C33CD B760C7CF
        2F0BC717 E1A7C79F 880522B3 EB10EF66 203FDFB8 BD78A4C9
```

```
    w_i is
        82393433 28419150 D8FAC3F7 943AFD48 5EE0F857 4E7A7EDD
        730B7D03 92DFB8A5 D933AF34 0677BBA0 24BE0983 4D86442E


    W is
        82393433 28419150 D8FAC3F7 943AFD48 5EE0F857 4E7A7EDD
        730B7D03 92DFB8A5 D933AF34 0677BBA0 24BE0983 4D86442E


    ------------

    i = 2

    data is
                            E0E8FA 8A274E1C 52EC32FF 2DB7B20D
        E311A687 FEDCCE16 BA2174D6 4979CBC4 EE88E38C 5041CC14
        49D9025C D7CA8CDB 4BD4AB3A 723B82DD FAE3726C DF444484
        7695254A 0927E159 EA84D51C 358B1E09 F63C33CD B760C7CF
        2F0BC717 E1A7C79F 880522B3 EB10EF66 203FDFB8 BD78A4CA


    w_i is
        CCAAAA83 6BF42EC2 3A1A86B7 2A645474 81EE7644 2297D058
        8BFC4356 7F09029B 41EE880C 1A5D60C9 ED4E843B 46958E04


    W is
        82393433 28419150 D8FAC3F7 943AFD48 5EE0F857 4E7A7EDD
        730B7D03 92DFB8A5 D933AF34 0677BBA0 24BE0983 4D86442E
        CCAAAA83 6BF42EC2 3A1A86B7 2A645474 81EE7644 2297D058
        8BFC4356 7F09029B 41EE880C 1A5D60C9 ED4E843B 46958E04


  returned_bits is
        82393433 28419150 D8FAC3F7 943AFD48 5EE0F857 4E7A7EDD
        730B7D03 92DFB8A5 D933AF34 0677BBA0 24BE0983 4D86442E
        CCAAAA83 6BF42EC2 3A1A86B7 2A645474 81EE7644 2297D058
        8BFC4356 7F09029B 41EE880C 1A5D60C9 ED4E843B 46958E04


--------------------------

  Update V
```

```
    0x03||V is
                          03E0E8FA 8A274E1C 52EC32FF 2DB7B20D
        E311A687 FEDCCE16 BA2174D6 4979CBC4 EE88E38C 5041CC14
        49D9025C D7CA8CDB 4BD4AB3A 723B82DD FAE3726C DF444484
        7695254A 0927E159 EA84D51C 358B1E09 F63C33CD B760C7CF
        2F0BC717 E1A7C79F 880522B3 EB10EF66 203FDFB8 BD78A4C9


    H is
        BF25C69C 42BC7161 B9408D6E 99DB68D9 74D76E32 CA975077
        D05014FF D5B7585B F40CE7DC DACF1A12 A56048AA 983103E5


  Updated values

  V is
                            D04B7A 916B15E7 D61B3AC7 C7E435C0
        9AF14DDD 532E8404 20AC6EF2 17B41D1E 6000E7E3 D38C4CFD
        882F16DD 5B3DDB45 D69549E9 718BBB4A EAA7B245 41ECBF59
        4A3DECE0 BE992C1B 31B1FB48 87BFC91B 1ECCC468 9A2E4A80
        97FC58F6 86318253 1BD2EB94 D17FD336 5D191BCD E0BE04FF


  reseed_counter is
                                                0000 00000002


rnd_val is
        82393433 28419150 D8FAC3F7 943AFD48 5EE0F857 4E7A7EDD
        730B7D03 92DFB8A5 D933AF34 0677BBA0 24BE0983 4D86442E
        CCAAAA83 6BF42EC2 3A1A86B7 2A645474 81EE7644 2297D058
        8BFC4356 7F09029B 41EE880C 1A5D60C9 ED4E843B 46958E04


###############################################################

Hash_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
```

```
    0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
    2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
    3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
    5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


EntropyInput1 (for Reseed1) =
                         808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


EntropyInput2 (for Reseed2) =
                         C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Nonce =
                                20212223 24252627 28292A2B


PersonalizationString =
                         404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


AdditionalInput1 =
                         606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


AdditionalInput2 =
                         A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
```

DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E

##

****

Hash_DRBG_Instantiate_algorithm

entropy_input is
000102 03040506 0708090A 0B0C0D0E
0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E

nonce is
20212223 24252627 28292A2B

personal_str is
404142 43444546 4748494A 4B4C4D4E
4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE

prediction_resistance_flag = "PredictionResistance"

Hash_df - Generate seed(which is V) - Step 2

seed_material is
0001 02030405 06070809 0A0B0C0D 0E0F1011
12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596

```
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
      010000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
    A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
    EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964


temp =
    A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
    EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964


------------

i = 2

counter||no_of_bits_to_return||input_string is
      020000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
```

```
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
    C74754B6 A1E77C6C 0DE0245E 3BC81E15 85F2F379 F4489643
    5F61C23D B552DB8B 3190F5F3 7B966F3D D000CEB5 373CA2BD


temp =
    A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
    EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964
    C74754B6 A1E77C6C 0DE0245E 3BC81E15 85F2F379 F4489643
    5F61C23D B552DB8B 3190F5F3 7B966F3D D000CEB5 373CA2BD


------------

i = 3

counter||no_of_bits_to_return||input_string is
      030000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
    A8989587 CED14C8E 80790CD7 146F3328 3D84860A 708750EA
    1FDCD1DA D814E76A CA6E310F 12AA0BBA 611A8E86 FC0EAE47


temp =
                        A028F8 43783D77 21E32AC5 FD923031
    884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
    C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
    1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
    3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


V is
```

```
                          A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                         00A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


    Hash(counter||no_of_bits_to_return||input_string) is
        DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
        273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D


    temp =
        DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
        273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D


    ------------

    i = 2
```

```
counter||no_of_bits_to_return||input_string is
          02 00000378 00A028F8 43783D77 21E32AC5 FD923031
    884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
    C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
    1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
    3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


Hash(counter||no_of_bits_to_return||input_string) is
    7B72F966 9A700AF1 C7E3466A 5E89A0DC A45282E7 1A39E4AA
    24585736 11785015 85B95258 C40A2016 2D1F62CA 988BBEC7


temp =
    DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
    273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D
    7B72F966 9A700AF1 C7E3466A 5E89A0DC A45282E7 1A39E4AA
    24585736 11785015 85B95258 C40A2016 2D1F62CA 988BBEC7


------------

i = 3

counter||no_of_bits_to_return||input_string is
          03 00000378 00A028F8 43783D77 21E32AC5 FD923031
    884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
    C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
    1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
    3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


Hash(counter||no_of_bits_to_return||input_string) is
    FD2CAD8E 501A9FA7 18212A41 9FA2251F 01E46C40 DDBF4D85
    223B6E11 48351858 CC99BE10 6D1A4301 A307DBAF DE079ADA


temp =
                        DE0424 3D3BB302 329A9112 4D780ADC
    F3672DDD 2CE78196 3E273BB2 49F6EC13 B16A903F 40D01C2D
    FF1464BF A6AFD698 7D7B72F9 669A700A F1C7E346 6A5E89A0
    DCA45282 E71A39E4 AA245857 36117850 1585B952 58C40A20
    162D1F62 CA988BBE C7FD2CAD 8E501A9F A718212A 419FA225
```

```
  C is
                            DE0424 3D3BB302 329A9112 4D780ADC
        F3672DDD 2CE78196 3E273BB2 49F6EC13 B16A903F 40D01C2D
        FF1464BF A6AFD698 7D7B72F9 669A700A F1C7E346 6A5E89A0
        DCA45282 E71A39E4 AA245857 36117850 1585B952 58C40A20
        162D1F62 CA988BBE C7FD2CAD 8E501A9F A718212A 419FA225


---------------------------------------------------------------

First call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Generate FAILED: Reseed is required
---------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  additional_input
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

```
---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01A0 28F84378 3D7721E3 2AC5FD92 3031884C F9D3F05F
        A2BE09EB 6A82C782 B6203C29 3847B98E C4B9C0C8 674DEAE0
        9EB964C7 4754B6A1 E77C6C0D E0245E3B C81E1585 F2F379F4
        4896435F 61C23DB5 52DB8B31 90F5F37B 966F3DD0 00CEB537
        3CA2BDA8 989587CE D14C8E80 790CD714 6F338081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
        9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
        B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                          010000
        037801A0 28F84378 3D7721E3 2AC5FD92 3031884C F9D3F05F
        A2BE09EB 6A82C782 B6203C29 3847B98E C4B9C0C8 674DEAE0
        9EB964C7 4754B6A1 E77C6C0D E0245E3B C81E1585 F2F379F4
        4896435F 61C23DB5 52DB8B31 90F5F37B 966F3DD0 00CEB537
        3CA2BDA8 989587CE D14C8E80 790CD714 6F338081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
        9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
        B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

```
Hash(counter||no_of_bits_to_return||input_string) is
    DB62C08C B482A38A D2D4EABC 474050BD FB0D1344 FBE6BB0F
    5BBBAF71 6D2BDF7D D3BA3B46 CE78908F 2DEC6B26 3BD00FEB


temp =
    DB62C08C B482A38A D2D4EABC 474050BD FB0D1344 FBE6BB0F
    5BBBAF71 6D2BDF7D D3BA3B46 CE78908F 2DEC6B26 3BD00FEB


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
    037801A0 28F84378 3D7721E3 2AC5FD92 3031884C F9D3F05F
    A2BE09EB 6A82C782 B6203C29 3847B98E C4B9C0C8 674DEAE0
    9EB964C7 4754B6A1 E77C6C0D E0245E3B C81E1585 F2F379F4
    4896435F 61C23DB5 52DB8B31 90F5F37B 966F3DD0 00CEB537
    3CA2BDA8 989587CE D14C8E80 790CD714 6F338081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Hash(counter||no_of_bits_to_return||input_string) is
    C329E496 23AE4992 EADE0E6B CDC36DE3 4B03FC5C FD61A532
    5582D29B C2780A96 8CBB5376 004D708B AE3B054F 1CF82925


temp =
    DB62C08C B482A38A D2D4EABC 474050BD FB0D1344 FBE6BB0F
    5BBBAF71 6D2BDF7D D3BA3B46 CE78908F 2DEC6B26 3BD00FEB
    C329E496 23AE4992 EADE0E6B CDC36DE3 4B03FC5C FD61A532
    5582D29B C2780A96 8CBB5376 004D708B AE3B054F 1CF82925


------------
```

```
    i = 3

    counter||no_of_bits_to_return||input_string is
                                                          030000
        037801A0 28F84378 3D7721E3 2AC5FD92 3031884C F9D3F05F
        A2BE09EB 6A82C782 B6203C29 3847B98E C4B9C0C8 674DEAE0
        9EB964C7 4754B6A1 E77C6C0D E0245E3B C81E1585 F2F379F4
        4896435F 61C23DB5 52DB8B31 90F5F37B 966F3DD0 00CEB537
        3CA2BDA8 989587CE D14C8E80 790CD714 6F338081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
        9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
        B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    Hash(counter||no_of_bits_to_return||input_string) is
        094C757A B0DAE5E9 4BFCDC9A 5A049377 21DB8F8A 8FCBD7C2
        DE6DE5B7 6658B977 3F0B2FF8 B824D1CE D60B7FAB 387347B2


    temp =
                            DB62C0 8CB482A3 8AD2D4EA BC474050
        BDFB0D13 44FBE6BB 0F5BBBAF 716D2BDF 7DD3BA3B 46CE7890
        8F2DEC6B 263BD00F EBC329E4 9623AE49 92EADE0E 6BCDC36D
        E34B03FC 5CFD61A5 325582D2 9BC2780A 968CBB53 76004D70
        8BAE3B05 4F1CF829 25094C75 7AB0DAE5 E94BFCDC 9A5A0493


  V is
                            DB62C0 8CB482A3 8AD2D4EA BC474050
        BDFB0D13 44FBE6BB 0F5BBBAF 716D2BDF 7DD3BA3B 46CE7890
        8F2DEC6B 263BD00F EBC329E4 9623AE49 92EADE0E 6BCDC36D
        E34B03FC 5CFD61A5 325582D2 9BC2780A 968CBB53 76004D70
        8BAE3B05 4F1CF829 25094C75 7AB0DAE5 E94BFCDC 9A5A0493


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
```

```
                    00DB62C0 8CB482A3 8AD2D4EA BC474050
    BDFB0D13 44FBE6BB 0F5BBBAF 716D2BDF 7DD3BA3B 46CE7890
    8F2DEC6B 263BD00F EBC329E4 9623AE49 92EADE0E 6BCDC36D
    E34B03FC 5CFD61A5 325582D2 9BC2780A 968CBB53 76004D70
    8BAE3B05 4F1CF829 25094C75 7AB0DAE5 E94BFCDC 9A5A0493


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
          01 00000378 00DB62C0 8CB482A3 8AD2D4EA BC474050
    BDFB0D13 44FBE6BB 0F5BBBAF 716D2BDF 7DD3BA3B 46CE7890
    8F2DEC6B 263BD00F EBC329E4 9623AE49 92EADE0E 6BCDC36D
    E34B03FC 5CFD61A5 325582D2 9BC2780A 968CBB53 76004D70
    8BAE3B05 4F1CF829 25094C75 7AB0DAE5 E94BFCDC 9A5A0493


Hash(counter||no_of_bits_to_return||input_string) is
    1FD805B7 12393932 B7F08472 36B8A96E D29CE6CC 7D1880B8
    81F3DA77 2E8850D8 56BD997E 5D5E3B20 75EB584F 9ACE259F


temp =
    1FD805B7 12393932 B7F08472 36B8A96E D29CE6CC 7D1880B8
    81F3DA77 2E8850D8 56BD997E 5D5E3B20 75EB584F 9ACE259F


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 00DB62C0 8CB482A3 8AD2D4EA BC474050
    BDFB0D13 44FBE6BB 0F5BBBAF 716D2BDF 7DD3BA3B 46CE7890
    8F2DEC6B 263BD00F EBC329E4 9623AE49 92EADE0E 6BCDC36D
    E34B03FC 5CFD61A5 325582D2 9BC2780A 968CBB53 76004D70
    8BAE3B05 4F1CF829 25094C75 7AB0DAE5 E94BFCDC 9A5A0493


Hash(counter||no_of_bits_to_return||input_string) is
    BD78AB1A CF9171F9 DBBE44E4 EFA42A0E 152868CA 4B27D976
    8C2E7157 A70442A8 DC5CDBCE 8084BE66 09817B44 79C30028
```

```
    temp =
        1FD805B7 12393932 B7F08472 36B8A96E D29CE6CC 7D1880B8
        81F3DA77 2E8850D8 56BD997E 5D5E3B20 75EB584F 9ACE259F
        BD78AB1A CF9171F9 DBBE44E4 EFA42A0E 152868CA 4B27D976
        8C2E7157 A70442A8 DC5CDBCE 8084BE66 09817B44 79C30028


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
              03 00000378 00DB62C0 8CB482A3 8AD2D4EA BC474050
        BDFB0D13 44FBE6BB 0F5BBBAF 716D2BDF 7DD3BA3B 46CE7890
        8F2DEC6B 263BD00F EBC329E4 9623AE49 92EADE0E 6BCDC36D
        E34B03FC 5CFD61A5 325582D2 9BC2780A 968CBB53 76004D70
        8BAE3B05 4F1CF829 25094C75 7AB0DAE5 E94BFCDC 9A5A0493


    Hash(counter||no_of_bits_to_return||input_string) is
        00FA7F1A E23870A1 11626EB7 3116C82A 57E59BE5 129548E3
        3D5C183C BD8DE667 FF128572 CA8344FC 77E057DD 7F143B17


    temp =
                            1FD805 B7123939 32B7F084 7236B8A9
        6ED29CE6 CC7D1880 B881F3DA 772E8850 D856BD99 7E5D5E3B
        2075EB58 4F9ACE25 9FBD78AB 1ACF9171 F9DBBE44 E4EFA42A
        0E152868 CA4B27D9 768C2E71 57A70442 A8DC5CDB CE8084BE
        6609817B 4479C300 2800FA7F 1AE23870 A111626E B73116C8


  C is
                            1FD805 B7123939 32B7F084 7236B8A9
        6ED29CE6 CC7D1880 B881F3DA 772E8850 D856BD99 7E5D5E3B
        2075EB58 4F9ACE25 9FBD78AB 1ACF9171 F9DBBE44 E4EFA42A
        0E152868 CA4B27D9 768C2E71 57A70442 A8DC5CDB CE8084BE
        6609817B 4479C300 2800FA7F 1AE23870 A111626E B73116C8


**************************************************************

Hash_DRBG_Generate_algorithm
```

```
  requested_number_of_bits = 768

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                            DB62C0 8CB482A3 8AD2D4EA BC474050
        BDFB0D13 44FBE6BB 0F5BBBAF 716D2BDF 7DD3BA3B 46CE7890
        8F2DEC6B 263BD00F EBC329E4 9623AE49 92EADE0E 6BCDC36D
        E34B03FC 5CFD61A5 325582D2 9BC2780A 968CBB53 76004D70
        8BAE3B05 4F1CF829 25094C75 7AB0DAE5 E94BFCDC 9A5A0493


    w_i is
        9CEE8FCB 915311B3 70DD3599 14067376 F24D8568 000895E2
        B56CD255 3E468D26 B9171B62 21910E90 A290F051 1A6F7486


    W is
        9CEE8FCB 915311B3 70DD3599 14067376 F24D8568 000895E2
        B56CD255 3E468D26 B9171B62 21910E90 A290F051 1A6F7486


    ------------

    i = 2

    data is
                            DB62C0 8CB482A3 8AD2D4EA BC474050
        BDFB0D13 44FBE6BB 0F5BBBAF 716D2BDF 7DD3BA3B 46CE7890
        8F2DEC6B 263BD00F EBC329E4 9623AE49 92EADE0E 6BCDC36D
        E34B03FC 5CFD61A5 325582D2 9BC2780A 968CBB53 76004D70
        8BAE3B05 4F1CF829 25094C75 7AB0DAE5 E94BFCDC 9A5A0494


    w_i is
        E19F8EF6 44BFF873 2E1F022F 7CE483A8 E538E7B8 A979C647
```

```
        63128B4A 54B0D7E3 9ADCD785 FC94469B 2C02726A 55122901


    W is
        9CEE8FCB 915311B3 70DD3599 14067376 F24D8568 000895E2
        B56CD255 3E468D26 B9171B62 21910E90 A290F051 1A6F7486
        E19F8EF6 44BFF873 2E1F022F 7CE483A8 E538E7B8 A979C647
        63128B4A 54B0D7E3 9ADCD785 FC94469B 2C02726A 55122901


  returned_bits is
        9CEE8FCB 915311B3 70DD3599 14067376 F24D8568 000895E2
        B56CD255 3E468D26 B9171B62 21910E90 A290F051 1A6F7486
        E19F8EF6 44BFF873 2E1F022F 7CE483A8 E538E7B8 A979C647
        63128B4A 54B0D7E3 9ADCD785 FC94469B 2C02726A 55122901


---------------------------

  Update V

    0x03||V is
                           03DB62C0 8CB482A3 8AD2D4EA BC474050
        BDFB0D13 44FBE6BB 0F5BBBAF 716D2BDF 7DD3BA3B 46CE7890
        8F2DEC6B 263BD00F EBC329E4 9623AE49 92EADE0E 6BCDC36D
        E34B03FC 5CFD61A5 325582D2 9BC2780A 968CBB53 76004D70
        8BAE3B05 4F1CF829 25094C75 7AB0DAE5 E94BFCDC 9A5A0493


    H is
        7A5A7039 09050FFC 52DC3BF5 9896C6A5 34E03732 C39B5756
        EDA3A9F6 D53E815F 9738EB81 5AE6F94B F9A785CA 8D4FC634


  Updated values

  V is
                             FB3AC6 43C6BBDC BD8AC56F 2E7DF8FA
        2CCDA9FA 1178FF3B C7DDAF89 E89BB430 562A77D4 C52BD6CB
        AFA3D7C3 75D69E35 8B80A28F B0F33FBB 8CC69C53 50BD6798
        6BBA9C9E 304D997A FBBDED39 8C0042F2 74494F62 081C2985
        DF5B6677 68D53C88 E4433275 F07A0CA2 8404E515 DEDAE190


  reseed_counter is
                                                0000 00000002
```

```
rnd_val is
        9CEE8FCB 915311B3 70DD3599 14067376 F24D8568 000895E2
        B56CD255 3E468D26 B9171B62 21910E90 A290F051 1A6F7486
        E19F8EF6 44BFF873 2E1F022F 7CE483A8 E538E7B8 A979C647
        63128B4A 54B0D7E3 9ADCD785 FC94469B 2C02726A 55122901


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Generate FAILED: Reseed is required
---------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  additional_input
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E
```

```
---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01FB 3AC643C6 BBDCBD8A C56F2E7D F8FA2CCD A9FA1178
        FF3BC7DD AF89E89B B430562A 77D4C52B D6CBAFA3 D7C375D6
        9E358B80 A28FB0F3 3FBB8CC6 9C5350BD 67986BBA 9C9E304D
        997AFBBD ED398C00 42F27449 4F62081C 2985DF5B 667768D5
        3C88E443 3275F07A 0CA28404 E515DEDA E190C0C1 C2C3C4C5
        C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
        DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                        010000
        037801FB 3AC643C6 BBDCBD8A C56F2E7D F8FA2CCD A9FA1178
        FF3BC7DD AF89E89B B430562A 77D4C52B D6CBAFA3 D7C375D6
        9E358B80 A28FB0F3 3FBB8CC6 9C5350BD 67986BBA 9C9E304D
        997AFBBD ED398C00 42F27449 4F62081C 2985DF5B 667768D5
        3C88E443 3275F07A 0CA28404 E515DEDA E190C0C1 C2C3C4C5
        C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
        DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E
```

```
Hash(counter||no_of_bits_to_return||input_string) is
    1C5C55A6 39ABE953 F81466FB 846F8CCC 974D024A CB68AA22
    11C29FA0 3D9766E7 6E5A87A0 805211E0 C28A85E7 82DE92FE


temp =
    1C5C55A6 39ABE953 F81466FB 846F8CCC 974D024A CB68AA22
    11C29FA0 3D9766E7 6E5A87A0 805211E0 C28A85E7 82DE92FE


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
    037801FB 3AC643C6 BBDCBD8A C56F2E7D F8FA2CCD A9FA1178
    FF3BC7DD AF89E89B B430562A 77D4C52B D6CBAFA3 D7C375D6
    9E358B80 A28FB0F3 3FBB8CC6 9C5350BD 67986BBA 9C9E304D
    997AFBBD ED398C00 42F27449 4F62081C 2985DF5B 667768D5
    3C88E443 3275F07A 0CA28404 E515DEDA E190C0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Hash(counter||no_of_bits_to_return||input_string) is
    0C89980C 03D37FC8 C9649303 3B5FF024 E3A13BD3 CB950C82
    42DAD044 CD1C4B3A ACE28237 4D967B21 4075B091 0E1FC16A


temp =
    1C5C55A6 39ABE953 F81466FB 846F8CCC 974D024A CB68AA22
    11C29FA0 3D9766E7 6E5A87A0 805211E0 C28A85E7 82DE92FE
    0C89980C 03D37FC8 C9649303 3B5FF024 E3A13BD3 CB950C82
    42DAD044 CD1C4B3A ACE28237 4D967B21 4075B091 0E1FC16A


------------
```

```
    i = 3

    counter||no_of_bits_to_return||input_string is
                                                          030000
        037801FB 3AC643C6 BBDCBD8A C56F2E7D F8FA2CCD A9FA1178
        FF3BC7DD AF89E89B B430562A 77D4C52B D6CBAFA3 D7C375D6
        9E358B80 A28FB0F3 3FBB8CC6 9C5350BD 67986BBA 9C9E304D
        997AFBBD ED398C00 42F27449 4F62081C 2985DF5B 667768D5
        3C88E443 3275F07A 0CA28404 E515DEDA E190C0C1 C2C3C4C5
        C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
        DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    Hash(counter||no_of_bits_to_return||input_string) is
        DA59C63A 7AD92A5E 050568E6 2A96FA0F 16DE14AD 3E4597F1
        C9215E33 B203E5EC A0182C22 D2A34099 83219A8A A89B1666


    temp =
                            1C5C55 A639ABE9 53F81466 FB846F8C
        CC974D02 4ACB68AA 2211C29F A03D9766 E76E5A87 A0805211
        E0C28A85 E782DE92 FE0C8998 0C03D37F C8C96493 033B5FF0
        24E3A13B D3CB950C 8242DAD0 44CD1C4B 3AACE282 374D967B
        214075B0 910E1FC1 6ADA59C6 3A7AD92A 5E050568 E62A96FA


  V is
                            1C5C55 A639ABE9 53F81466 FB846F8C
        CC974D02 4ACB68AA 2211C29F A03D9766 E76E5A87 A0805211
        E0C28A85 E782DE92 FE0C8998 0C03D37F C8C96493 033B5FF0
        24E3A13B D3CB950C 8242DAD0 44CD1C4B 3AACE282 374D967B
        214075B0 910E1FC1 6ADA59C6 3A7AD92A 5E050568 E62A96FA


--------------------------

  Hash_df - Generate C - Step 4
```

```
0x00||V is
                      001C5C55 A639ABE9 53F81466 FB846F8C
    CC974D02 4ACB68AA 2211C29F A03D9766 E76E5A87 A0805211
    E0C28A85 E782DE92 FE0C8998 0C03D37F C8C96493 033B5FF0
    24E3A13B D3CB950C 8242DAD0 44CD1C4B 3AACE282 374D967B
    214075B0 910E1FC1 6ADA59C6 3A7AD92A 5E050568 E62A96FA


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
          01 00000378 001C5C55 A639ABE9 53F81466 FB846F8C
    CC974D02 4ACB68AA 2211C29F A03D9766 E76E5A87 A0805211
    E0C28A85 E782DE92 FE0C8998 0C03D37F C8C96493 033B5FF0
    24E3A13B D3CB950C 8242DAD0 44CD1C4B 3AACE282 374D967B
    214075B0 910E1FC1 6ADA59C6 3A7AD92A 5E050568 E62A96FA


Hash(counter||no_of_bits_to_return||input_string) is
    143C078E 3B909E09 9399AB04 683F27CF B77221F7 BBB9720C
    1ED63F27 C6664449 B8536D54 35EFFA5F C13B937D 0FE423F5


temp =
    143C078E 3B909E09 9399AB04 683F27CF B77221F7 BBB9720C
    1ED63F27 C6664449 B8536D54 35EFFA5F C13B937D 0FE423F5


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 001C5C55 A639ABE9 53F81466 FB846F8C
    CC974D02 4ACB68AA 2211C29F A03D9766 E76E5A87 A0805211
    E0C28A85 E782DE92 FE0C8998 0C03D37F C8C96493 033B5FF0
    24E3A13B D3CB950C 8242DAD0 44CD1C4B 3AACE282 374D967B
    214075B0 910E1FC1 6ADA59C6 3A7AD92A 5E050568 E62A96FA


Hash(counter||no_of_bits_to_return||input_string) is
    12176168 89B7B466 7CF9CAFA 266048EA 24BA75B7 9E9A8093
```

```
        E14C3AA1 A44F3007 5351D077 412E08A3 8BB9CE5A CAC9B822


    temp =
        143C078E 3B909E09 9399AB04 683F27CF B77221F7 BBB9720C
        1ED63F27 C6664449 B8536D54 35EFFA5F C13B937D 0FE423F5
        12176168 89B7B466 7CF9CAFA 266048EA 24BA75B7 9E9A8093
        E14C3AA1 A44F3007 5351D077 412E08A3 8BB9CE5A CAC9B822


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
              03 00000378 001C5C55 A639ABE9 53F81466 FB846F8C
        CC974D02 4ACB68AA 2211C29F A03D9766 E76E5A87 A0805211
        E0C28A85 E782DE92 FE0C8998 0C03D37F C8C96493 033B5FF0
        24E3A13B D3CB950C 8242DAD0 44CD1C4B 3AACE282 374D967B
        214075B0 910E1FC1 6ADA59C6 3A7AD92A 5E050568 E62A96FA


    Hash(counter||no_of_bits_to_return||input_string) is
        F6D9E446 0241694F 2DD12B6C FB07BC69 C9022603 DCE63FA7
        FDAFCA3A B05C0F3B BA73DAB0 4E0E3977 F0C0BC0C DA52464C


    temp =
                            143C07 8E3B909E 099399AB 04683F27
        CFB77221 F7BBB972 0C1ED63F 27C66644 49B8536D 5435EFFA
        5FC13B93 7D0FE423 F5121761 6889B7B4 667CF9CA FA266048
        EA24BA75 B79E9A80 93E14C3A A1A44F30 075351D0 77412E08
        A38BB9CE 5ACAC9B8 22F6D9E4 46024169 4F2DD12B 6CFB07BC


  C is
                            143C07 8E3B909E 099399AB 04683F27
        CFB77221 F7BBB972 0C1ED63F 27C66644 49B8536D 5435EFFA
        5FC13B93 7D0FE423 F5121761 6889B7B4 667CF9CA FA266048
        EA24BA75 B79E9A80 93E14C3A A1A44F30 075351D0 77412E08
        A38BB9CE 5ACAC9B8 22F6D9E4 46024169 4F2DD12B 6CFB07BC


**************************************************************

Hash_DRBG_Generate_algorithm
```

```
  requested_number_of_bits = 768

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                            1C5C55 A639ABE9 53F81466 FB846F8C
        CC974D02 4ACB68AA 2211C29F A03D9766 E76E5A87 A0805211
        E0C28A85 E782DE92 FE0C8998 0C03D37F C8C96493 033B5FF0
        24E3A13B D3CB950C 8242DAD0 44CD1C4B 3AACE282 374D967B
        214075B0 910E1FC1 6ADA59C6 3A7AD92A 5E050568 E62A96FA


    w_i is
        476727C7 96489765 62C987DA 997128A7 5CD23971 265F89E6
        65448938 1A619DE0 AB3E707E 2A071A47 FD5D5B09 2711A6E4


    W is
        476727C7 96489765 62C987DA 997128A7 5CD23971 265F89E6
        65448938 1A619DE0 AB3E707E 2A071A47 FD5D5B09 2711A6E4


    ------------

    i = 2

    data is
                            1C5C55 A639ABE9 53F81466 FB846F8C
        CC974D02 4ACB68AA 2211C29F A03D9766 E76E5A87 A0805211
        E0C28A85 E782DE92 FE0C8998 0C03D37F C8C96493 033B5FF0
        24E3A13B D3CB950C 8242DAD0 44CD1C4B 3AACE282 374D967B
        214075B0 910E1FC1 6ADA59C6 3A7AD92A 5E050568 E62A96FB


    w_i is
```

```
        69E20CEE 2F5A18DE E45988E5 A02EA991 40DB6EB6 F74B703D
        1D56C025 08AF1E8E 6033B480 26CED342 C0A0FF4C 00DE1DE5


    W is
        476727C7 96489765 62C987DA 997128A7 5CD23971 265F89E6
        65448938 1A619DE0 AB3E707E 2A071A47 FD5D5B09 2711A6E4
        69E20CEE 2F5A18DE E45988E5 A02EA991 40DB6EB6 F74B703D
        1D56C025 08AF1E8E 6033B480 26CED342 C0A0FF4C 00DE1DE5


  returned_bits is
        476727C7 96489765 62C987DA 997128A7 5CD23971 265F89E6
        65448938 1A619DE0 AB3E707E 2A071A47 FD5D5B09 2711A6E4
        69E20CEE 2F5A18DE E45988E5 A02EA991 40DB6EB6 F74B703D
        1D56C025 08AF1E8E 6033B480 26CED342 C0A0FF4C 00DE1DE5


--------------------------

  Update V

    0x03||V is
                          031C5C55 A639ABE9 53F81466 FB846F8C
        CC974D02 4ACB68AA 2211C29F A03D9766 E76E5A87 A0805211
        E0C28A85 E782DE92 FE0C8998 0C03D37F C8C96493 033B5FF0
        24E3A13B D3CB950C 8242DAD0 44CD1C4B 3AACE282 374D967B
        214075B0 910E1FC1 6ADA59C6 3A7AD92A 5E050568 E62A96FA


    H is
        858F0D53 6D7F0A1D E63050A9 8502F779 3800C351 9083D52C
        B182332F 1C7D372C 586404E6 6940B71D D0EAF869 6ECF536D


  Updated values

  V is
                            30985D 34753C87 5D8BAE11 FFECAEB4
        9C4EBF24 4287221C 2E3098DE C803FDAB 3126ADF4 F4B6420C
        4083C619 6492C2B6 F31EA0F9 748D8B34 2F465E5D FD61C039
        94976904 F8E939AA FC5477B4 6B7462F4 7A00F7A4 3F1299B0
        764E62AE 085620A5 E6353890 E9BDD1B1 7E1DCEFD C1F4F224


  reseed_counter is
```

0000 00000002

rnd_val is
476727C7 96489765 62C987DA 997128A7 5CD23971 265F89E6
65448938 1A619DE0 AB3E707E 2A071A47 FD5D5B09 2711A6E4
69E20CEE 2F5A18DE E45988E5 A02EA991 40DB6EB6 F74B703D
1D56C025 08AF1E8E 6033B480 26CED342 C0A0FF4C 00DE1DE5

```
##############################################################

Hash_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                           20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput = <empty>

##############################################################

**************************************************************

Hash_DRBG_Instantiate_algorithm
```

```
    entropy_input is
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                           20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                    01000003 78000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
                      152D908B 0EDF7253 D5D19F0A F96518D3
    AD33F2EF 3151A0C9 56D9D3EE 6DC08B70 F1EB7598 2501CE67
    BB7294F1 BC43B322 DCD25C14 67212CAB 0CD5E695 4C5B6F6A


temp =
                      152D908B 0EDF7253 D5D19F0A F96518D3
    AD33F2EF 3151A0C9 56D9D3EE 6DC08B70 F1EB7598 2501CE67
    BB7294F1 BC43B322 DCD25C14 67212CAB 0CD5E695 4C5B6F6A


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                02000003 78000102 03040506
    0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
    1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
    3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


Hash(counter||no_of_bits_to_return||input_string) is
                      D466C1D9 AC010D21 B28CD9FD 124DF56D
    4D3B75B9 604827B3 CF49928E C4DA204F C374888E 278C0319
    DB45E1FD 3BCAD38C C355D2D6 55C1D606 60AEA6D6 BBE4E7C1


temp =
                        152D90 8B0EDF72 53D5D19F 0AF96518
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
    6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
    B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


V is
                        152D90 8B0EDF72 53D5D19F 0AF96518
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
    6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
    B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3
```

```
---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
        6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
        B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
        6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
        B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


    Hash(counter||no_of_bits_to_return||input_string) is
                          2B22189F 32CB92C1 508BC343 69B8C37F
        D9593FD9 EC56B559 844E605D 67B4A586 2F1C7B75 3F68DF75
        10BE1F64 A7AAB557 9821195F FF0357CC 5464CAC5 D07655D6


    temp =
                          2B22189F 32CB92C1 508BC343 69B8C37F
        D9593FD9 EC56B559 844E605D 67B4A586 2F1C7B75 3F68DF75
        10BE1F64 A7AAB557 9821195F FF0357CC 5464CAC5 D07655D6


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
              02 00000378 00152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
```

```
        6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
        B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


    Hash(counter||no_of_bits_to_return||input_string) is
                         051F8441 D411B910 71605B9A 44B6643E
        67225358 2AE3148F 4A57E8FD A8E81155 108E4AFC C0E939BF
        D95FAB62 E8B1E4FD BDA34B60 C9220A37 EC6BD096 A6DAE159


    temp =
                           2B2218 9F32CB92 C1508BC3 4369B8C3
        7FD9593F D9EC56B5 59844E60 5D67B4A5 862F1C7B 753F68DF
        7510BE1F 64A7AAB5 57982119 5FFF0357 CC5464CA C5D07655
        D6051F84 41D411B9 1071605B 9A44B664 3E672253 582AE314
        8F4A57E8 FDA8E811 55108E4A FCC0E939 BFD95FAB 62E8B1E4


  C is
                           2B2218 9F32CB92 C1508BC3 4369B8C3
        7FD9593F D9EC56B5 59844E60 5D67B4A5 862F1C7B 753F68DF
        7510BE1F 64A7AAB5 57982119 5FFF0357 CC5464CA C5D07655
        D6051F84 41D411B9 1071605B 9A44B664 3E672253 582AE314
        8F4A57E8 FDA8E811 55108E4A FCC0E939 BFD95FAB 62E8B1E4


---------------------------------------------------------------

First call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------
```

```
i = 1

data is
                        152D90 8B0EDF72 53D5D19F 0AF96518
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
    6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
    B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


w_i is
                      170CC707 C71C69CE 45C43CBA FF521014
    0572D478 59521BA1 3141BADD 2E5B9A7B 3E802062 5CD8893F
    D6A4739C 581ED5BE 7FA3148A 05D7F54A E9EADAE8 F1A7194D


W is
                      170CC707 C71C69CE 45C43CBA FF521014
    0572D478 59521BA1 3141BADD 2E5B9A7B 3E802062 5CD8893F
    D6A4739C 581ED5BE 7FA3148A 05D7F54A E9EADAE8 F1A7194D


------------

i = 2

data is
                        152D90 8B0EDF72 53D5D19F 0AF96518
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
    6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
    B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD4


w_i is
                      F94B6B75 5B948E0C 27E1747F 02F663D6
    B514A0F5 86F94E53 D32169E1 CCC6211A D0348124 19B6BA8F
    3C829304 898393BF 39E57E2F EDF775FC 6E5EB0E3 07EDCA0B


W is
                                          170CC707 C71C69CE
    45C43CBA FF521014 0572D478 59521BA1 3141BADD 2E5B9A7B
    3E802062 5CD8893F D6A4739C 581ED5BE 7FA3148A 05D7F54A
    E9EADAE8 F1A7194D F94B6B75 5B948E0C 27E1747F 02F663D6
    B514A0F5 86F94E53 D32169E1 CCC6211A D0348124 19B6BA8F
```

```
       3C829304 898393BF 39E57E2F EDF775FC 6E5EB0E3 07EDCA0B


  returned_bits is
                                                 170CC707 C71C69CE
       45C43CBA FF521014 0572D478 59521BA1 3141BADD 2E5B9A7B
       3E802062 5CD8893F D6A4739C 581ED5BE 7FA3148A 05D7F54A
       E9EADAE8 F1A7194D F94B6B75 5B948E0C 27E1747F 02F663D6
       B514A0F5 86F94E53 D32169E1 CCC6211A D0348124 19B6BA8F
       3C829304 898393BF 39E57E2F EDF775FC 6E5EB0E3 07EDCA0B


--------------------------

  Update V

    0x03||V is
                          03152D90 8B0EDF72 53D5D19F 0AF96518
       D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
       67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
       6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
       B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


    H is
                          DB1068C4 546A551B 34DEFD9B 7C714A81
       3F648F40 D44A98B7 C5E730ED D5CB6EC3 B665FCA6 9A490F4F
       7C033201 72F4A20D 632C24D0 A0833718 A57BAA63 AA2E269E


  Updated values

  V is
                            404FA9 2A41AB05 15265D62 4E631DDC
       53868D32 C91DA856 22DB2834 4BD57530 F72107F1 0D646AAD
       DCCC30B4 5663EE69 55855C39 C8D0799F AC40384C D78E1C46
       803E1586 EFCAAB7D F80B1E23 6D22731D 621A5A6F ABD43A8B
       BF1CD37C FF62643F 080027A4 2B6BAC55 7F304FF1 0A52A356


  reseed_counter is
                                                     0000 00000002


rnd_val is
                                                 170CC707 C71C69CE
```

```
        45C43CBA FF521014 0572D478 59521BA1 3141BADD 2E5B9A7B
        3E802062 5CD8893F D6A4739C 581ED5BE 7FA3148A 05D7F54A
        E9EADAE8 F1A7194D F94B6B75 5B948E0C 27E1747F 02F663D6
        B514A0F5 86F94E53 D32169E1 CCC6211A D0348124 19B6BA8F
        3C829304 898393BF 39E57E2F EDF775FC 6E5EB0E3 07EDCA0B


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                          404FA9 2A41AB05 15265D62 4E631DDC
        53868D32 C91DA856 22DB2834 4BD57530 F72107F1 0D646AAD
        DCCC30B4 5663EE69 55855C39 C8D0799F AC40384C D78E1C46
        803E1586 EFCAAB7D F80B1E23 6D22731D 621A5A6F ABD43A8B
        BF1CD37C FF62643F 080027A4 2B6BAC55 7F304FF1 0A52A356


    w_i is
                         D515B92B 1811F5AA D02AAC9B 39DFA5B8
        B1A95048 7D3429B1 081D0FEC 28D57686 D85BC6B4 5AB8B84C
        54DD80B2 82591F55 07ED9B3F B1CDEEFD 58AD5A98 12ED929C


    W is
                         D515B92B 1811F5AA D02AAC9B 39DFA5B8
        B1A95048 7D3429B1 081D0FEC 28D57686 D85BC6B4 5AB8B84C
```

```
        54DD80B2 82591F55 07ED9B3F B1CDEEFD 58AD5A98 12ED929C


    ------------

    i = 2

    data is
                            404FA9 2A41AB05 15265D62 4E631DDC
        53868D32 C91DA856 22DB2834 4BD57530 F72107F1 0D646AAD
        DCCC30B4 5663EE69 55855C39 C8D0799F AC40384C D78E1C46
        803E1586 EFCAAB7D F80B1E23 6D22731D 621A5A6F ABD43A8B
        BF1CD37C FF62643F 080027A4 2B6BAC55 7F304FF1 0A52A357


    w_i is
                          779B0F54 BADF2CAF BACFACB3 ECACC127
        C7640CBB 67154F54 5A622BE0 A9B552A2 4208313B FA491F53
        AAA3074B DC48BC5B DB3FF0E2 D05BB477 B59F87E3 A1EAB3E6


    W is
                                             D515B92B 1811F5AA
        D02AAC9B 39DFA5B8 B1A95048 7D3429B1 081D0FEC 28D57686
        D85BC6B4 5AB8B84C 54DD80B2 82591F55 07ED9B3F B1CDEEFD
        58AD5A98 12ED929C 779B0F54 BADF2CAF BACFACB3 ECACC127
        C7640CBB 67154F54 5A622BE0 A9B552A2 4208313B FA491F53
        AAA3074B DC48BC5B DB3FF0E2 D05BB477 B59F87E3 A1EAB3E6


  returned_bits is
                                             D515B92B 1811F5AA
        D02AAC9B 39DFA5B8 B1A95048 7D3429B1 081D0FEC 28D57686
        D85BC6B4 5AB8B84C 54DD80B2 82591F55 07ED9B3F B1CDEEFD
        58AD5A98 12ED929C 779B0F54 BADF2CAF BACFACB3 ECACC127
        C7640CBB 67154F54 5A622BE0 A9B552A2 4208313B FA491F53
        AAA3074B DC48BC5B DB3FF0E2 D05BB477 B59F87E3 A1EAB3E6


--------------------------

  Update V

    0x03||V is
                          03404FA9 2A41AB05 15265D62 4E631DDC
        53868D32 C91DA856 22DB2834 4BD57530 F72107F1 0D646AAD
```

```
        DCCC30B4 5663EE69 55855C39 C8D0799F AC40384C D78E1C46
        803E1586 EFCAAB7D F80B1E23 6D22731D 621A5A6F ABD43A8B
        BF1CD37C FF62643F 080027A4 2B6BAC55 7F304FF1 0A52A356


    H is
                         21A210E7 77772CDB 2F0C82FD 86A05AA6
        691E02D8 DCCC8546 F427A69B FFF1CA7B 189EB235 85E48648
        64134F01 F2824DD7 92BBBA16 5B61BB5E A840C4DC AA129622


  Updated values

  V is
                           6B71C1 C9747697 D676E925 91CCD69F
        D35FE672 A309FF0B 7C5F7694 A93D29D6 7D50246C 82A3D38D
        51DCEED3 BB0B991E CEBF8E3A A046A9D2 A7A12015 23FEED42
        BF6137E4 0E6B427D FCA4251B 0758F3FC B9202EF8 89E3A3E8
        B27A7A67 EF8D9A27 EFCC7005 838E50ED E74A7479 174DEB5E


  reseed_counter is
                                                0000 00000003


rnd_val is
                                              D515B92B 1811F5AA
        D02AAC9B 39DFA5B8 B1A95048 7D3429B1 081D0FEC 28D57686
        D85BC6B4 5AB8B84C 54DD80B2 82591F55 07ED9B3F B1CDEEFD
        58AD5A98 12ED929C 779B0F54 BADF2CAF BACFACB3 ECACC127
        C7640CBB 67154F54 5A622BE0 A9B552A2 4208313B FA491F53
        AAA3074B DC48BC5B DB3FF0E2 D05BB477 B59F87E3 A1EAB3E6


##################################################################

Hash_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                           000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
```

```
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput1 =
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    AdditionalInput2 =
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E

################################################################

****************************************************************
```

```
Hash_DRBG_Instantiate_algorithm

    entropy_input is
                              000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                           20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                   01000003 78000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F
```

```
  Hash(counter||no_of_bits_to_return||input_string) is
                        152D908B 0EDF7253 D5D19F0A F96518D3
      AD33F2EF 3151A0C9 56D9D3EE 6DC08B70 F1EB7598 2501CE67
      BB7294F1 BC43B322 DCD25C14 67212CAB 0CD5E695 4C5B6F6A


  temp =
                        152D908B 0EDF7253 D5D19F0A F96518D3
      AD33F2EF 3151A0C9 56D9D3EE 6DC08B70 F1EB7598 2501CE67
      BB7294F1 BC43B322 DCD25C14 67212CAB 0CD5E695 4C5B6F6A


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                                02000003 78000102 03040506
      0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
      1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
      3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
      4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
      6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


  Hash(counter||no_of_bits_to_return||input_string) is
                        D466C1D9 AC010D21 B28CD9FD 124DF56D
      4D3B75B9 604827B3 CF49928E C4DA204F C374888E 278C0319
      DB45E1FD 3BCAD38C C355D2D6 55C1D606 60AEA6D6 BBE4E7C1


  temp =
                          152D90 8B0EDF72 53D5D19F 0AF96518
      D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
      67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
      6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
      B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


V is
                          152D90 8B0EDF72 53D5D19F 0AF96518
      D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
      67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
      6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
      B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3
```

```
---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
        6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
        B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
        6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
        B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


    Hash(counter||no_of_bits_to_return||input_string) is
                          2B22189F 32CB92C1 508BC343 69B8C37F
        D9593FD9 EC56B559 844E605D 67B4A586 2F1C7B75 3F68DF75
        10BE1F64 A7AAB557 9821195F FF0357CC 5464CAC5 D07655D6


    temp =
                          2B22189F 32CB92C1 508BC343 69B8C37F
        D9593FD9 EC56B559 844E605D 67B4A586 2F1C7B75 3F68DF75
        10BE1F64 A7AAB557 9821195F FF0357CC 5464CAC5 D07655D6


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
              02 00000378 00152D90 8B0EDF72 53D5D19F 0AF96518
```

```
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
        6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
        B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


    Hash(counter||no_of_bits_to_return||input_string) is
                            051F8441 D411B910 71605B9A 44B6643E
        67225358 2AE3148F 4A57E8FD A8E81155 108E4AFC C0E939BF
        D95FAB62 E8B1E4FD BDA34B60 C9220A37 EC6BD096 A6DAE159


    temp =
                              2B2218 9F32CB92 C1508BC3 4369B8C3
        7FD9593F D9EC56B5 59844E60 5D67B4A5 862F1C7B 753F68DF
        7510BE1F 64A7AAB5 57982119 5FFF0357 CC5464CA C5D07655
        D6051F84 41D411B9 1071605B 9A44B664 3E672253 582AE314
        8F4A57E8 FDA8E811 55108E4A FCC0E939 BFD95FAB 62E8B1E4


  C is
                              2B2218 9F32CB92 C1508BC3 4369B8C3
        7FD9593F D9EC56B5 59844E60 5D67B4A5 862F1C7B 753F68DF
        7510BE1F 64A7AAB5 57982119 5FFF0357 CC5464CA C5D07655
        D6051F84 41D411B9 1071605B 9A44B664 3E672253 582AE314
        8F4A57E8 FDA8E811 55108E4A FCC0E939 BFD95FAB 62E8B1E4


----------------------------------------------------------------

First call to Generate

****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input
                              606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

```
---------------------------

  Process additional_input

    0x02||V||additional_input is
                                                 02152D 908B0EDF
        7253D5D1 9F0AF965 18D3AD33 F2EF3151 A0C956D9 D3EE6DC0
        8B70F1EB 75982501 CE67BB72 94F1BC43 B322DCD2 5C146721
        2CAB0CD5 E6954C5B 6F6AD466 C1D9AC01 0D21B28C D9FD124D
        F56D4D3B 75B96048 27B3CF49 928EC4DA 204FC374 888E278C
        0319DB45 E1FD3BCA D3606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    w=Hash(0x02||V||additional_input) is
                          79FD8B26 36E78437 378D4914 89E1A32D
        D89A9B62 4AD030DD E1748E57 D996D7DB 727AF114 4808A659
        52CBF908 7F4379BC 9DB1D25B 78D27EC8 BDC583D7 63C3122E


    V is
                            152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 9CDA5D82 4B4EA563 E29A1EFB 1F2DFE9D
        436F0224 247C31EB 03271B31 D6A925D0 DFC82C8A 0168EE81
        069B429B 0E0853DC ED7546E4 06FA0ACB D7A0C9B9 60FEDD01


---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                            152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 9CDA5D82 4B4EA563 E29A1EFB 1F2DFE9D
        436F0224 247C31EB 03271B31 D6A925D0 DFC82C8A 0168EE81
```

```
    069B429B 0E0853DC ED7546E4 06FA0ACB D7A0C9B9 60FEDD01


  w_i is
                       3EF283D8 E1A5F5A8 D5D8AD9C 45577576
    DD018161 387C97B3 2EB5A104 A9649E9E DC85F9E4 DF40A823
    A66E5494 CB3FB655 99D81A02 E415704C A738D2C8 D5020C42


  W is
                       3EF283D8 E1A5F5A8 D5D8AD9C 45577576
    DD018161 387C97B3 2EB5A104 A9649E9E DC85F9E4 DF40A823
    A66E5494 CB3FB655 99D81A02 E415704C A738D2C8 D5020C42


  ------------

  i = 2

  data is
                         152D90 8B0EDF72 53D5D19F 0AF96518
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 9CDA5D82 4B4EA563 E29A1EFB 1F2DFE9D
    436F0224 247C31EB 03271B31 D6A925D0 DFC82C8A 0168EE81
    069B429B 0E0853DC ED7546E4 06FA0ACB D7A0C9B9 60FEDD02


  w_i is
                       08F364A8 750251A8 74AF6FFD 88638094
    8B7138A6 81E093B5 32A6E67E 9F3AC97E 1364A1E2 BC8E1121
    5771CA69 4D933FCF 86CD3500 121AD1AF 66821B61 92BE3C97


  W is
                                          3EF283D8 E1A5F5A8
    D5D8AD9C 45577576 DD018161 387C97B3 2EB5A104 A9649E9E
    DC85F9E4 DF40A823 A66E5494 CB3FB655 99D81A02 E415704C
    A738D2C8 D5020C42 08F364A8 750251A8 74AF6FFD 88638094
    8B7138A6 81E093B5 32A6E67E 9F3AC97E 1364A1E2 BC8E1121
    5771CA69 4D933FCF 86CD3500 121AD1AF 66821B61 92BE3C97


returned_bits is
                                          3EF283D8 E1A5F5A8
    D5D8AD9C 45577576 DD018161 387C97B3 2EB5A104 A9649E9E
    DC85F9E4 DF40A823 A66E5494 CB3FB655 99D81A02 E415704C
```

```
        A738D2C8 D5020C42 08F364A8 750251A8 74AF6FFD 88638094
        8B7138A6 81E093B5 32A6E67E 9F3AC97E 1364A1E2 BC8E1121
        5771CA69 4D933FCF 86CD3500 121AD1AF 66821B61 92BE3C97


---------------------------

  Update V

    0x03||V is
                          03152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 9CDA5D82 4B4EA563 E29A1EFB 1F2DFE9D
        436F0224 247C31EB 03271B31 D6A925D0 DFC82C8A 0168EE81
        069B429B 0E0853DC ED7546E4 06FA0ACB D7A0C9B9 60FEDD01


    H is
                          E2C0A9BB 3EF85708 AA5C141C 81558C82
        383E2BB6 27DAE468 AB6C9849 CC42948C 7068AD57 D722FDCF
        AA7FE7D4 C792F1A1 0FA378F9 21534BAE 4F52B5CE 6E324F13


  Updated values

  V is
                            404FA9 2A41AB05 15265D62 4E631DDC
        53868D32 C91DA856 22DB2834 4BD57530 F72107F1 0D646AAD
        DCCC30B4 5663EE69 D7332856 EA45FFC4 594A97E2 66540175
        51B24D5E 8E2B280C BF0513D7 3D3070C1 8E97FC35 30B6CF65
        40658258 D3442D8F 52294E28 250E3FB3 E6CCDF33 3219DDF9


  reseed_counter is
                                                0000 00000002


rnd_val is
                                             3EF283D8 E1A5F5A8
        D5D8AD9C 45577576 DD018161 387C97B3 2EB5A104 A9649E9E
        DC85F9E4 DF40A823 A66E5494 CB3FB655 99D81A02 E415704C
        A738D2C8 D5020C42 08F364A8 750251A8 74AF6FFD 88638094
        8B7138A6 81E093B5 32A6E67E 9F3AC97E 1364A1E2 BC8E1121
        5771CA69 4D933FCF 86CD3500 121AD1AF 66821B61 92BE3C97
```

```
-----------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


---------------------------

  Process additional_input

    0x02||V||additional_input is
                                              02404F A92A41AB
        0515265D 624E631D DC53868D 32C91DA8 5622DB28 344BD575
        30F72107 F10D646A ADDCCC30 B45663EE 69D73328 56EA45FF
        C4594A97 E2665401 7551B24D 5E8E2B28 0CBF0513 D73D3070
        C18E97FC 3530B6CF 65406582 58D3442D 8F52294E 28250E3F
        B3E6CCDF 333219DD F9A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    w=Hash(0x02||V||additional_input) is
                         16873523 6B8FA61E 40744598 B64BD50D
        F278C925 8E1A8849 E2EA3F54 70867ABA D5E797B3 C459A0F2
        64B9F8F8 8B5500D6 FDDB804E 6ED9134E EA77C7BF B255702F


    V is
                           404FA9 2A41AB05 15265D62 4E631DDC
        53868D32 C91DA856 22DB2834 4BD57530 F72107F1 0D646AAD
        DCCC30B4 5663EE69 EDBA5D7A 55D5A5E2 99BEDD7B 1C9FD683
        442B1684 1C45B056 A1EF532B ADB6EB7C 647F93E8 F5107057
```

```
        A51F7B51 5E992E66 5004CE76 93E75302 D144A6F2 E46F4E28


---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                            404FA9 2A41AB05 15265D62 4E631DDC
        53868D32 C91DA856 22DB2834 4BD57530 F72107F1 0D646AAD
        DCCC30B4 5663EE69 EDBA5D7A 55D5A5E2 99BEDD7B 1C9FD683
        442B1684 1C45B056 A1EF532B ADB6EB7C 647F93E8 F5107057
        A51F7B51 5E992E66 5004CE76 93E75302 D144A6F2 E46F4E28


    w_i is
                           8EB0575C E1500BB0 52259F8A 995DC7AE
        F54FBD38 E9CE6AEA F3F05FA7 0768AF36 99A24D90 BF60E3E6
        509B4326 A5473B2C E98DE137 DB06EF9F 03A125BF 1367DEFB


    W is
                           8EB0575C E1500BB0 52259F8A 995DC7AE
        F54FBD38 E9CE6AEA F3F05FA7 0768AF36 99A24D90 BF60E3E6
        509B4326 A5473B2C E98DE137 DB06EF9F 03A125BF 1367DEFB


    ------------

    i = 2

    data is
                            404FA9 2A41AB05 15265D62 4E631DDC
        53868D32 C91DA856 22DB2834 4BD57530 F72107F1 0D646AAD
        DCCC30B4 5663EE69 EDBA5D7A 55D5A5E2 99BEDD7B 1C9FD683
        442B1684 1C45B056 A1EF532B ADB6EB7C 647F93E8 F5107057
        A51F7B51 5E992E66 5004CE76 93E75302 D144A6F2 E46F4E29


    w_i is
```

```
                        8098633F A2EF8493 454F6792 F1F94C52
        5282EEC9 D0352D93 B966966B AA85DBAC 596B3240 E2E28D35
        E71E7B73 05C92473 AE706480 E9061CD8 DA37F147 700B67B8


    W is
                                              8EB0575C E1500BB0
        52259F8A 995DC7AE F54FBD38 E9CE6AEA F3F05FA7 0768AF36
        99A24D90 BF60E3E6 509B4326 A5473B2C E98DE137 DB06EF9F
        03A125BF 1367DEFB 8098633F A2EF8493 454F6792 F1F94C52
        5282EEC9 D0352D93 B966966B AA85DBAC 596B3240 E2E28D35
        E71E7B73 05C92473 AE706480 E9061CD8 DA37F147 700B67B8


  returned_bits is
                                              8EB0575C E1500BB0
        52259F8A 995DC7AE F54FBD38 E9CE6AEA F3F05FA7 0768AF36
        99A24D90 BF60E3E6 509B4326 A5473B2C E98DE137 DB06EF9F
        03A125BF 1367DEFB 8098633F A2EF8493 454F6792 F1F94C52
        5282EEC9 D0352D93 B966966B AA85DBAC 596B3240 E2E28D35
        E71E7B73 05C92473 AE706480 E9061CD8 DA37F147 700B67B8


---------------------------

  Update V

    0x03||V is
                        03404FA9 2A41AB05 15265D62 4E631DDC
        53868D32 C91DA856 22DB2834 4BD57530 F72107F1 0D646AAD
        DCCC30B4 5663EE69 EDBA5D7A 55D5A5E2 99BEDD7B 1C9FD683
        442B1684 1C45B056 A1EF532B ADB6EB7C 647F93E8 F5107057
        A51F7B51 5E992E66 5004CE76 93E75302 D144A6F2 E46F4E28


    H is
                        A2513F21 58ED78EB 67F6DA75 18BA4DEA
        E2E65C34 302C18FC 88A55FD2 0D84168D FF0297D3 D129D4B7
        B0B35603 CE3C2BDF 5E7A617D 5EC2FAC6 049C7270 C0C39507


  Updated values

  V is
                          6B71C1 C9747697 D676E925 91CCD69F
        D35FE672 A309FF0B 7C5F7694 A93D29D6 7D50246C 82A3D38D
```

```
        51DCEED3 BB0B991F E7A3BDB5 0EC22225 CE0A1CBA FB2A9AC3
        FD16923C 8E45DB0C 3B061359 557FB86E A1E94E10 1E652823
        E51D293E 2A7E4257 038FBE3E EF6B3702 95BA790F 081B9515


  reseed_counter is
                                                 0000 00000003


rnd_val is
                                               8EB0575C E1500BB0
        52259F8A 995DC7AE F54FBD38 E9CE6AEA F3F05FA7 0768AF36
        99A24D90 BF60E3E6 509B4326 A5473B2C E98DE137 DB06EF9F
        03A125BF 1367DEFB 8098633F A2EF8493 454F6792 F1F94C52
        5282EEC9 D0352D93 B966966B AA85DBAC 596B3240 E2E28D35
        E71E7B73 05C92473 AE706480 E9061CD8 DA37F147 700B67B8


################################################################

Hash_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
```

```
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString =
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    AdditionalInput = <empty>

###############################################################

***************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                          20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "No PredictionResistance"
```

```
---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                          010000
        03780001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    Hash(counter||no_of_bits_to_return||input_string) is
                          E5A5C585 D6A9E11C 58581F35 14EE19A7
        048CF096 A3E9B139 D9C0A2C0 67931041 4073C104 E2F6F8A3
        7C7C666E 11FF4439 33ABA1CF AD4C620C DFF5DA8C 0860CEEE


    temp =
                          E5A5C585 D6A9E11C 58581F35 14EE19A7
```

```
        048CF096 A3E9B139 D9C0A2C0 67931041 4073C104 E2F6F8A3
        7C7C666E 11FF4439 33ABA1CF AD4C620C DFF5DA8C 0860CEEE


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                        020000
        03780001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    Hash(counter||no_of_bits_to_return||input_string) is
                          80B87195 7508538D 2D87A4A3 B5728ADB
        4191974A 384F323D 2E585869 5C152F99 D0E8CF4C B41BC2A6
        12955B4C 4838B9FB EB00568D 36F727E1 742FF774 E8542A4B


    temp =
                            E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


  V is
                            E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


--------------------------
```

```
Hash_df - Generate C - Step 4

  0x00||V is
                       00E5A5C5 85D6A9E1 1C58581F 3514EE19
      A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
      A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
      EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
      3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


  no_of_bits_to_return = 888

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
            01 00000378 00E5A5C5 85D6A9E1 1C58581F 3514EE19
      A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
      A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
      EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
      3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


  Hash(counter||no_of_bits_to_return||input_string) is
                       0C193DBC 1942C121 C63513ED 95ECA91C
      62C55031 7506462C 47B0F34F 99716F36 EAD9FF51 ACAB423C
      421CAB62 DF4D8C79 2E38D533 9D60AA24 0292E134 A249A577


  temp =
                       0C193DBC 1942C121 C63513ED 95ECA91C
      62C55031 7506462C 47B0F34F 99716F36 EAD9FF51 ACAB423C
      421CAB62 DF4D8C79 2E38D533 9D60AA24 0292E134 A249A577


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
            02 00000378 00E5A5C5 85D6A9E1 1C58581F 3514EE19
      A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
      A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
      EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
      3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                          0176FE93 A4C199A2 258615DD A840AE6F
        C2E7DB39 1315119E 57774F94 396C81F5 F8D4835D 618D960B
        297E97F1 A21B35E3 E450A877 4819D918 961DFC01 FFC73630


    temp =
                            0C193D BC1942C1 21C63513 ED95ECA9
        1C62C550 31750646 2C47B0F3 4F99716F 36EAD9FF 51ACAB42
        3C421CAB 62DF4D8C 792E38D5 339D60AA 240292E1 34A249A5
        770176FE 93A4C199 A2258615 DDA840AE 6FC2E7DB 39131511
        9E57774F 94396C81 F5F8D483 5D618D96 0B297E97 F1A21B35


  C is
                            0C193D BC1942C1 21C63513 ED95ECA9
        1C62C550 31750646 2C47B0F3 4F99716F 36EAD9FF 51ACAB42
        3C421CAB 62DF4D8C 792E38D5 339D60AA 240292E1 34A249A5
        770176FE 93A4C199 A2258615 DDA840AE 6FC2E7DB 39131511
        9E57774F 94396C81 F5F8D483 5D618D96 0B297E97 F1A21B35


---------------------------------------------------------------

First call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1
```

```
data is
                        E5A5C5 85D6A9E1 1C58581F 3514EE19
    A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
    A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
    EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
    3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


w_i is
                      B72E446C 3985DA7B F5009134 C2C59BAF
    7918AEA7 27FAC3CA 39C31DD6 45357AC9 168DA218 027BD5D8
    642C1306 895765A0 4757EF52 F4D81C55 8DE70751 3FE96C08


W is
                      B72E446C 3985DA7B F5009134 C2C59BAF
    7918AEA7 27FAC3CA 39C31DD6 45357AC9 168DA218 027BD5D8
    642C1306 895765A0 4757EF52 F4D81C55 8DE70751 3FE96C08


------------

i = 2

data is
                        E5A5C5 85D6A9E1 1C58581F 3514EE19
    A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
    A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
    EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
    3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838BA


w_i is
                      56E390B1 45F5B016 A3649D07 A1A9F5C6
    DF1E27A8 830451DB FA12AB97 70A998D7 AD7D3EB3 488328FF
    874E6C12 94A60539 199C9A99 C75BFE5F A0446DAE 248E0DCB


W is
                                        B72E446C 3985DA7B
    F5009134 C2C59BAF 7918AEA7 27FAC3CA 39C31DD6 45357AC9
    168DA218 027BD5D8 642C1306 895765A0 4757EF52 F4D81C55
    8DE70751 3FE96C08 56E390B1 45F5B016 A3649D07 A1A9F5C6
    DF1E27A8 830451DB FA12AB97 70A998D7 AD7D3EB3 488328FF
    874E6C12 94A60539 199C9A99 C75BFE5F A0446DAE 248E0DCB
```

```
  returned_bits is
                                                B72E446C 3985DA7B
        F5009134 C2C59BAF 7918AEA7 27FAC3CA 39C31DD6 45357AC9
        168DA218 027BD5D8 642C1306 895765A0 4757EF52 F4D81C55
        8DE70751 3FE96C08 56E390B1 45F5B016 A3649D07 A1A9F5C6
        DF1E27A8 830451DB FA12AB97 70A998D7 AD7D3EB3 488328FF
        874E6C12 94A60539 199C9A99 C75BFE5F A0446DAE 248E0DCB


---------------------------

  Update V

    0x03||V is
                          03E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


    H is
                          BBC2684F FBE0AA6C E4E6F228 15A9A70E
        B8B8749B 143EAC0C EEB60CAF F29BC1D7 3B76C880 78C8D124
        ABD77981 93EB39CE 0AC5380A 7A5F0F30 4559F487 AE775A58


  Updated values

  V is
                            F1BF03 41EFECA2 3E1E8D33 22AADAC2
        C3675240 C818EFF7 66217196 1001047F 782B4DC0 568FA23A
        DFBE9911 D0F14CD1 6E244CC6 FF2B5779 15C97AE3 D6545183
        1E3AA40B 3D5875FA 1E091A6A 73F97510 867B41F2 FC143568
        875D4929 9180BB7F 9A8EF55D 2474B888 F696087A EC61AE47


  reseed_counter is
                                                    0000 00000002


rnd_val is
                                                B72E446C 3985DA7B
        F5009134 C2C59BAF 7918AEA7 27FAC3CA 39C31DD6 45357AC9
        168DA218 027BD5D8 642C1306 895765A0 4757EF52 F4D81C55
```

```
        8DE70751 3FE96C08 56E390B1 45F5B016 A3649D07 A1A9F5C6
        DF1E27A8 830451DB FA12AB97 70A998D7 AD7D3EB3 488328FF
        874E6C12 94A60539 199C9A99 C75BFE5F A0446DAE 248E0DCB


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                           F1BF03 41EFECA2 3E1E8D33 22AADAC2
        C3675240 C818EFF7 66217196 1001047F 782B4DC0 568FA23A
        DFBE9911 D0F14CD1 6E244CC6 FF2B5779 15C97AE3 D6545183
        1E3AA40B 3D5875FA 1E091A6A 73F97510 867B41F2 FC143568
        875D4929 9180BB7F 9A8EF55D 2474B888 F696087A EC61AE47


    w_i is
                         557C2284 16B46E30 A3E703F6 A5270130
        7003615D 0DFCD1D4 F5E1F147 BAB4461F 4AF69FE4 13AAA932
        F537BA0B BEF93FA0 BA6EE187 8B86312A E9259DEC 73D73F27


    W is
                         557C2284 16B46E30 A3E703F6 A5270130
        7003615D 0DFCD1D4 F5E1F147 BAB4461F 4AF69FE4 13AAA932
        F537BA0B BEF93FA0 BA6EE187 8B86312A E9259DEC 73D73F27
```

```
    ------------

    i = 2

    data is
                            F1BF03 41EFECA2 3E1E8D33 22AADAC2
        C3675240 C818EFF7 66217196 1001047F 782B4DC0 568FA23A
        DFBE9911 D0F14CD1 6E244CC6 FF2B5779 15C97AE3 D6545183
        1E3AA40B 3D5875FA 1E091A6A 73F97510 867B41F2 FC143568
        875D4929 9180BB7F 9A8EF55D 2474B888 F696087A EC61AE48


    w_i is
                           345DFCFC F7D18E29 CF66DE2C 0615AF35
        A6C9218C E1EF2DA9 4C865A47 7A64FAC3 9D21D344 F19F8344
        53C68BC1 5FD929B2 B9B32D71 0E145F08 DA0FBD5E 0924061C


    W is
                                              557C2284 16B46E30
        A3E703F6 A5270130 7003615D 0DFCD1D4 F5E1F147 BAB4461F
        4AF69FE4 13AAA932 F537BA0B BEF93FA0 BA6EE187 8B86312A
        E9259DEC 73D73F27 345DFCFC F7D18E29 CF66DE2C 0615AF35
        A6C9218C E1EF2DA9 4C865A47 7A64FAC3 9D21D344 F19F8344
        53C68BC1 5FD929B2 B9B32D71 0E145F08 DA0FBD5E 0924061C


  returned_bits is
                                              557C2284 16B46E30
        A3E703F6 A5270130 7003615D 0DFCD1D4 F5E1F147 BAB4461F
        4AF69FE4 13AAA932 F537BA0B BEF93FA0 BA6EE187 8B86312A
        E9259DEC 73D73F27 345DFCFC F7D18E29 CF66DE2C 0615AF35
        A6C9218C E1EF2DA9 4C865A47 7A64FAC3 9D21D344 F19F8344
        53C68BC1 5FD929B2 B9B32D71 0E145F08 DA0FBD5E 0924061C


---------------------------

  Update V

    0x03||V is
                           03F1BF03 41EFECA2 3E1E8D33 22AADAC2
        C3675240 C818EFF7 66217196 1001047F 782B4DC0 568FA23A
        DFBE9911 D0F14CD1 6E244CC6 FF2B5779 15C97AE3 D6545183
        1E3AA40B 3D5875FA 1E091A6A 73F97510 867B41F2 FC143568
```

```
        875D4929 9180BB7F 9A8EF55D 2474B888 F696087A EC61AE47


    H is
                            58EB8BE5 2DA8F5EC 0D2DDCF9 B0FF4F6C
        3445EDCC FC8549EF DAC23C18 C5186B2B 0AB36AC6 89C6A2B1
        A7C06102 8BD219DE 86891787 9EE72862 8E008E8B 5F193920


  Updated values

  V is
                              FDD840 FE092F63 5FE4C247 1040C76B
        DFCA1790 F98DF63D 92692289 5F9A75EE AF1627BF A83C4D7D
        1C00B5BD 33D09A5E 403E1181 6071AE0F 46F9EABE BBF5EA94
        C98208D6 CD828183 9AF0DC99 16BA20EA 00F19494 BEEDED2B
        CD75217B B18C41E0 1710E168 20BD6E81 8FC0159E 3D1D029E


  reseed_counter is
                                                  0000 00000003


rnd_val is
                                               557C2284 16B46E30
        A3E703F6 A5270130 7003615D 0DFCD1D4 F5E1F147 BAB4461F
        4AF69FE4 13AAA932 F537BA0B BEF93FA0 BA6EE187 8B86312A
        E9259DEC 73D73F27 345DFCFC F7D18E29 CF66DE2C 0615AF35
        A6C9218C E1EF2DA9 4C865A47 7A64FAC3 9D21D344 F19F8344
        53C68BC1 5FD929B2 B9B32D71 0E145F08 DA0FBD5E 0924061C


##############################################################

Hash_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                              000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
```

```
    5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


EntropyInput1 (for Reseed1) =
                         808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


EntropyInput2 (for Reseed2) =
                         C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Nonce =
                       20212223 24252627 28292A2B 2C2D2E2F


PersonalizationString =
                         404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


AdditionalInput1 =
                         606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


AdditionalInput2 =
                         A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E
```

```
################################################################

****************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                           20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
                             404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
```

```
no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                                        010000
    03780001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
    46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
    5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
    2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
                      E5A5C585 D6A9E11C 58581F35 14EE19A7
    048CF096 A3E9B139 D9C0A2C0 67931041 4073C104 E2F6F8A3
    7C7C666E 11FF4439 33ABA1CF AD4C620C DFF5DA8C 0860CEEE


temp =
                      E5A5C585 D6A9E11C 58581F35 14EE19A7
    048CF096 A3E9B139 D9C0A2C0 67931041 4073C104 E2F6F8A3
    7C7C666E 11FF4439 33ABA1CF AD4C620C DFF5DA8C 0860CEEE


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                        020000
    03780001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
    46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
    5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
    2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
```

```
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    Hash(counter||no_of_bits_to_return||input_string) is
                          80B87195 7508538D 2D87A4A3 B5728ADB
        4191974A 384F323D 2E585869 5C152F99 D0E8CF4C B41BC2A6
        12955B4C 4838B9FB EB00568D 36F727E1 742FF774 E8542A4B


    temp =
                            E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


  V is
                            E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00E5A5C5 85D6A9E1 1C58581F 3514EE19
```

```
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


    Hash(counter||no_of_bits_to_return||input_string) is
                            0C193DBC 1942C121 C63513ED 95ECA91C
        62C55031 7506462C 47B0F34F 99716F36 EAD9FF51 ACAB423C
        421CAB62 DF4D8C79 2E38D533 9D60AA24 0292E134 A249A577


    temp =
                            0C193DBC 1942C121 C63513ED 95ECA91C
        62C55031 7506462C 47B0F34F 99716F36 EAD9FF51 ACAB423C
        421CAB62 DF4D8C79 2E38D533 9D60AA24 0292E134 A249A577


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
              02 00000378 00E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


    Hash(counter||no_of_bits_to_return||input_string) is
                            0176FE93 A4C199A2 258615DD A840AE6F
        C2E7DB39 1315119E 57774F94 396C81F5 F8D4835D 618D960B
        297E97F1 A21B35E3 E450A877 4819D918 961DFC01 FFC73630


    temp =
                              0C193D BC1942C1 21C63513 ED95ECA9
        1C62C550 31750646 2C47B0F3 4F99716F 36EAD9FF 51ACAB42
        3C421CAB 62DF4D8C 792E38D5 339D60AA 240292E1 34A249A5
        770176FE 93A4C199 A2258615 DDA840AE 6FC2E7DB 39131511
        9E57774F 94396C81 F5F8D483 5D618D96 0B297E97 F1A21B35


C is
                            0C193D BC1942C1 21C63513 ED95ECA9
```

```
        1C62C550 31750646 2C47B0F3 4F99716F 36EAD9FF 51ACAB42
        3C421CAB 62DF4D8C 792E38D5 339D60AA 240292E1 34A249A5
        770176FE 93A4C199 A2258615 DDA840AE 6FC2E7DB 39131511
        9E57774F 94396C81 F5F8D483 5D618D96 0B297E97 F1A21B35


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input
                           606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


--------------------------

  Process additional_input

    0x02||V||additional_input is
                                              02E5A5 C585D6A9
        E11C5858 1F3514EE 19A7048C F096A3E9 B139D9C0 A2C06793
        10414073 C104E2F6 F8A37C7C 666E11FF 443933AB A1CFAD4C
        620CDFF5 DA8C0860 CEEE80B8 71957508 538D2D87 A4A3B572
        8ADB4191 974A384F 323D2E58 58695C15 2F99D0E8 CF4CB41B
        C2A61295 5B4C4838 B9606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    w=Hash(0x02||V||additional_input) is
                          45751730 26074982 F90C7520 DCB4E495
        C5560C97 F73D6910 A6DD9382 06980B1B 59811FF1 2923D007
        9CBCA198 7ADA2DBB D41C17E6 6D8CBA09 1EA4006D 10B606BE
```

```
    V is
                            E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 7EA8C2D1 F5B495E5 05EC6AFB 68BD4564
        B3D6C509 8CB27164 340B1B26 AA4D7DA6 34C2B188 735C1F39
        D9EAF9F0 E43642EB 6DED00B5 BA40D5CB C4B695C8 5CFE3F77


---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                            E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 7EA8C2D1 F5B495E5 05EC6AFB 68BD4564
        B3D6C509 8CB27164 340B1B26 AA4D7DA6 34C2B188 735C1F39
        D9EAF9F0 E43642EB 6DED00B5 BA40D5CB C4B695C8 5CFE3F77


    w_i is
                           DA126CF9 5C6BF97E 2F731F21 37A907AC
        C70FD7AC 9EBACD1C 6E31C740 29B052E3 AABC48F3 B00993F2
        B2381F76 50A55322 A968C86E 05DE88E6 367F6EF8 9A601DB4


    W is
                           DA126CF9 5C6BF97E 2F731F21 37A907AC
        C70FD7AC 9EBACD1C 6E31C740 29B052E3 AABC48F3 B00993F2
        B2381F76 50A55322 A968C86E 05DE88E6 367F6EF8 9A601DB4


    ------------

    i = 2

    data is
                            E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
```

```
        A37C7C66 6E11FF44 7EA8C2D1 F5B495E5 05EC6AFB 68BD4564
        B3D6C509 8CB27164 340B1B26 AA4D7DA6 34C2B188 735C1F39
        D9EAF9F0 E43642EB 6DED00B5 BA40D5CB C4B695C8 5CFE3F78


    w_i is
                         342E9086 C7AC13B5 E56C32E9 E668040B
        73847893 C5BFD38A 1CF44F34 8B4EEE4C D68ADB7E 7B8C837F
        19BC4F90 2761F7CF F24AB1D7 04FD11C4 E929D855 3753B55D


    W is
                                           DA126CF9 5C6BF97E
        2F731F21 37A907AC C70FD7AC 9EBACD1C 6E31C740 29B052E3
        AABC48F3 B00993F2 B2381F76 50A55322 A968C86E 05DE88E6
        367F6EF8 9A601DB4 342E9086 C7AC13B5 E56C32E9 E668040B
        73847893 C5BFD38A 1CF44F34 8B4EEE4C D68ADB7E 7B8C837F
        19BC4F90 2761F7CF F24AB1D7 04FD11C4 E929D855 3753B55D


  returned_bits is
                                           DA126CF9 5C6BF97E
        2F731F21 37A907AC C70FD7AC 9EBACD1C 6E31C740 29B052E3
        AABC48F3 B00993F2 B2381F76 50A55322 A968C86E 05DE88E6
        367F6EF8 9A601DB4 342E9086 C7AC13B5 E56C32E9 E668040B
        73847893 C5BFD38A 1CF44F34 8B4EEE4C D68ADB7E 7B8C837F
        19BC4F90 2761F7CF F24AB1D7 04FD11C4 E929D855 3753B55D


---------------------------

  Update V

    0x03||V is
                         03E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 7EA8C2D1 F5B495E5 05EC6AFB 68BD4564
        B3D6C509 8CB27164 340B1B26 AA4D7DA6 34C2B188 735C1F39
        D9EAF9F0 E43642EB 6DED00B5 BA40D5CB C4B695C8 5CFE3F77


    H is
                         C9F3F96E 42CF0833 F5230A54 B1846C4C
        07E4282C 2851B4A5 91561F87 062D7A87 0016631E 18E3B559
        256B7E72 D0E2B60F DF2912BE BE24D3B0 9E2F4334 10A7E1F7
```

```
  Updated values

  V is
                            F1BF03 41EFECA2 3E1E8D33 22AADAC2
        C3675240 C818EFF7 66217196 1001047F 782B4DC0 568FA23A
        DFBE9911 D0F14CD1 C1CAF515 6C20FEC3 1F120831 4EE3FB56
        32BC6434 48A8E7A3 6786C0C3 8E2338DB A49BFC81 C552E9A4
        9DADEFB3 4952657D 430EE7F7 D5C73712 6E0F5794 5F483CA4


  reseed_counter is
                                                0000 00000002


rnd_val is
                                              DA126CF9 5C6BF97E
        2F731F21 37A907AC C70FD7AC 9EBACD1C 6E31C740 29B052E3
        AABC48F3 B00993F2 B2381F76 50A55322 A968C86E 05DE88E6
        367F6EF8 9A601DB4 342E9086 C7AC13B5 E56C32E9 E668040B
        73847893 C5BFD38A 1CF44F34 8B4EEE4C D68ADB7E 7B8C837F
        19BC4F90 2761F7CF F24AB1D7 04FD11C4 E929D855 3753B55D


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


--------------------------

  Process additional_input
```

0x02||V||additional_input is

02F1BF 0341EFEC
A23E1E8D 3322AADA C2C36752 40C818EF F7662171 96100104
7F782B4D C0568FA2 3ADFBE99 11D0F14C D1C1CAF5 156C20FE
C31F1208 314EE3FB 5632BC64 3448A8E7 A36786C0 C38E2338
DBA49BFC 81C552E9 A49DADEF B3495265 7D430EE7 F7D5C737
126E0F57 945F483C A4A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E

w=Hash(0x02||V||additional_input) is

144F2001 03C8A031 4B9926FF C2B70B97
494663C9 A27EEC51 A44E9281 6BC1BB05 22FE594A AFE4574D
AC175FFD 3320DB34 C7D1AD98 3A94C970 740F7C27 F178D3EE

V is

F1BF03 41EFECA2 3E1E8D33 22AADAC2
C3675240 C818EFF7 66217196 1001047F 782B4DC0 568FA23A
DFBE9911 D0F14CD1 D61A1516 6FE99EF4 6AAB2F31 119B06ED
7C02C7FD EB27D3F5 0BD55344 F9E4F3E0 C79A55CC 753740F2
49C54FB0 7C7340B2 0AE09590 105C0082 E21ED3BC 50C11092

Hashgen

requested_no_of_bits = 1024

---

i = 1

data is

F1BF03 41EFECA2 3E1E8D33 22AADAC2
C3675240 C818EFF7 66217196 1001047F 782B4DC0 568FA23A
DFBE9911 D0F14CD1 D61A1516 6FE99EF4 6AAB2F31 119B06ED
7C02C7FD EB27D3F5 0BD55344 F9E4F3E0 C79A55CC 753740F2
49C54FB0 7C7340B2 0AE09590 105C0082 E21ED3BC 50C11092

w_i is

```
                      400B977C E8A2BB6A 84C6FD1C F9014596
    85ABF540 8CFF4588 CEDF52E2 D2DC300A A9B4FAED 8CD0161C
    2172B1FD 26925319 5883D6EB F21020F2 C20E5F2C 81AE60C8


  W is
                      400B977C E8A2BB6A 84C6FD1C F9014596
    85ABF540 8CFF4588 CEDF52E2 D2DC300A A9B4FAED 8CD0161C
    2172B1FD 26925319 5883D6EB F21020F2 C20E5F2C 81AE60C8


  ------------

  i = 2

  data is
                        F1BF03 41EFECA2 3E1E8D33 22AADAC2
    C3675240 C818EFF7 66217196 1001047F 782B4DC0 568FA23A
    DFBE9911 D0F14CD1 D61A1516 6FE99EF4 6AAB2F31 119B06ED
    7C02C7FD EB27D3F5 0BD55344 F9E4F3E0 C79A55CC 753740F2
    49C54FB0 7C7340B2 0AE09590 105C0082 E21ED3BC 50C11093


  w_i is
                      595B834A 229B1F5B 726C1125 717E6207
    8886EF38 E61E3270 7AD5F811 6C6393DF B6E7C7AE 0E8E92BB
    D7E0C3D0 4BBA02F5 169F2F56 9A581589 15FEE4C9 D28D45DB


  W is
                                        400B977C E8A2BB6A
    84C6FD1C F9014596 85ABF540 8CFF4588 CEDF52E2 D2DC300A
    A9B4FAED 8CD0161C 2172B1FD 26925319 5883D6EB F21020F2
    C20E5F2C 81AE60C8 595B834A 229B1F5B 726C1125 717E6207
    8886EF38 E61E3270 7AD5F811 6C6393DF B6E7C7AE 0E8E92BB
    D7E0C3D0 4BBA02F5 169F2F56 9A581589 15FEE4C9 D28D45DB


returned_bits is
                                        400B977C E8A2BB6A
    84C6FD1C F9014596 85ABF540 8CFF4588 CEDF52E2 D2DC300A
    A9B4FAED 8CD0161C 2172B1FD 26925319 5883D6EB F21020F2
    C20E5F2C 81AE60C8 595B834A 229B1F5B 726C1125 717E6207
    8886EF38 E61E3270 7AD5F811 6C6393DF B6E7C7AE 0E8E92BB
    D7E0C3D0 4BBA02F5 169F2F56 9A581589 15FEE4C9 D28D45DB
```

```
---------------------------

  Update V

    0x03||V is
                          03F1BF03 41EFECA2 3E1E8D33 22AADAC2
        C3675240 C818EFF7 66217196 1001047F 782B4DC0 568FA23A
        DFBE9911 D0F14CD1 D61A1516 6FE99EF4 6AAB2F31 119B06ED
        7C02C7FD EB27D3F5 0BD55344 F9E4F3E0 C79A55CC 753740F2
        49C54FB0 7C7340B2 0AE09590 105C0082 E21ED3BC 50C11092


    H is
                          AF6B255D F26B42E3 135836C5 FF96BDB5
        5D6642FA D8346A99 27BA263E 0478B510 1FBC8FFA 358E930C
        CE1DE3F0 CA627639 B9A936F7 EEE22574 27C4B8CE E193F4C0


  Updated values

  V is
                            FDD840 FE092F63 5FE4C247 1040C76B
        DFCA1790 F98DF63D 92692289 5F9A75EE AF1627BF A83C4D7D
        1C00B5BD 33D09A5E FEB37349 95F24281 A205F8D8 45D40E48
        506A81F7 57010027 D5B4FF98 DC05E99F 5719CDA1 E3D8E910
        B63AAAF0 DB0F236D BA82A10B 5C9FB38D 150D0B23 23F72089


  reseed_counter is
                                                0000 00000003


rnd_val is
                                              400B977C E8A2BB6A
        84C6FD1C F9014596 85ABF540 8CFF4588 CEDF52E2 D2DC300A
        A9B4FAED 8CD0161C 2172B1FD 26925319 5883D6EB F21020F2
        C20E5F2C 81AE60C8 595B834A 229B1F5B 726C1125 717E6207
        8886EF38 E61E3270 7AD5F811 6C6393DF B6E7C7AE 0E8E92BB
        D7E0C3D0 4BBA02F5 169F2F56 9A581589 15FEE4C9 D28D45DB


################################################################

Hash_DRBG
```

```
    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                           000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                           808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                           C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                           000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
```

```
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                            20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                    01000003 78000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    Hash(counter||no_of_bits_to_return||input_string) is
                            152D908B 0EDF7253 D5D19F0A F96518D3
        AD33F2EF 3151A0C9 56D9D3EE 6DC08B70 F1EB7598 2501CE67
        BB7294F1 BC43B322 DCD25C14 67212CAB 0CD5E695 4C5B6F6A
```

```
    temp =
                          152D908B 0EDF7253 D5D19F0A F96518D3
        AD33F2EF 3151A0C9 56D9D3EE 6DC08B70 F1EB7598 2501CE67
        BB7294F1 BC43B322 DCD25C14 67212CAB 0CD5E695 4C5B6F6A


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                   02000003 78000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    Hash(counter||no_of_bits_to_return||input_string) is
                          D466C1D9 AC010D21 B28CD9FD 124DF56D
        4D3B75B9 604827B3 CF49928E C4DA204F C374888E 278C0319
        DB45E1FD 3BCAD38C C355D2D6 55C1D606 60AEA6D6 BBE4E7C1


    temp =
                            152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
        6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
        B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


  V is
                            152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
        6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
        B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


--------------------------

  Hash_df - Generate C - Step 4
```

```
0x00||V is
                      00152D90 8B0EDF72 53D5D19F 0AF96518
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
    6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
    B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
          01 00000378 00152D90 8B0EDF72 53D5D19F 0AF96518
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
    6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
    B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


Hash(counter||no_of_bits_to_return||input_string) is
                      2B22189F 32CB92C1 508BC343 69B8C37F
    D9593FD9 EC56B559 844E605D 67B4A586 2F1C7B75 3F68DF75
    10BE1F64 A7AAB557 9821195F FF0357CC 5464CAC5 D07655D6


temp =
                      2B22189F 32CB92C1 508BC343 69B8C37F
    D9593FD9 EC56B559 844E605D 67B4A586 2F1C7B75 3F68DF75
    10BE1F64 A7AAB557 9821195F FF0357CC 5464CAC5 D07655D6


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 00152D90 8B0EDF72 53D5D19F 0AF96518
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
    6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
    B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                           051F8441 D411B910 71605B9A 44B6643E
        67225358 2AE3148F 4A57E8FD A8E81155 108E4AFC C0E939BF
        D95FAB62 E8B1E4FD BDA34B60 C9220A37 EC6BD096 A6DAE159


    temp =
                             2B2218 9F32CB92 C1508BC3 4369B8C3
        7FD9593F D9EC56B5 59844E60 5D67B4A5 862F1C7B 753F68DF
        7510BE1F 64A7AAB5 57982119 5FFF0357 CC5464CA C5D07655
        D6051F84 41D411B9 1071605B 9A44B664 3E672253 582AE314
        8F4A57E8 FDA8E811 55108E4A FCC0E939 BFD95FAB 62E8B1E4


  C is
                             2B2218 9F32CB92 C1508BC3 4369B8C3
        7FD9593F D9EC56B5 59844E60 5D67B4A5 862F1C7B 753F68DF
        7510BE1F 64A7AAB5 57982119 5FFF0357 CC5464CA C5D07655
        D6051F84 41D411B9 1071605B 9A44B664 3E672253 582AE314
        8F4A57E8 FDA8E811 55108E4A FCC0E939 BFD95FAB 62E8B1E4


-----------------------------------------------------------------

First call to Generate

*****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

Generate FAILED: Reseed is required
-----------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                             808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE
```

```
  additional_input <empty>

--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                 01152D 908B0EDF
        7253D5D1 9F0AF965 18D3AD33 F2EF3151 A0C956D9 D3EE6DC0
        8B70F1EB 75982501 CE67BB72 94F1BC43 B322DCD2 5C146721
        2CAB0CD5 E6954C5B 6F6AD466 C1D9AC01 0D21B28C D9FD124D
        F56D4D3B 75B96048 27B3CF49 928EC4DA 204FC374 888E278C
        0319DB45 E1FD3BCA D3808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                 01000003 7801152D 908B0EDF
        7253D5D1 9F0AF965 18D3AD33 F2EF3151 A0C956D9 D3EE6DC0
        8B70F1EB 75982501 CE67BB72 94F1BC43 B322DCD2 5C146721
        2CAB0CD5 E6954C5B 6F6AD466 C1D9AC01 0D21B28C D9FD124D
        F56D4D3B 75B96048 27B3CF49 928EC4DA 204FC374 888E278C
        0319DB45 E1FD3BCA D3808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    Hash(counter||no_of_bits_to_return||input_string) is
                          17CE08BA 0E4651EA DF0FC284 53E6FB22
        268D86FC 36726062 9EEB49F1 3078D76D A5D5FB23 B8ED59BC
        101FE6D1 16EE9EE8 9A05CCB3 F636E348 1A82B307 79B8A687


    temp =
```

```
                        17CE08BA 0E4651EA DF0FC284 53E6FB22
        268D86FC 36726062 9EEB49F1 3078D76D A5D5FB23 B8ED59BC
        101FE6D1 16EE9EE8 9A05CCB3 F636E348 1A82B307 79B8A687


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                   02000003 7801152D 908B0EDF
        7253D5D1 9F0AF965 18D3AD33 F2EF3151 A0C956D9 D3EE6DC0
        8B70F1EB 75982501 CE67BB72 94F1BC43 B322DCD2 5C146721
        2CAB0CD5 E6954C5B 6F6AD466 C1D9AC01 0D21B28C D9FD124D
        F56D4D3B 75B96048 27B3CF49 928EC4DA 204FC374 888E278C
        0319DB45 E1FD3BCA D3808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    Hash(counter||no_of_bits_to_return||input_string) is
                        69E3C22C CD045AC3 1040FDBE 6CED62C2
        89607123 9A203F90 65DADAE6 51D56694 E76EC358 BBD4E673
        08A9A921 C6B71923 97235978 5AE5EE19 ECDB5D35 87552BC4


    temp =
                          17CE08 BA0E4651 EADF0FC2 8453E6FB
        22268D86 FC367260 629EEB49 F13078D7 6DA5D5FB 23B8ED59
        BC101FE6 D116EE9E E89A05CC B3F636E3 481A82B3 0779B8A6
        8769E3C2 2CCD045A C31040FD BE6CED62 C2896071 239A203F
        9065DADA E651D566 94E76EC3 58BBD4E6 7308A9A9 21C6B719


  V is
                          17CE08 BA0E4651 EADF0FC2 8453E6FB
        22268D86 FC367260 629EEB49 F13078D7 6DA5D5FB 23B8ED59
        BC101FE6 D116EE9E E89A05CC B3F636E3 481A82B3 0779B8A6
        8769E3C2 2CCD045A C31040FD BE6CED62 C2896071 239A203F
        9065DADA E651D566 94E76EC3 58BBD4E6 7308A9A9 21C6B719


--------------------------
```

```
Hash_df - Generate C - Step 4

  0x00||V is
                        0017CE08 BA0E4651 EADF0FC2 8453E6FB
      22268D86 FC367260 629EEB49 F13078D7 6DA5D5FB 23B8ED59
      BC101FE6 D116EE9E E89A05CC B3F636E3 481A82B3 0779B8A6
      8769E3C2 2CCD045A C31040FD BE6CED62 C2896071 239A203F
      9065DADA E651D566 94E76EC3 58BBD4E6 7308A9A9 21C6B719


  no_of_bits_to_return = 888

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
            01 00000378 0017CE08 BA0E4651 EADF0FC2 8453E6FB
      22268D86 FC367260 629EEB49 F13078D7 6DA5D5FB 23B8ED59
      BC101FE6 D116EE9E E89A05CC B3F636E3 481A82B3 0779B8A6
      8769E3C2 2CCD045A C31040FD BE6CED62 C2896071 239A203F
      9065DADA E651D566 94E76EC3 58BBD4E6 7308A9A9 21C6B719


  Hash(counter||no_of_bits_to_return||input_string) is
                        4B0CA37A 6183A4D3 B14843C0 C8D603FD
      BC738838 A93506BB C567FD4F 8B54F665 0CB04697 A5380BFE
      108BFCB0 4195F953 3A87E871 74769A7D 24E97D26 27416E7F


  temp =
                        4B0CA37A 6183A4D3 B14843C0 C8D603FD
      BC738838 A93506BB C567FD4F 8B54F665 0CB04697 A5380BFE
      108BFCB0 4195F953 3A87E871 74769A7D 24E97D26 27416E7F


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
            02 00000378 0017CE08 BA0E4651 EADF0FC2 8453E6FB
      22268D86 FC367260 629EEB49 F13078D7 6DA5D5FB 23B8ED59
      BC101FE6 D116EE9E E89A05CC B3F636E3 481A82B3 0779B8A6
      8769E3C2 2CCD045A C31040FD BE6CED62 C2896071 239A203F
      9065DADA E651D566 94E76EC3 58BBD4E6 7308A9A9 21C6B719
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                          B974D8B5 F1C1D7A2 4ADFED81 E2382AE9
        089FF637 76DAF544 0661405E 13A67D43 6BABF056 22D9BC9A
        A7B9D848 862F6858 93B94E18 D4FEDB4E C3A87782 D47CE6CA


    temp =
                            4B0CA3 7A6183A4 D3B14843 C0C8D603
        FDBC7388 38A93506 BBC567FD 4F8B54F6 650CB046 97A5380B
        FE108BFC B04195F9 533A87E8 7174769A 7D24E97D 2627416E
        7FB974D8 B5F1C1D7 A24ADFED 81E2382A E9089FF6 3776DAF5
        44066140 5E13A67D 436BABF0 5622D9BC 9AA7B9D8 48862F68


  C is
                            4B0CA3 7A6183A4 D3B14843 C0C8D603
        FDBC7388 38A93506 BBC567FD 4F8B54F6 650CB046 97A5380B
        FE108BFC B04195F9 533A87E8 7174769A 7D24E97D 2627416E
        7FB974D8 B5F1C1D7 A24ADFED 81E2382A E9089FF6 3776DAF5
        44066140 5E13A67D 436BABF0 5622D9BC 9AA7B9D8 48862F68


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                            17CE08 BA0E4651 EADF0FC2 8453E6FB
        22268D86 FC367260 629EEB49 F13078D7 6DA5D5FB 23B8ED59
        BC101FE6 D116EE9E E89A05CC B3F636E3 481A82B3 0779B8A6
```

```
        8769E3C2 2CCD045A C31040FD BE6CED62 C2896071 239A203F
        9065DADA E651D566 94E76EC3 58BBD4E6 7308A9A9 21C6B719


    w_i is
                           F93CA685 5590A77F 07354097 E90E0266
        48B6115D F008FFED BD9D9811 F54E8286 EF00FDD6 BA1E58DF
        2535E3FB DD9A9BA3 754A97F3 6EE83322 1582060A 1F37FCE4


    W is
                           F93CA685 5590A77F 07354097 E90E0266
        48B6115D F008FFED BD9D9811 F54E8286 EF00FDD6 BA1E58DF
        2535E3FB DD9A9BA3 754A97F3 6EE83322 1582060A 1F37FCE4


    ------------

    i = 2

    data is
                             17CE08 BA0E4651 EADF0FC2 8453E6FB
        22268D86 FC367260 629EEB49 F13078D7 6DA5D5FB 23B8ED59
        BC101FE6 D116EE9E E89A05CC B3F636E3 481A82B3 0779B8A6
        8769E3C2 2CCD045A C31040FD BE6CED62 C2896071 239A203F
        9065DADA E651D566 94E76EC3 58BBD4E6 7308A9A9 21C6B71A


    w_i is
                           EE882663 6B28EAD5 89593F4C A8B64738
        8F24EB3F 0A347969 68D21BDE E6F81FD5 DF93536F 935937B8
        025EC8CB F57DDB0C 61F2E414 63CC1516 D657DA28 29C6BF90


    W is
                                               F93CA685 5590A77F
        07354097 E90E0266 48B6115D F008FFED BD9D9811 F54E8286
        EF00FDD6 BA1E58DF 2535E3FB DD9A9BA3 754A97F3 6EE83322
        1582060A 1F37FCE4 EE882663 6B28EAD5 89593F4C A8B64738
        8F24EB3F 0A347969 68D21BDE E6F81FD5 DF93536F 935937B8
        025EC8CB F57DDB0C 61F2E414 63CC1516 D657DA28 29C6BF90


returned_bits is
                                               F93CA685 5590A77F
        07354097 E90E0266 48B6115D F008FFED BD9D9811 F54E8286
```

```
        EF00FDD6 BA1E58DF 2535E3FB DD9A9BA3 754A97F3 6EE83322
        1582060A 1F37FCE4 EE882663 6B28EAD5 89593F4C A8B64738
        8F24EB3F 0A347969 68D21BDE E6F81FD5 DF93536F 935937B8
        025EC8CB F57DDB0C 61F2E414 63CC1516 D657DA28 29C6BF90


--------------------------

  Update V

    0x03||V is
                         0317CE08 BA0E4651 EADF0FC2 8453E6FB
        22268D86 FC367260 629EEB49 F13078D7 6DA5D5FB 23B8ED59
        BC101FE6 D116EE9E E89A05CC B3F636E3 481A82B3 0779B8A6
        8769E3C2 2CCD045A C31040FD BE6CED62 C2896071 239A203F
        9065DADA E651D566 94E76EC3 58BBD4E6 7308A9A9 21C6B719


    H is
                         9947CEAD BF7B9EFF B4167AA7 7DEEEF78
        AB54762F BDDA12AF A034B7A3 0B837D85 5954FE7C 7C89A480
        CDFB25CE 69CD76B8 07D1095C 1C6018D7 FC0152D8 9E063488


  Updated values

  V is
                           62DAAC 346FC9F6 BE905806 451CBCFF
        1FE3010F 34DFA767 1E645347 40BBCDCD D2B28641 BB5E2565
        BA20ABE3 81588498 D51C5C62 E4E64C7D 7955E6D7 AB8FE98D
        B277CECA A098D8E2 058FD88E 4BD2A313 04E6FEE3 D79A9FB5
        A26761E9 AE32F29B E024240F CB3EC77B 09B1B65A 08531B0A


  reseed_counter is
                                                0000 00000002


rnd_val is
                                             F93CA685 5590A77F
        07354097 E90E0266 48B6115D F008FFED BD9D9811 F54E8286
        EF00FDD6 BA1E58DF 2535E3FB DD9A9BA3 754A97F3 6EE83322
        1582060A 1F37FCE4 EE882663 6B28EAD5 89593F4C A8B64738
        8F24EB3F 0A347969 68D21BDE E6F81FD5 DF93536F 935937B8
        025EC8CB F57DDB0C 61F2E414 63CC1516 D657DA28 29C6BF90
```

```
-------------------------------------------------------------

Second call to Generate

*************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

Generate FAILED: Reseed is required
-------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                              0162DA AC346FC9
        F6BE9058 06451CBC FF1FE301 0F34DFA7 671E6453 4740BBCD
        CDD2B286 41BB5E25 65BA20AB E3815884 98D51C5C 62E4E64C
        7D7955E6 D7AB8FE9 8DB277CE CAA098D8 E2058FD8 8E4BD2A3
        1304E6FE E3D79A9F B5A26761 E9AE32F2 9BE02424 0FCB3EC7
        7B09B1B6 5A08531B 0AC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    no_of_bits_to_return = 888
```

```
------------

i = 1

counter||no_of_bits_to_return||input_string is
                                01000003 780162DA AC346FC9
    F6BE9058 06451CBC FF1FE301 0F34DFA7 671E6453 4740BBCD
    CDD2B286 41BB5E25 65BA20AB E3815884 98D51C5C 62E4E64C
    7D7955E6 D7AB8FE9 8DB277CE CAA098D8 E2058FD8 8E4BD2A3
    1304E6FE E3D79A9F B5A26761 E9AE32F2 9BE02424 0FCB3EC7
    7B09B1B6 5A08531B 0AC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Hash(counter||no_of_bits_to_return||input_string) is
                        26F8B3C0 A59D2E12 74CA61F9 D896F8F9
    0AE012FE 512AA300 72DD2BAA 5BCE6F16 BF9398BC 247FE40F
    76079262 EEC76476 2CB5B8CF 738ED7C7 249EC615 CA579D68


temp =
                        26F8B3C0 A59D2E12 74CA61F9 D896F8F9
    0AE012FE 512AA300 72DD2BAA 5BCE6F16 BF9398BC 247FE40F
    76079262 EEC76476 2CB5B8CF 738ED7C7 249EC615 CA579D68


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                02000003 780162DA AC346FC9
    F6BE9058 06451CBC FF1FE301 0F34DFA7 671E6453 4740BBCD
    CDD2B286 41BB5E25 65BA20AB E3815884 98D51C5C 62E4E64C
    7D7955E6 D7AB8FE9 8DB277CE CAA098D8 E2058FD8 8E4BD2A3
    1304E6FE E3D79A9F B5A26761 E9AE32F2 9BE02424 0FCB3EC7
    7B09B1B6 5A08531B 0AC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                          107F58B6 1187B19B A9FB47F9 06F1698D
        5B0F3967 D7E7D97C 6D6F25C7 5FC403C1 C6E05077 0951F57F
        997DFDB1 F6B6506D E75F9D00 953ED240 28C8DE4D C22ADD87


    temp =
                            26F8B3 C0A59D2E 1274CA61 F9D896F8
        F90AE012 FE512AA3 0072DD2B AA5BCE6F 16BF9398 BC247FE4
        0F760792 62EEC764 762CB5B8 CF738ED7 C7249EC6 15CA579D
        68107F58 B61187B1 9BA9FB47 F906F169 8D5B0F39 67D7E7D9
        7C6D6F25 C75FC403 C1C6E050 770951F5 7F997DFD B1F6B650


  V is
                            26F8B3 C0A59D2E 1274CA61 F9D896F8
        F90AE012 FE512AA3 0072DD2B AA5BCE6F 16BF9398 BC247FE4
        0F760792 62EEC764 762CB5B8 CF738ED7 C7249EC6 15CA579D
        68107F58 B61187B1 9BA9FB47 F906F169 8D5B0F39 67D7E7D9
        7C6D6F25 C75FC403 C1C6E050 770951F5 7F997DFD B1F6B650


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          0026F8B3 C0A59D2E 1274CA61 F9D896F8
        F90AE012 FE512AA3 0072DD2B AA5BCE6F 16BF9398 BC247FE4
        0F760792 62EEC764 762CB5B8 CF738ED7 C7249EC6 15CA579D
        68107F58 B61187B1 9BA9FB47 F906F169 8D5B0F39 67D7E7D9
        7C6D6F25 C75FC403 C1C6E050 770951F5 7F997DFD B1F6B650


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 0026F8B3 C0A59D2E 1274CA61 F9D896F8
        F90AE012 FE512AA3 0072DD2B AA5BCE6F 16BF9398 BC247FE4
        0F760792 62EEC764 762CB5B8 CF738ED7 C7249EC6 15CA579D
        68107F58 B61187B1 9BA9FB47 F906F169 8D5B0F39 67D7E7D9
```

```
        7C6D6F25 C75FC403 C1C6E050 770951F5 7F997DFD B1F6B650


    Hash(counter||no_of_bits_to_return||input_string) is
                           E35403EB 642047D2 4B2913A6 A064EC86
        3D44541A 951BD377 04EEEC2A C67FB0B3 9968ED22 5646700F
        24FA3A0A 7C42F941 1840ED9E 067D5AE9 F54A7E20 4E5AEB6C


    temp =
                           E35403EB 642047D2 4B2913A6 A064EC86
        3D44541A 951BD377 04EEEC2A C67FB0B3 9968ED22 5646700F
        24FA3A0A 7C42F941 1840ED9E 067D5AE9 F54A7E20 4E5AEB6C


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
              02 00000378 0026F8B3 C0A59D2E 1274CA61 F9D896F8
        F90AE012 FE512AA3 0072DD2B AA5BCE6F 16BF9398 BC247FE4
        0F760792 62EEC764 762CB5B8 CF738ED7 C7249EC6 15CA579D
        68107F58 B61187B1 9BA9FB47 F906F169 8D5B0F39 67D7E7D9
        7C6D6F25 C75FC403 C1C6E050 770951F5 7F997DFD B1F6B650


    Hash(counter||no_of_bits_to_return||input_string) is
                           47BC945E 0C7B6F91 8B4BAA5D 3EED85CC
        20B0EE1D 46BF14C1 3D189703 69EF6C55 A8AB988D 7E3F356F
        2E328856 E356FDEE 3D2976E3 CB55E90C 61FB3FBF BA296DB4


    temp =
                             E35403 EB642047 D24B2913 A6A064EC
        863D4454 1A951BD3 7704EEEC 2AC67FB0 B39968ED 22564670
        0F24FA3A 0A7C42F9 411840ED 9E067D5A E9F54A7E 204E5AEB
        6C47BC94 5E0C7B6F 918B4BAA 5D3EED85 CC20B0EE 1D46BF14
        C13D1897 0369EF6C 55A8AB98 8D7E3F35 6F2E3288 56E356FD


C is
                             E35403 EB642047 D24B2913 A6A064EC
        863D4454 1A951BD3 7704EEEC 2AC67FB0 B39968ED 22564670
        0F24FA3A 0A7C42F9 411840ED 9E067D5A E9F54A7E 204E5AEB
        6C47BC94 5E0C7B6F 918B4BAA 5D3EED85 CC20B0EE 1D46BF14
```

```
        C13D1897 0369EF6C 55A8AB98 8D7E3F35 6F2E3288 56E356FD


************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                            26F8B3 C0A59D2E 1274CA61 F9D896F8
        F90AE012 FE512AA3 0072DD2B AA5BCE6F 16BF9398 BC247FE4
        0F760792 62EEC764 762CB5B8 CF738ED7 C7249EC6 15CA579D
        68107F58 B61187B1 9BA9FB47 F906F169 8D5B0F39 67D7E7D9
        7C6D6F25 C75FC403 C1C6E050 770951F5 7F997DFD B1F6B650


    w_i is
                          4817618F 48C60FB1 CE5BFBDA 0CAF4591
        882A31F6 EE3FE0F7 8779992A 06EC60F3 7FB9A8D6 108C231F
        0A927754 B0599FA4 FA27A4E2 5E065EF0 3085B892 979DC0E7


    W is
                          4817618F 48C60FB1 CE5BFBDA 0CAF4591
        882A31F6 EE3FE0F7 8779992A 06EC60F3 7FB9A8D6 108C231F
        0A927754 B0599FA4 FA27A4E2 5E065EF0 3085B892 979DC0E7


    ------------

    i = 2

    data is
```

```
                          26F8B3 C0A59D2E 1274CA61 F9D896F8
        F90AE012 FE512AA3 0072DD2B AA5BCE6F 16BF9398 BC247FE4
        0F760792 62EEC764 762CB5B8 CF738ED7 C7249EC6 15CA579D
        68107F58 B61187B1 9BA9FB47 F906F169 8D5B0F39 67D7E7D9
        7C6D6F25 C75FC403 C1C6E050 770951F5 7F997DFD B1F6B651


    w_i is
                         A1080883 CAEBFDFD 3665A8F2 D061C521
        F7D6E3DA 2AF8B97B 6B43B6EC 831AF515 070A83BB B9AC95ED
        4EF49B75 6A2377A5 F0833D84 7E27A88D DB0C2CE4 AD782E7B


    W is
                                             4817618F 48C60FB1
        CE5BFBDA 0CAF4591 882A31F6 EE3FE0F7 8779992A 06EC60F3
        7FB9A8D6 108C231F 0A927754 B0599FA4 FA27A4E2 5E065EF0
        3085B892 979DC0E7 A1080883 CAEBFDFD 3665A8F2 D061C521
        F7D6E3DA 2AF8B97B 6B43B6EC 831AF515 070A83BB B9AC95ED
        4EF49B75 6A2377A5 F0833D84 7E27A88D DB0C2CE4 AD782E7B


  returned_bits is
                                             4817618F 48C60FB1
        CE5BFBDA 0CAF4591 882A31F6 EE3FE0F7 8779992A 06EC60F3
        7FB9A8D6 108C231F 0A927754 B0599FA4 FA27A4E2 5E065EF0
        3085B892 979DC0E7 A1080883 CAEBFDFD 3665A8F2 D061C521
        F7D6E3DA 2AF8B97B 6B43B6EC 831AF515 070A83BB B9AC95ED
        4EF49B75 6A2377A5 F0833D84 7E27A88D DB0C2CE4 AD782E7B


---------------------------

  Update V

    0x03||V is
                         0326F8B3 C0A59D2E 1274CA61 F9D896F8
        F90AE012 FE512AA3 0072DD2B AA5BCE6F 16BF9398 BC247FE4
        0F760792 62EEC764 762CB5B8 CF738ED7 C7249EC6 15CA579D
        68107F58 B61187B1 9BA9FB47 F906F169 8D5B0F39 67D7E7D9
        7C6D6F25 C75FC403 C1C6E050 770951F5 7F997DFD B1F6B650


    H is
                         7F116A9A 5EE60219 CB56CF14 EA153D77
        D31DD052 0D1D8407 79B39FD8 3750B4F3 76BE499E 43F66A07
```

```
        63E03D8D 39F32DA9 1BB2A0CF 1D4D97A5 FDB1B238 5DED4D0B


  Updated values

  V is
                           0A4CB7 AC09BD75 E4BFF375 A078FBE5
        7F482467 18E64676 7777CC17 D5224E1F CA58FC85 DE7AC654
        1E9B01CC 6D6B0A5E 36566140 CC600E4C 7C70B859 202DF000
        A7760C3F 213B8728 A6E8E6CA 8D9693E2 D03A09C5 C91510F5
        A18AC54A 04BCE119 33222CB8 21D528D0 EC7962BE 66C75A59


  reseed_counter is
                                                0000 00000002


rnd_val is
                                             4817618F 48C60FB1
        CE5BFBDA 0CAF4591 882A31F6 EE3FE0F7 8779992A 06EC60F3
        7FB9A8D6 108C231F 0A927754 B0599FA4 FA27A4E2 5E065EF0
        3085B892 979DC0E7 A1080883 CAEBFDFD 3665A8F2 D061C521
        F7D6E3DA 2AF8B97B 6B43B6EC 831AF515 070A83BB B9AC95ED
        4EF49B75 6A2377A5 F0833D84 7E27A88D DB0C2CE4 AD782E7B


##############################################################

Hash_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                           000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                           808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
```

```
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                           20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput1 =
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    AdditionalInput2 =
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


##############################################################

**************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
```

```
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                           20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                    01000003 78000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    Hash(counter||no_of_bits_to_return||input_string) is
                           152D908B 0EDF7253 D5D19F0A F96518D3
        AD33F2EF 3151A0C9 56D9D3EE 6DC08B70 F1EB7598 2501CE67
        BB7294F1 BC43B322 DCD25C14 67212CAB 0CD5E695 4C5B6F6A


    temp =
```

```
                        152D908B 0EDF7253 D5D19F0A F96518D3
        AD33F2EF 3151A0C9 56D9D3EE 6DC08B70 F1EB7598 2501CE67
        BB7294F1 BC43B322 DCD25C14 67212CAB 0CD5E695 4C5B6F6A


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                   02000003 78000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    Hash(counter||no_of_bits_to_return||input_string) is
                           D466C1D9 AC010D21 B28CD9FD 124DF56D
        4D3B75B9 604827B3 CF49928E C4DA204F C374888E 278C0319
        DB45E1FD 3BCAD38C C355D2D6 55C1D606 60AEA6D6 BBE4E7C1


    temp =
                             152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
        6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
        B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


  V is
                             152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
        6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
        B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           00152D90 8B0EDF72 53D5D19F 0AF96518
```

```
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
    6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
    B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
          01 00000378 00152D90 8B0EDF72 53D5D19F 0AF96518
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
    6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
    B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


Hash(counter||no_of_bits_to_return||input_string) is
                     2B22189F 32CB92C1 508BC343 69B8C37F
    D9593FD9 EC56B559 844E605D 67B4A586 2F1C7B75 3F68DF75
    10BE1F64 A7AAB557 9821195F FF0357CC 5464CAC5 D07655D6


temp =
                     2B22189F 32CB92C1 508BC343 69B8C37F
    D9593FD9 EC56B559 844E605D 67B4A586 2F1C7B75 3F68DF75
    10BE1F64 A7AAB557 9821195F FF0357CC 5464CAC5 D07655D6


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 00152D90 8B0EDF72 53D5D19F 0AF96518
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
    6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
    B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


Hash(counter||no_of_bits_to_return||input_string) is
                     051F8441 D411B910 71605B9A 44B6643E
```

```
        67225358 2AE3148F 4A57E8FD A8E81155 108E4AFC C0E939BF
        D95FAB62 E8B1E4FD BDA34B60 C9220A37 EC6BD096 A6DAE159


    temp =
                           2B2218 9F32CB92 C1508BC3 4369B8C3
        7FD9593F D9EC56B5 59844E60 5D67B4A5 862F1C7B 753F68DF
        7510BE1F 64A7AAB5 57982119 5FFF0357 CC5464CA C5D07655
        D6051F84 41D411B9 1071605B 9A44B664 3E672253 582AE314
        8F4A57E8 FDA8E811 55108E4A FCC0E939 BFD95FAB 62E8B1E4


  C is
                           2B2218 9F32CB92 C1508BC3 4369B8C3
        7FD9593F D9EC56B5 59844E60 5D67B4A5 862F1C7B 753F68DF
        7510BE1F 64A7AAB5 57982119 5FFF0357 CC5464CA C5D07655
        D6051F84 41D411B9 1071605B 9A44B664 3E672253 582AE314
        8F4A57E8 FDA8E811 55108E4A FCC0E939 BFD95FAB 62E8B1E4


----------------------------------------------------------------

First call to Generate

****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input
                           606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Generate FAILED: Reseed is required
----------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                           808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
```

```
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  additional_input
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


----------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0115 2D908B0E DF7253D5 D19F0AF9 6518D3AD 33F2EF31
        51A0C956 D9D3EE6D C08B70F1 EB759825 01CE67BB 7294F1BC
        43B322DC D25C1467 212CAB0C D5E6954C 5B6F6AD4 66C1D9AC
        010D21B2 8CD9FD12 4DF56D4D 3B75B960 4827B3CF 49928EC4
        DA204FC3 74888E27 8C0319DB 45E1FD3B CAD38081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
        9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
        B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                          010000
        03780115 2D908B0E DF7253D5 D19F0AF9 6518D3AD 33F2EF31
        51A0C956 D9D3EE6D C08B70F1 EB759825 01CE67BB 7294F1BC
        43B322DC D25C1467 212CAB0C D5E6954C 5B6F6AD4 66C1D9AC
        010D21B2 8CD9FD12 4DF56D4D 3B75B960 4827B3CF 49928EC4
```

```
    DA204FC3 74888E27 8C0319DB 45E1FD3B CAD38081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Hash(counter||no_of_bits_to_return||input_string) is
                      E027DDFE D6A43806 62480926 0DA6610E
    27531429 5772E9B2 3B44BB5F EAE132FB 6E6B69EA 539D3699
    192CD0A3 9D869CCD BEA14C8C CD3E4A54 D1777BD7 E6C7301D


temp =
                      E027DDFE D6A43806 62480926 0DA6610E
    27531429 5772E9B2 3B44BB5F EAE132FB 6E6B69EA 539D3699
    192CD0A3 9D869CCD BEA14C8C CD3E4A54 D1777BD7 E6C7301D


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
    03780115 2D908B0E DF7253D5 D19F0AF9 6518D3AD 33F2EF31
    51A0C956 D9D3EE6D C08B70F1 EB759825 01CE67BB 7294F1BC
    43B322DC D25C1467 212CAB0C D5E6954C 5B6F6AD4 66C1D9AC
    010D21B2 8CD9FD12 4DF56D4D 3B75B960 4827B3CF 49928EC4
    DA204FC3 74888E27 8C0319DB 45E1FD3B CAD38081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                          E1BD13FD 14135A06 878D0E14 56BEDE0F
        9C155E5D 4BC6FC5E 53263EEB E7FC1DA9 2342A29A C9E0EEEE
        BAF1BE2F 043DB8A2 F0009B69 9051F360 D881C2DC B8198588


    temp =
                            E027DD FED6A438 06624809 260DA661
        0E275314 295772E9 B23B44BB 5FEAE132 FB6E6B69 EA539D36
        99192CD0 A39D869C CDBEA14C 8CCD3E4A 54D1777B D7E6C730
        1DE1BD13 FD14135A 06878D0E 1456BEDE 0F9C155E 5D4BC6FC
        5E53263E EBE7FC1D A92342A2 9AC9E0EE EEBAF1BE 2F043DB8


  V is
                            E027DD FED6A438 06624809 260DA661
        0E275314 295772E9 B23B44BB 5FEAE132 FB6E6B69 EA539D36
        99192CD0 A39D869C CDBEA14C 8CCD3E4A 54D1777B D7E6C730
        1DE1BD13 FD14135A 06878D0E 1456BEDE 0F9C155E 5D4BC6FC
        5E53263E EBE7FC1D A92342A2 9AC9E0EE EEBAF1BE 2F043DB8


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00E027DD FED6A438 06624809 260DA661
        0E275314 295772E9 B23B44BB 5FEAE132 FB6E6B69 EA539D36
        99192CD0 A39D869C CDBEA14C 8CCD3E4A 54D1777B D7E6C730
        1DE1BD13 FD14135A 06878D0E 1456BEDE 0F9C155E 5D4BC6FC
        5E53263E EBE7FC1D A92342A2 9AC9E0EE EEBAF1BE 2F043DB8


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00E027DD FED6A438 06624809 260DA661
        0E275314 295772E9 B23B44BB 5FEAE132 FB6E6B69 EA539D36
        99192CD0 A39D869C CDBEA14C 8CCD3E4A 54D1777B D7E6C730
        1DE1BD13 FD14135A 06878D0E 1456BEDE 0F9C155E 5D4BC6FC
        5E53263E EBE7FC1D A92342A2 9AC9E0EE EEBAF1BE 2F043DB8
```

```
  Hash(counter||no_of_bits_to_return||input_string) is
                       006B8A26 5897C2B3 7B02C787 66692916
      B0E0839A 7F778736 0D5F2A08 F9C380CD 083ADBE1 A758EA52
      FF0672B2 3F5976B1 1225D0BA 3D990E2C 198F7CAC 3EA6ECAD


  temp =
                       006B8A26 5897C2B3 7B02C787 66692916
      B0E0839A 7F778736 0D5F2A08 F9C380CD 083ADBE1 A758EA52
      FF0672B2 3F5976B1 1225D0BA 3D990E2C 198F7CAC 3EA6ECAD


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
            02 00000378 00E027DD FED6A438 06624809 260DA661
      0E275314 295772E9 B23B44BB 5FEAE132 FB6E6B69 EA539D36
      99192CD0 A39D869C CDBEA14C 8CCD3E4A 54D1777B D7E6C730
      1DE1BD13 FD14135A 06878D0E 1456BEDE 0F9C155E 5D4BC6FC
      5E53263E EBE7FC1D A92342A2 9AC9E0EE EEBAF1BE 2F043DB8


  Hash(counter||no_of_bits_to_return||input_string) is
                       35D7E097 B14DA223 67788C5E 5F6CB178
      D3F5EF2D 58751980 F8706DA8 6E078431 0AE61865 25FAA503
      8A9312BA 5040A72D 7BCE3632 6382B5EE EB173EAA ED1E7857


  temp =
                         006B8A 265897C2 B37B02C7 87666929
      16B0E083 9A7F7787 360D5F2A 08F9C380 CD083ADB E1A758EA
      52FF0672 B23F5976 B11225D0 BA3D990E 2C198F7C AC3EA6EC
      AD35D7E0 97B14DA2 2367788C 5E5F6CB1 78D3F5EF 2D587519
      80F8706D A86E0784 310AE618 6525FAA5 038A9312 BA5040A7


C is
                         006B8A 265897C2 B37B02C7 87666929
      16B0E083 9A7F7787 360D5F2A 08F9C380 CD083ADB E1A758EA
      52FF0672 B23F5976 B11225D0 BA3D990E 2C198F7C AC3EA6EC
      AD35D7E0 97B14DA2 2367788C 5E5F6CB1 78D3F5EF 2D587519
      80F8706D A86E0784 310AE618 6525FAA5 038A9312 BA5040A7
```

```
***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                           E027DD FED6A438 06624809 260DA661
        0E275314 295772E9 B23B44BB 5FEAE132 FB6E6B69 EA539D36
        99192CD0 A39D869C CDBEA14C 8CCD3E4A 54D1777B D7E6C730
        1DE1BD13 FD14135A 06878D0E 1456BEDE 0F9C155E 5D4BC6FC
        5E53263E EBE7FC1D A92342A2 9AC9E0EE EEBAF1BE 2F043DB8


    w_i is
                          0455DD4A D7DBACB2 410BE58D F7248D76
        5A4547AB AEE1743B 0BCAD37E BD06DA7C F7CE5E22 16E52532
        7E9E2005 EBEF2CE5 3BD733B1 8128627D 3FD61530 89373AF2


    W is
                          0455DD4A D7DBACB2 410BE58D F7248D76
        5A4547AB AEE1743B 0BCAD37E BD06DA7C F7CE5E22 16E52532
        7E9E2005 EBEF2CE5 3BD733B1 8128627D 3FD61530 89373AF2


    ------------

    i = 2

    data is
                           E027DD FED6A438 06624809 260DA661
```

```
        0E275314 295772E9 B23B44BB 5FEAE132 FB6E6B69 EA539D36
        99192CD0 A39D869C CDBEA14C 8CCD3E4A 54D1777B D7E6C730
        1DE1BD13 FD14135A 06878D0E 1456BEDE 0F9C155E 5D4BC6FC
        5E53263E EBE7FC1D A92342A2 9AC9E0EE EEBAF1BE 2F043DB9


    w_i is
                             606A1584 646A0EA4 88BFEF45 228699A0
        89CEA8AE C44502D8 6D9591F3 552C688B 7F7B45FC B0C3C2B9
        43C1CD8A 6FC63DF4 D81C3DA5 43C9CF28 43855EA8 4E4F959C


    W is
                                              0455DD4A D7DBACB2
        410BE58D F7248D76 5A4547AB AEE1743B 0BCAD37E BD06DA7C
        F7CE5E22 16E52532 7E9E2005 EBEF2CE5 3BD733B1 8128627D
        3FD61530 89373AF2 606A1584 646A0EA4 88BFEF45 228699A0
        89CEA8AE C44502D8 6D9591F3 552C688B 7F7B45FC B0C3C2B9
        43C1CD8A 6FC63DF4 D81C3DA5 43C9CF28 43855EA8 4E4F959C


  returned_bits is
                                              0455DD4A D7DBACB2
        410BE58D F7248D76 5A4547AB AEE1743B 0BCAD37E BD06DA7C
        F7CE5E22 16E52532 7E9E2005 EBEF2CE5 3BD733B1 8128627D
        3FD61530 89373AF2 606A1584 646A0EA4 88BFEF45 228699A0
        89CEA8AE C44502D8 6D9591F3 552C688B 7F7B45FC B0C3C2B9
        43C1CD8A 6FC63DF4 D81C3DA5 43C9CF28 43855EA8 4E4F959C


--------------------------

  Update V

    0x03||V is
                             03E027DD FED6A438 06624809 260DA661
        0E275314 295772E9 B23B44BB 5FEAE132 FB6E6B69 EA539D36
        99192CD0 A39D869C CDBEA14C 8CCD3E4A 54D1777B D7E6C730
        1DE1BD13 FD14135A 06878D0E 1456BEDE 0F9C155E 5D4BC6FC
        5E53263E EBE7FC1D A92342A2 9AC9E0EE EEBAF1BE 2F043DB8


    H is
                             FEA33CEC E4551052 A5620E9F F9CE37B0
        93C77E97 BDBBD15E 358C8A42 CE1D47DC FC587048 90D8ECD8
        86703CE6 334C5D2B 9093A57D E6E85638 5A96E601 1F73F8AA
```

```
  Updated values

  V is
                            E09368 252F3BFA B9DD4AD0 AD740F8A
        24D83397 C3D6EA70 E848A3E5 68E4A4B3 C876A645 CBFAF620
        EC183343 55DCE014 7D74040A 2B5FE7AB 264D1598 7DF3A5CD
        5EDF138C 5281325A 5F7B8FDD 40D3736C 84C87B96 1B7D28EE
        65BBD392 C7A260CD 6AC1CE38 E6D831CC 4CDC6AD2 08C8770A


  reseed_counter is
                                                0000 00000002


rnd_val is
                                               0455DD4A D7DBACB2
        410BE58D F7248D76 5A4547AB AEE1743B 0BCAD37E BD06DA7C
        F7CE5E22 16E52532 7E9E2005 EBEF2CE5 3BD733B1 8128627D
        3FD61530 89373AF2 606A1584 646A0EA4 88BFEF45 228699A0
        89CEA8AE C44502D8 6D9591F3 552C688B 7F7B45FC B0C3C2B9
        43C1CD8A 6FC63DF4 D81C3DA5 43C9CF28 43855EA8 4E4F959C


----------------------------------------------------------------

Second call to Generate

****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Generate FAILED: Reseed is required
----------------------------------------------------------------
```

Hash_DRBG_Reseed_algorithm

  entropy_input
                          C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E

  additional_input
                          A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01E0 9368252F 3BFAB9DD 4AD0AD74 0F8A24D8 3397C3D6
        EA70E848 A3E568E4 A4B3C876 A645CBFA F620EC18 334355DC
        E0147D74 040A2B5F E7AB264D 15987DF3 A5CD5EDF 138C5281
        325A5F7B 8FDD40D3 736C84C8 7B961B7D 28EE65BB D392C7A2
        60CD6AC1 CE38E6D8 31CC4CDC 6AD208C8 770AC0C1 C2C3C4C5
        C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
        DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E

    no_of_bits_to_return = 888

    ----

    i = 1

    counter||no_of_bits_to_return||input_string is

                                                        010000
    037801E0 9368252F 3BFAB9DD 4AD0AD74 0F8A24D8 3397C3D6
    EA70E848 A3E568E4 A4B3C876 A645CBFA F620EC18 334355DC
    E0147D74 040A2B5F E7AB264D 15987DF3 A5CD5EDF 138C5281
    325A5F7B 8FDD40D3 736C84C8 7B961B7D 28EE65BB D392C7A2
    60CD6AC1 CE38E6D8 31CC4CDC 6AD208C8 770AC0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E

Hash(counter||no_of_bits_to_return||input_string) is
                        FED11DEE 23C9EB92 D1D700B2 E41A74C9
    31FAC151 E1A405CC C786043D 5828D57E 40132987 BD791906
    E19D29BE A6C99FDF CF342F6B 4112165B BEC738FD 296465F9

temp =
                        FED11DEE 23C9EB92 D1D700B2 E41A74C9
    31FAC151 E1A405CC C786043D 5828D57E 40132987 BD791906
    E19D29BE A6C99FDF CF342F6B 4112165B BEC738FD 296465F9

----

i = 2

counter||no_of_bits_to_return||input_string is
                                                        020000
    037801E0 9368252F 3BFAB9DD 4AD0AD74 0F8A24D8 3397C3D6
    EA70E848 A3E568E4 A4B3C876 A645CBFA F620EC18 334355DC
    E0147D74 040A2B5F E7AB264D 15987DF3 A5CD5EDF 138C5281
    325A5F7B 8FDD40D3 736C84C8 7B961B7D 28EE65BB D392C7A2
    60CD6AC1 CE38E6D8 31CC4CDC 6AD208C8 770AC0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6

```
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    Hash(counter||no_of_bits_to_return||input_string) is
                           53607D77 80E07836 D3CF926B 4575368D
        2891F587 9804CCBE 4414F228 BD0FBBDF 89378390 1DA7536E
        C301B2EB AC27DA53 82919EFF 3675946B 4CE8EB63 6C2BC483


    temp =
                             FED11D EE23C9EB 92D1D700 B2E41A74
        C931FAC1 51E1A405 CCC78604 3D5828D5 7E401329 87BD7919
        06E19D29 BEA6C99F DFCF342F 6B411216 5BBEC738 FD296465
        F953607D 7780E078 36D3CF92 6B457536 8D2891F5 879804CC
        BE4414F2 28BD0FBB DF893783 901DA753 6EC301B2 EBAC27DA


  V is
                             FED11D EE23C9EB 92D1D700 B2E41A74
        C931FAC1 51E1A405 CCC78604 3D5828D5 7E401329 87BD7919
        06E19D29 BEA6C99F DFCF342F 6B411216 5BBEC738 FD296465
        F953607D 7780E078 36D3CF92 6B457536 8D2891F5 879804CC
        BE4414F2 28BD0FBB DF893783 901DA753 6EC301B2 EBAC27DA


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           00FED11D EE23C9EB 92D1D700 B2E41A74
        C931FAC1 51E1A405 CCC78604 3D5828D5 7E401329 87BD7919
        06E19D29 BEA6C99F DFCF342F 6B411216 5BBEC738 FD296465
        F953607D 7780E078 36D3CF92 6B457536 8D2891F5 879804CC
        BE4414F2 28BD0FBB DF893783 901DA753 6EC301B2 EBAC27DA


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
```

```
          01 00000378 00FED11D EE23C9EB 92D1D700 B2E41A74
      C931FAC1 51E1A405 CCC78604 3D5828D5 7E401329 87BD7919
      06E19D29 BEA6C99F DFCF342F 6B411216 5BBEC738 FD296465
      F953607D 7780E078 36D3CF92 6B457536 8D2891F5 879804CC
      BE4414F2 28BD0FBB DF893783 901DA753 6EC301B2 EBAC27DA


   Hash(counter||no_of_bits_to_return||input_string) is
                        5B0257EF F0741C93 45764EE4 D2D630BE
      02725A7F 0AFD9873 2BB98E9F C7CB759A 57830B67 0F22F97D
      7CC91247 AA8F7458 DC72B067 01C9CE4B BBFCCCE9 B44B43AF


   temp =
                        5B0257EF F0741C93 45764EE4 D2D630BE
      02725A7F 0AFD9873 2BB98E9F C7CB759A 57830B67 0F22F97D
      7CC91247 AA8F7458 DC72B067 01C9CE4B BBFCCCE9 B44B43AF


   ------------

   i = 2

   counter||no_of_bits_to_return||input_string is
             02 00000378 00FED11D EE23C9EB 92D1D700 B2E41A74
      C931FAC1 51E1A405 CCC78604 3D5828D5 7E401329 87BD7919
      06E19D29 BEA6C99F DFCF342F 6B411216 5BBEC738 FD296465
      F953607D 7780E078 36D3CF92 6B457536 8D2891F5 879804CC
      BE4414F2 28BD0FBB DF893783 901DA753 6EC301B2 EBAC27DA


   Hash(counter||no_of_bits_to_return||input_string) is
                        E891AF3C 8B4D3730 C877550D 41F944A6
      D18919A5 22F668CD 9AFBE283 E42A2C85 D95BA607 F3635B1F
      A473EA1D AB14476B 082C537E 965D206E D75165A3 299B56FB


   temp =
                          5B0257 EFF0741C 9345764E E4D2D630
      BE02725A 7F0AFD98 732BB98E 9FC7CB75 9A57830B 670F22F9
      7D7CC912 47AA8F74 58DC72B0 6701C9CE 4BBBFCCC E9B44B43
      AFE891AF 3C8B4D37 30C87755 0D41F944 A6D18919 A522F668
      CD9AFBE2 83E42A2C 85D95BA6 07F3635B 1FA473EA 1DAB1447


C is
```

```
                          5B0257 EFF0741C 9345764E E4D2D630
        BE02725A 7F0AFD98 732BB98E 9FC7CB75 9A57830B 670F22F9
        7D7CC912 47AA8F74 58DC72B0 6701C9CE 4BBBFCCC E9B44B43
        AFE891AF 3C8B4D37 30C87755 0D41F944 A6D18919 A522F668
        CD9AFBE2 83E42A2C 85D95BA6 07F3635B 1FA473EA 1DAB1447


************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                          FED11D EE23C9EB 92D1D700 B2E41A74
        C931FAC1 51E1A405 CCC78604 3D5828D5 7E401329 87BD7919
        06E19D29 BEA6C99F DFCF342F 6B411216 5BBEC738 FD296465
        F953607D 7780E078 36D3CF92 6B457536 8D2891F5 879804CC
        BE4414F2 28BD0FBB DF893783 901DA753 6EC301B2 EBAC27DA


    w_i is
                         C047D46D 7F614E4E 4A7952C7 9A451F8F
        7ACA3799 67E2977C 401C626A 2ED70D74 A6366057 9A354115
        BC8C8C8C C3AEA305 0686A0CF CDB6FA9C F78D4C21 65BAF851


    W is
                         C047D46D 7F614E4E 4A7952C7 9A451F8F
        7ACA3799 67E2977C 401C626A 2ED70D74 A6366057 9A354115
        BC8C8C8C C3AEA305 0686A0CF CDB6FA9C F78D4C21 65BAF851


    ------------
```

```
    i = 2

    data is
                             FED11D EE23C9EB 92D1D700 B2E41A74
        C931FAC1 51E1A405 CCC78604 3D5828D5 7E401329 87BD7919
        06E19D29 BEA6C99F DFCF342F 6B411216 5BBEC738 FD296465
        F953607D 7780E078 36D3CF92 6B457536 8D2891F5 879804CC
        BE4414F2 28BD0FBB DF893783 901DA753 6EC301B2 EBAC27DB


    w_i is
                           C6F9B1CD 16A2E14C 15C6DAAC 56C16E75
        FC84A14D 58B41622 E88B0F1B 1995587F D8BAA999 CBA98025
        4C8AB9A9 691DF7B8 4D88B639 A9A3106D EABEB637 48B99C09


    W is
                                               C047D46D 7F614E4E
        4A7952C7 9A451F8F 7ACA3799 67E2977C 401C626A 2ED70D74
        A6366057 9A354115 BC8C8C8C C3AEA305 0686A0CF CDB6FA9C
        F78D4C21 65BAF851 C6F9B1CD 16A2E14C 15C6DAAC 56C16E75
        FC84A14D 58B41622 E88B0F1B 1995587F D8BAA999 CBA98025
        4C8AB9A9 691DF7B8 4D88B639 A9A3106D EABEB637 48B99C09


  returned_bits is
                                               C047D46D 7F614E4E
        4A7952C7 9A451F8F 7ACA3799 67E2977C 401C626A 2ED70D74
        A6366057 9A354115 BC8C8C8C C3AEA305 0686A0CF CDB6FA9C
        F78D4C21 65BAF851 C6F9B1CD 16A2E14C 15C6DAAC 56C16E75
        FC84A14D 58B41622 E88B0F1B 1995587F D8BAA999 CBA98025
        4C8AB9A9 691DF7B8 4D88B639 A9A3106D EABEB637 48B99C09


---------------------------

  Update V

    0x03||V is
                           03FED11D EE23C9EB 92D1D700 B2E41A74
        C931FAC1 51E1A405 CCC78604 3D5828D5 7E401329 87BD7919
        06E19D29 BEA6C99F DFCF342F 6B411216 5BBEC738 FD296465
        F953607D 7780E078 36D3CF92 6B457536 8D2891F5 879804CC
        BE4414F2 28BD0FBB DF893783 901DA753 6EC301B2 EBAC27DA
```

```
    H is
                          11F64E29 6D412BE7 B8B5F5D6 86844A6D
        6660FC31 DA53314D A4DD6D8A E87B2BA5 D03A7172 BE903116
        CA50EFEE 37E6582E ACDB7E3B 13BC60EA 7D6E8907 E1215603


  Updated values

  V is
                            59D375 DE143E08 26174D4F 97B6F0A5
        87346D1B D0ECA19E 3FF33F92 DD1FF44B 18979634 EECC9C12
        845E663C 06515914 4AA1F509 3F8407CC 6030B9DC 6D61FA17
        0F9CEE5E 8E5F5EFD 0C79B472 61029A21 04348C81 EB4B2C4C
        563000C2 E4879217 123E1164 ABCD6B99 0BD5FEA4 EA789225


  reseed_counter is
                                                 0000 00000002


rnd_val is
                                               C047D46D 7F614E4E
        4A7952C7 9A451F8F 7ACA3799 67E2977C 401C626A 2ED70D74
        A6366057 9A354115 BC8C8C8C C3AEA305 0686A0CF CDB6FA9C
        F78D4C21 65BAF851 C6F9B1CD 16A2E14C 15C6DAAC 56C16E75
        FC84A14D 58B41622 E88B0F1B 1995587F D8BAA999 CBA98025
        4C8AB9A9 691DF7B8 4D88B639 A9A3106D EABEB637 48B99C09


################################################################

Hash_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E
```

```
    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString =
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    AdditionalInput = <empty>

################################################################

****************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
```

```
                          20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
                             404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                          010000
        03780001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
```

```
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
                     E5A5C585 D6A9E11C 58581F35 14EE19A7
    048CF096 A3E9B139 D9C0A2C0 67931041 4073C104 E2F6F8A3
    7C7C666E 11FF4439 33ABA1CF AD4C620C DFF5DA8C 0860CEEE


temp =
                     E5A5C585 D6A9E11C 58581F35 14EE19A7
    048CF096 A3E9B139 D9C0A2C0 67931041 4073C104 E2F6F8A3
    7C7C666E 11FF4439 33ABA1CF AD4C620C DFF5DA8C 0860CEEE


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
    03780001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
    46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
    5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
    2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
                     80B87195 7508538D 2D87A4A3 B5728ADB
    4191974A 384F323D 2E585869 5C152F99 D0E8CF4C B41BC2A6
    12955B4C 4838B9FB EB00568D 36F727E1 742FF774 E8542A4B


temp =
                       E5A5C5 85D6A9E1 1C58581F 3514EE19
    A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
    A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
    EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
    3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9
```

```
  V is
                           E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


----------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


    Hash(counter||no_of_bits_to_return||input_string) is
                          0C193DBC 1942C121 C63513ED 95ECA91C
        62C55031 7506462C 47B0F34F 99716F36 EAD9FF51 ACAB423C
        421CAB62 DF4D8C79 2E38D533 9D60AA24 0292E134 A249A577


    temp =
                          0C193DBC 1942C121 C63513ED 95ECA91C
        62C55031 7506462C 47B0F34F 99716F36 EAD9FF51 ACAB423C
        421CAB62 DF4D8C79 2E38D533 9D60AA24 0292E134 A249A577
```

```
    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
              02 00000378 00E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


    Hash(counter||no_of_bits_to_return||input_string) is
                          0176FE93 A4C199A2 258615DD A840AE6F
        C2E7DB39 1315119E 57774F94 396C81F5 F8D4835D 618D960B
        297E97F1 A21B35E3 E450A877 4819D918 961DFC01 FFC73630


    temp =
                            0C193D BC1942C1 21C63513 ED95ECA9
        1C62C550 31750646 2C47B0F3 4F99716F 36EAD9FF 51ACAB42
        3C421CAB 62DF4D8C 792E38D5 339D60AA 240292E1 34A249A5
        770176FE 93A4C199 A2258615 DDA840AE 6FC2E7DB 39131511
        9E57774F 94396C81 F5F8D483 5D618D96 0B297E97 F1A21B35


  C is
                            0C193D BC1942C1 21C63513 ED95ECA9
        1C62C550 31750646 2C47B0F3 4F99716F 36EAD9FF 51ACAB42
        3C421CAB 62DF4D8C 792E38D5 339D60AA 240292E1 34A249A5
        770176FE 93A4C199 A2258615 DDA840AE 6FC2E7DB 39131511
        9E57774F 94396C81 F5F8D483 5D618D96 0B297E97 F1A21B35


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024
```

```
  additional_input <empty>

Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                 01E5A5 C585D6A9
        E11C5858 1F3514EE 19A7048C F096A3E9 B139D9C0 A2C06793
        10414073 C104E2F6 F8A37C7C 666E11FF 443933AB A1CFAD4C
        620CDFF5 DA8C0860 CEEE80B8 71957508 538D2D87 A4A3B572
        8ADB4191 974A384F 323D2E58 58695C15 2F99D0E8 CF4CB41B
        C2A61295 5B4C4838 B9808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                  01000003 7801E5A5 C585D6A9
        E11C5858 1F3514EE 19A7048C F096A3E9 B139D9C0 A2C06793
        10414073 C104E2F6 F8A37C7C 666E11FF 443933AB A1CFAD4C
        620CDFF5 DA8C0860 CEEE80B8 71957508 538D2D87 A4A3B572
        8ADB4191 974A384F 323D2E58 58695C15 2F99D0E8 CF4CB41B
```

```
    C2A61295 5B4C4838 B9808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


Hash(counter||no_of_bits_to_return||input_string) is
                      90710EB6 88DF0184 891E9AE5 B0996022
    A3CA8E79 D7769CE7 5B00BAF2 E6D6EAB7 761DC6FB 1E76DB71
    77737E44 41F0AF58 6138E43C A81E70D2 3F71DD61 CCF5FA8D


temp =
                      90710EB6 88DF0184 891E9AE5 B0996022
    A3CA8E79 D7769CE7 5B00BAF2 E6D6EAB7 761DC6FB 1E76DB71
    77737E44 41F0AF58 6138E43C A81E70D2 3F71DD61 CCF5FA8D


------------

i = 2

counter||no_of_bits_to_return||input_string is
                               02000003 7801E5A5 C585D6A9
    E11C5858 1F3514EE 19A7048C F096A3E9 B139D9C0 A2C06793
    10414073 C104E2F6 F8A37C7C 666E11FF 443933AB A1CFAD4C
    620CDFF5 DA8C0860 CEEE80B8 71957508 538D2D87 A4A3B572
    8ADB4191 974A384F 323D2E58 58695C15 2F99D0E8 CF4CB41B
    C2A61295 5B4C4838 B9808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


Hash(counter||no_of_bits_to_return||input_string) is
                      46829AC7 E211C76E 9391E914 9A96C5F0
    FC5239BE BDB5CD05 F22E0B8D A207A408 C44975D7 F1894EC2
    3A47A047 B8657C9E 50FDDFE3 0B1D6523 C96ABD2F 39547413


temp =
                        90710E B688DF01 84891E9A E5B09960
    22A3CA8E 79D7769C E75B00BA F2E6D6EA B7761DC6 FB1E76DB
    7177737E 4441F0AF 586138E4 3CA81E70 D23F71DD 61CCF5FA
```

```
        8D46829A C7E211C7 6E9391E9 149A96C5 F0FC5239 BEBDB5CD
        05F22E0B 8DA207A4 08C44975 D7F1894E C23A47A0 47B8657C


  V is
                            90710E B688DF01 84891E9A E5B09960
        22A3CA8E 79D7769C E75B00BA F2E6D6EA B7761DC6 FB1E76DB
        7177737E 4441F0AF 586138E4 3CA81E70 D23F71DD 61CCF5FA
        8D46829A C7E211C7 6E9391E9 149A96C5 F0FC5239 BEBDB5CD
        05F22E0B 8DA207A4 08C44975 D7F1894E C23A47A0 47B8657C


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           0090710E B688DF01 84891E9A E5B09960
        22A3CA8E 79D7769C E75B00BA F2E6D6EA B7761DC6 FB1E76DB
        7177737E 4441F0AF 586138E4 3CA81E70 D23F71DD 61CCF5FA
        8D46829A C7E211C7 6E9391E9 149A96C5 F0FC5239 BEBDB5CD
        05F22E0B 8DA207A4 08C44975 D7F1894E C23A47A0 47B8657C


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 0090710E B688DF01 84891E9A E5B09960
        22A3CA8E 79D7769C E75B00BA F2E6D6EA B7761DC6 FB1E76DB
        7177737E 4441F0AF 586138E4 3CA81E70 D23F71DD 61CCF5FA
        8D46829A C7E211C7 6E9391E9 149A96C5 F0FC5239 BEBDB5CD
        05F22E0B 8DA207A4 08C44975 D7F1894E C23A47A0 47B8657C


    Hash(counter||no_of_bits_to_return||input_string) is
                           458CFE66 103B99E5 F76853E8 AD6B7D35
        EDEAED91 4B58D2A4 8FDC6735 959CC6BE 0CA35FFF 9E90B25D
        825B1399 7453576C 2640B98F D6EC56DA 2D0384DE 71C5C73E


    temp =
                           458CFE66 103B99E5 F76853E8 AD6B7D35
```

```
        EDEAED91 4B58D2A4 8FDC6735 959CC6BE 0CA35FFF 9E90B25D
        825B1399 7453576C 2640B98F D6EC56DA 2D0384DE 71C5C73E


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
              02 00000378 0090710E B688DF01 84891E9A E5B09960
        22A3CA8E 79D7769C E75B00BA F2E6D6EA B7761DC6 FB1E76DB
        7177737E 4441F0AF 586138E4 3CA81E70 D23F71DD 61CCF5FA
        8D46829A C7E211C7 6E9391E9 149A96C5 F0FC5239 BEBDB5CD
        05F22E0B 8DA207A4 08C44975 D7F1894E C23A47A0 47B8657C


    Hash(counter||no_of_bits_to_return||input_string) is
                           A74A55CD 25DDE339 128FE35F D5BFB9FF
        FFC9A246 25A1ECD4 517EC083 ADB5D61B 2ADF04CE 914C4486
        5E0A96FC FF9CAD70 0FF4902F 07B21CC2 402F9894 ABFD9F78


    temp =
                             458CFE 66103B99 E5F76853 E8AD6B7D
        35EDEAED 914B58D2 A48FDC67 35959CC6 BE0CA35F FF9E90B2
        5D825B13 99745357 6C2640B9 8FD6EC56 DA2D0384 DE71C5C7
        3EA74A55 CD25DDE3 39128FE3 5FD5BFB9 FFFFC9A2 4625A1EC
        D4517EC0 83ADB5D6 1B2ADF04 CE914C44 865E0A96 FCFF9CAD


  C is
                             458CFE 66103B99 E5F76853 E8AD6B7D
        35EDEAED 914B58D2 A48FDC67 35959CC6 BE0CA35F FF9E90B2
        5D825B13 99745357 6C2640B9 8FD6EC56 DA2D0384 DE71C5C7
        3EA74A55 CD25DDE3 39128FE3 5FD5BFB9 FFFFC9A2 4625A1EC
        D4517EC0 83ADB5D6 1B2ADF04 CE914C44 865E0A96 FCFF9CAD


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>
```

```
---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                            90710E B688DF01 84891E9A E5B09960
        22A3CA8E 79D7769C E75B00BA F2E6D6EA B7761DC6 FB1E76DB
        7177737E 4441F0AF 586138E4 3CA81E70 D23F71DD 61CCF5FA
        8D46829A C7E211C7 6E9391E9 149A96C5 F0FC5239 BEBDB5CD
        05F22E0B 8DA207A4 08C44975 D7F1894E C23A47A0 47B8657C


    w_i is
                          22EB93A6 7911DA73 85D9180C 78127DE1
        A04FF713 114C07C9 C615F7CC 5EF72744 A2DDCD7C 3CB85E65
        DED8EF5F 240FBDCB EBBDE2BA AC8ECF7D CBC8AC33 3E54607A


    W is
                          22EB93A6 7911DA73 85D9180C 78127DE1
        A04FF713 114C07C9 C615F7CC 5EF72744 A2DDCD7C 3CB85E65
        DED8EF5F 240FBDCB EBBDE2BA AC8ECF7D CBC8AC33 3E54607A


    ------------

    i = 2

    data is
                            90710E B688DF01 84891E9A E5B09960
        22A3CA8E 79D7769C E75B00BA F2E6D6EA B7761DC6 FB1E76DB
        7177737E 4441F0AF 586138E4 3CA81E70 D23F71DD 61CCF5FA
        8D46829A C7E211C7 6E9391E9 149A96C5 F0FC5239 BEBDB5CD
        05F22E0B 8DA207A4 08C44975 D7F1894E C23A47A0 47B8657D


    w_i is
                          D41DC495 D83DF72A 05EF55B1 27C1441C
        9A0EFFDA 2C7954DB 6C2D0434 2EB812E5 E0B11D6C 395F41ED
        A2702ECE 5BA479E2 DFA18F95 30974926 36C12FE3 0CE5C968
```

```
  W is
                                              22EB93A6 7911DA73
       85D9180C 78127DE1 A04FF713 114C07C9 C615F7CC 5EF72744
       A2DDCD7C 3CB85E65 DED8EF5F 240FBDCB EBBDE2BA AC8ECF7D
       CBC8AC33 3E54607A D41DC495 D83DF72A 05EF55B1 27C1441C
       9A0EFFDA 2C7954DB 6C2D0434 2EB812E5 E0B11D6C 395F41ED
       A2702ECE 5BA479E2 DFA18F95 30974926 36C12FE3 0CE5C968


  returned_bits is
                                              22EB93A6 7911DA73
       85D9180C 78127DE1 A04FF713 114C07C9 C615F7CC 5EF72744
       A2DDCD7C 3CB85E65 DED8EF5F 240FBDCB EBBDE2BA AC8ECF7D
       CBC8AC33 3E54607A D41DC495 D83DF72A 05EF55B1 27C1441C
       9A0EFFDA 2C7954DB 6C2D0434 2EB812E5 E0B11D6C 395F41ED
       A2702ECE 5BA479E2 DFA18F95 30974926 36C12FE3 0CE5C968


---------------------------

  Update V

    0x03||V is
                          0390710E B688DF01 84891E9A E5B09960
       22A3CA8E 79D7769C E75B00BA F2E6D6EA B7761DC6 FB1E76DB
       7177737E 4441F0AF 586138E4 3CA81E70 D23F71DD 61CCF5FA
       8D46829A C7E211C7 6E9391E9 149A96C5 F0FC5239 BEBDB5CD
       05F22E0B 8DA207A4 08C44975 D7F1894E C23A47A0 47B8657C


    H is
                          DE0335C1 4096439E 3FA51263 D05A0A38
       290A1B62 938F241B 39364DA5 21AD1132 EF54EE5B 2D9B8206
       AF5F7051 283BB5CB 28EE232C 4F216171 E2DEA414 78400EFE


  Updated values

  V is
                            D5FE0D 1C991A9B 6A8086EE CE5E04DD
       5891B57C 0B22CF6F 8BEADD22 287C73B1 7582C126 FABD078D
       CEF9CE91 DDB64407 A28AAF5F 0D154E65 EC1187C6 1098C5F9
       F4F7E853 289713C5 E0DC6F71 961D67B2 E0510A37 327ED9C0
       89A31D1D 398B7345 4CDD4BA6 F5A43705 2B76F64B BCF81128
```

```
  reseed_counter is
                                                  0000 00000002


rnd_val is
                                                22EB93A6 7911DA73
        85D9180C 78127DE1 A04FF713 114C07C9 C615F7CC 5EF72744
        A2DDCD7C 3CB85E65 DED8EF5F 240FBDCB EBBDE2BA AC8ECF7D
        CBC8AC33 3E54607A D41DC495 D83DF72A 05EF55B1 27C1441C
        9A0EFFDA 2C7954DB 6C2D0434 2EB812E5 E0B11D6C 395F41ED
        A2702ECE 5BA479E2 DFA18F95 30974926 36C12FE3 0CE5C968


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                           C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2
```

```
seed_material is
                                                01D5FE 0D1C991A
    9B6A8086 EECE5E04 DD5891B5 7C0B22CF 6F8BEADD 22287C73
    B17582C1 26FABD07 8DCEF9CE 91DDB644 07A28AAF 5F0D154E
    65EC1187 C61098C5 F9F4F7E8 53289713 C5E0DC6F 71961D67
    B2E0510A 37327ED9 C089A31D 1D398B73 454CDD4B A6F5A437
    052B76F6 4BBCF811 28C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                 01000003 7801D5FE 0D1C991A
    9B6A8086 EECE5E04 DD5891B5 7C0B22CF 6F8BEADD 22287C73
    B17582C1 26FABD07 8DCEF9CE 91DDB644 07A28AAF 5F0D154E
    65EC1187 C61098C5 F9F4F7E8 53289713 C5E0DC6F 71961D67
    B2E0510A 37327ED9 C089A31D 1D398B73 454CDD4B A6F5A437
    052B76F6 4BBCF811 28C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Hash(counter||no_of_bits_to_return||input_string) is
                       53AA08A1 A34FCCBD 82A0817A F3C88C35
    49BCDFCB DFBC1D74 08B137E5 0B3ABA20 0D1524B5 BCA3138F
    77C45377 B501948B 2A4C5AD5 1BE5F99E 9AE264A3 2AEFE040


temp =
                       53AA08A1 A34FCCBD 82A0817A F3C88C35
    49BCDFCB DFBC1D74 08B137E5 0B3ABA20 0D1524B5 BCA3138F
    77C45377 B501948B 2A4C5AD5 1BE5F99E 9AE264A3 2AEFE040


------------
```

```
    i = 2

    counter||no_of_bits_to_return||input_string is
                                  02000003 7801D5FE 0D1C991A
        9B6A8086 EECE5E04 DD5891B5 7C0B22CF 6F8BEADD 22287C73
        B17582C1 26FABD07 8DCEF9CE 91DDB644 07A28AAF 5F0D154E
        65EC1187 C61098C5 F9F4F7E8 53289713 C5E0DC6F 71961D67
        B2E0510A 37327ED9 C089A31D 1D398B73 454CDD4B A6F5A437
        052B76F6 4BBCF811 28C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Hash(counter||no_of_bits_to_return||input_string) is
                           39A298BE 17D00D28 8868EA39 7B9CF3F3
        FC352224 74AB0B61 15E44543 4AAB903B 4611A783 0734A7AF
        5A36DDE2 3C45BDEC 2B2ACB7D 047D5246 3537076A 0A6FF410


    temp =
                             53AA08 A1A34FCC BD82A081 7AF3C88C
        3549BCDF CBDFBC1D 7408B137 E50B3ABA 200D1524 B5BCA313
        8F77C453 77B50194 8B2A4C5A D51BE5F9 9E9AE264 A32AEFE0
        4039A298 BE17D00D 288868EA 397B9CF3 F3FC3522 2474AB0B
        6115E445 434AAB90 3B4611A7 830734A7 AF5A36DD E23C45BD


  V is
                             53AA08 A1A34FCC BD82A081 7AF3C88C
        3549BCDF CBDFBC1D 7408B137 E50B3ABA 200D1524 B5BCA313
        8F77C453 77B50194 8B2A4C5A D51BE5F9 9E9AE264 A32AEFE0
        4039A298 BE17D00D 288868EA 397B9CF3 F3FC3522 2474AB0B
        6115E445 434AAB90 3B4611A7 830734A7 AF5A36DD E23C45BD


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           0053AA08 A1A34FCC BD82A081 7AF3C88C
        3549BCDF CBDFBC1D 7408B137 E50B3ABA 200D1524 B5BCA313
        8F77C453 77B50194 8B2A4C5A D51BE5F9 9E9AE264 A32AEFE0
        4039A298 BE17D00D 288868EA 397B9CF3 F3FC3522 2474AB0B
```

```
    6115E445 434AAB90 3B4611A7 830734A7 AF5A36DD E23C45BD


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
          01 00000378 0053AA08 A1A34FCC BD82A081 7AF3C88C
    3549BCDF CBDFBC1D 7408B137 E50B3ABA 200D1524 B5BCA313
    8F77C453 77B50194 8B2A4C5A D51BE5F9 9E9AE264 A32AEFE0
    4039A298 BE17D00D 288868EA 397B9CF3 F3FC3522 2474AB0B
    6115E445 434AAB90 3B4611A7 830734A7 AF5A36DD E23C45BD


Hash(counter||no_of_bits_to_return||input_string) is
                     C0D57BB6 D50B2114 4F2FFFEC 22B980F1
    0317AD7C A1814A87 CE8000B1 6C56D396 9F54F093 201CC480
    85360AA0 DAB042C8 8ED611B9 615748A4 9A73869C 3C0052CC


temp =
                     C0D57BB6 D50B2114 4F2FFFEC 22B980F1
    0317AD7C A1814A87 CE8000B1 6C56D396 9F54F093 201CC480
    85360AA0 DAB042C8 8ED611B9 615748A4 9A73869C 3C0052CC


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 0053AA08 A1A34FCC BD82A081 7AF3C88C
    3549BCDF CBDFBC1D 7408B137 E50B3ABA 200D1524 B5BCA313
    8F77C453 77B50194 8B2A4C5A D51BE5F9 9E9AE264 A32AEFE0
    4039A298 BE17D00D 288868EA 397B9CF3 F3FC3522 2474AB0B
    6115E445 434AAB90 3B4611A7 830734A7 AF5A36DD E23C45BD


Hash(counter||no_of_bits_to_return||input_string) is
                     B6390CA9 72DE5FD8 51C4D013 8172E71B
    47EE2D77 A622962B 7A47E3E6 8FE8C5C7 4D809631 DA6D8F45
    E235F725 903499A3 676CD633 AC73AFFC C895889E 4CD7E12E
```

```
    temp =
                            C0D57B B6D50B21 144F2FFF EC22B980
        F10317AD 7CA1814A 87CE8000 B16C56D3 969F54F0 93201CC4
        8085360A A0DAB042 C88ED611 B9615748 A49A7386 9C3C0052
        CCB6390C A972DE5F D851C4D0 138172E7 1B47EE2D 77A62296
        2B7A47E3 E68FE8C5 C74D8096 31DA6D8F 45E235F7 25903499


  C is
                            C0D57B B6D50B21 144F2FFF EC22B980
        F10317AD 7CA1814A 87CE8000 B16C56D3 969F54F0 93201CC4
        8085360A A0DAB042 C88ED611 B9615748 A49A7386 9C3C0052
        CCB6390C A972DE5F D851C4D0 138172E7 1B47EE2D 77A62296
        2B7A47E3 E68FE8C5 C74D8096 31DA6D8F 45E235F7 25903499


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                            53AA08 A1A34FCC BD82A081 7AF3C88C
        3549BCDF CBDFBC1D 7408B137 E50B3ABA 200D1524 B5BCA313
        8F77C453 77B50194 8B2A4C5A D51BE5F9 9E9AE264 A32AEFE0
        4039A298 BE17D00D 288868EA 397B9CF3 F3FC3522 2474AB0B
        6115E445 434AAB90 3B4611A7 830734A7 AF5A36DD E23C45BD


    w_i is
                           E66698CF BF1B3F2E 919C0303 6E584EAA
        81CF1C66 66240AF0 5F706370 43733954 D8A1E5A6 6A04C53C
```

```
        6900FDC1 45D4A3A8 0A31F586 8ACE9AC9 4E14E205 1F624A05


    W is
                            E66698CF BF1B3F2E 919C0303 6E584EAA
        81CF1C66 66240AF0 5F706370 43733954 D8A1E5A6 6A04C53C
        6900FDC1 45D4A3A8 0A31F586 8ACE9AC9 4E14E205 1F624A05


    ------------

    i = 2

    data is
                              53AA08 A1A34FCC BD82A081 7AF3C88C
        3549BCDF CBDFBC1D 7408B137 E50B3ABA 200D1524 B5BCA313
        8F77C453 77B50194 8B2A4C5A D51BE5F9 9E9AE264 A32AEFE0
        4039A298 BE17D00D 288868EA 397B9CF3 F3FC3522 2474AB0B
        6115E445 434AAB90 3B4611A7 830734A7 AF5A36DD E23C45BE


    w_i is
                            EEA1F8B6 84AA5410 BCE315E7 6EA07C71
        5D6F3473 1320FF0D CF78D795 E6EFA2DF 92B98BE6 36CDFBA2
        9008DD39 2112AEC2 02F2E481 CB9D83F9 87FEA69C D1B368BB


    W is
                                                E66698CF BF1B3F2E
        919C0303 6E584EAA 81CF1C66 66240AF0 5F706370 43733954
        D8A1E5A6 6A04C53C 6900FDC1 45D4A3A8 0A31F586 8ACE9AC9
        4E14E205 1F624A05 EEA1F8B6 84AA5410 BCE315E7 6EA07C71
        5D6F3473 1320FF0D CF78D795 E6EFA2DF 92B98BE6 36CDFBA2
        9008DD39 2112AEC2 02F2E481 CB9D83F9 87FEA69C D1B368BB


  returned_bits is
                                                E66698CF BF1B3F2E
        919C0303 6E584EAA 81CF1C66 66240AF0 5F706370 43733954
        D8A1E5A6 6A04C53C 6900FDC1 45D4A3A8 0A31F586 8ACE9AC9
        4E14E205 1F624A05 EEA1F8B6 84AA5410 BCE315E7 6EA07C71
        5D6F3473 1320FF0D CF78D795 E6EFA2DF 92B98BE6 36CDFBA2
        9008DD39 2112AEC2 02F2E481 CB9D83F9 87FEA69C D1B368BB


--------------------------
```

```
  Update V

    0x03||V is
                          0353AA08 A1A34FCC BD82A081 7AF3C88C
        3549BCDF CBDFBC1D 7408B137 E50B3ABA 200D1524 B5BCA313
        8F77C453 77B50194 8B2A4C5A D51BE5F9 9E9AE264 A32AEFE0
        4039A298 BE17D00D 288868EA 397B9CF3 F3FC3522 2474AB0B
        6115E445 434AAB90 3B4611A7 830734A7 AF5A36DD E23C45BD


    H is
                          9570EF86 9B34C000 8DFC9B32 5EB45FB7
        F4B68DF6 244CA3C5 49A08912 7263A47D A717A227 4105C9E8
        87C48A0D C5FD6557 269EAA07 20C14DB4 69FEE6AF 34355EC0


  Updated values

  V is
                            147F84 58785AED D1D1D081 6716820D
        264CD48D 48813D67 FBD73138 9677918D B6AC6A15 48DCBFD8
        0FFCFA5E 188FB1D7 E92A11F3 29B1FD42 D131F11D 9E1B4FEB
        01A6699B 8BD75232 4A7AB6CC BF60B458 B65BC576 DD20978A
        1454B636 EFD7F9AD 29323C44 D5A2EFEB 5F3B5384 3C01D917


  reseed_counter is
                                                0000 00000002


rnd_val is
                                              E66698CF BF1B3F2E
        919C0303 6E584EAA 81CF1C66 66240AF0 5F706370 43733954
        D8A1E5A6 6A04C53C 6900FDC1 45D4A3A8 0A31F586 8ACE9AC9
        4E14E205 1F624A05 EEA1F8B6 84AA5410 BCE315E7 6EA07C71
        5D6F3473 1320FF0D CF78D795 E6EFA2DF 92B98BE6 36CDFBA2
        9008DD39 2112AEC2 02F2E481 CB9D83F9 87FEA69C D1B368BB


################################################################

Hash_DRBG

    Requested Security Strength = 256
```

```
Requested Hash Algorithm = SHA-512

prediction_resistance_flag = "ENABLED"
EntropyInput =
                          000102 03040506 0708090A 0B0C0D0E
    0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
    2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
    3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
    5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


EntropyInput1 (for Reseed1) =
                          808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


EntropyInput2 (for Reseed2) =
                          C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Nonce =
                        20212223 24252627 28292A2B 2C2D2E2F


PersonalizationString =
                          404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


AdditionalInput1 =
                          606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

```
    AdditionalInput2 =
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


##############################################################

**************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                          20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
```

```
    5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
    2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                                      010000
    03780001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
    46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
    5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
    2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
                      E5A5C585 D6A9E11C 58581F35 14EE19A7
    048CF096 A3E9B139 D9C0A2C0 67931041 4073C104 E2F6F8A3
    7C7C666E 11FF4439 33ABA1CF AD4C620C DFF5DA8C 0860CEEE


temp =
                      E5A5C585 D6A9E11C 58581F35 14EE19A7
    048CF096 A3E9B139 D9C0A2C0 67931041 4073C104 E2F6F8A3
    7C7C666E 11FF4439 33ABA1CF AD4C620C DFF5DA8C 0860CEEE


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
```

```
        03780001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    Hash(counter||no_of_bits_to_return||input_string) is
                            80B87195 7508538D 2D87A4A3 B5728ADB
        4191974A 384F323D 2E585869 5C152F99 D0E8CF4C B41BC2A6
        12955B4C 4838B9FB EB00568D 36F727E1 742FF774 E8542A4B


    temp =
                              E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


  V is
                              E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                            00E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9
```

```
no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
          01 00000378 00E5A5C5 85D6A9E1 1C58581F 3514EE19
    A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
    A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
    EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
    3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


Hash(counter||no_of_bits_to_return||input_string) is
                      0C193DBC 1942C121 C63513ED 95ECA91C
    62C55031 7506462C 47B0F34F 99716F36 EAD9FF51 ACAB423C
    421CAB62 DF4D8C79 2E38D533 9D60AA24 0292E134 A249A577


temp =
                      0C193DBC 1942C121 C63513ED 95ECA91C
    62C55031 7506462C 47B0F34F 99716F36 EAD9FF51 ACAB423C
    421CAB62 DF4D8C79 2E38D533 9D60AA24 0292E134 A249A577


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 00E5A5C5 85D6A9E1 1C58581F 3514EE19
    A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
    A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
    EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
    3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


Hash(counter||no_of_bits_to_return||input_string) is
                      0176FE93 A4C199A2 258615DD A840AE6F
    C2E7DB39 1315119E 57774F94 396C81F5 F8D4835D 618D960B
    297E97F1 A21B35E3 E450A877 4819D918 961DFC01 FFC73630


temp =
                        0C193D BC1942C1 21C63513 ED95ECA9
```

```
        1C62C550 31750646 2C47B0F3 4F99716F 36EAD9FF 51ACAB42
        3C421CAB 62DF4D8C 792E38D5 339D60AA 240292E1 34A249A5
        770176FE 93A4C199 A2258615 DDA840AE 6FC2E7DB 39131511
        9E57774F 94396C81 F5F8D483 5D618D96 0B297E97 F1A21B35


  C is
                            0C193D BC1942C1 21C63513 ED95ECA9
        1C62C550 31750646 2C47B0F3 4F99716F 36EAD9FF 51ACAB42
        3C421CAB 62DF4D8C 792E38D5 339D60AA 240292E1 34A249A5
        770176FE 93A4C199 A2258615 DDA840AE 6FC2E7DB 39131511
        9E57774F 94396C81 F5F8D483 5D618D96 0B297E97 F1A21B35


----------------------------------------------------------------

First call to Generate

****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Generate FAILED: Reseed is required
----------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  additional_input
```

```
                          606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


----------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01E5 A5C585D6 A9E11C58 581F3514 EE19A704 8CF096A3
        E9B139D9 C0A2C067 93104140 73C104E2 F6F8A37C 7C666E11
        FF443933 ABA1CFAD 4C620CDF F5DA8C08 60CEEE80 B8719575
        08538D2D 87A4A3B5 728ADB41 91974A38 4F323D2E 5858695C
        152F99D0 E8CF4CB4 1BC2A612 955B4C48 38B98081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
        9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
        B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                        010000
        037801E5 A5C585D6 A9E11C58 581F3514 EE19A704 8CF096A3
        E9B139D9 C0A2C067 93104140 73C104E2 F6F8A37C 7C666E11
        FF443933 ABA1CFAD 4C620CDF F5DA8C08 60CEEE80 B8719575
        08538D2D 87A4A3B5 728ADB41 91974A38 4F323D2E 5858695C
        152F99D0 E8CF4CB4 1BC2A612 955B4C48 38B98081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
        9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
        B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
```

```
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Hash(counter||no_of_bits_to_return||input_string) is
                      04F0F3B8 9552F8C0 006FE2BA 33D069A4
    08885EB0 AE9A9618 F8381C83 2B8A6FD8 1FFFFF52 5C4BD7E2
    E3EDE6ED 7AC02DED 66DFBFA0 50134D3B 1A828DA2 D4818482


temp =
                      04F0F3B8 9552F8C0 006FE2BA 33D069A4
    08885EB0 AE9A9618 F8381C83 2B8A6FD8 1FFFFF52 5C4BD7E2
    E3EDE6ED 7AC02DED 66DFBFA0 50134D3B 1A828DA2 D4818482


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
    037801E5 A5C585D6 A9E11C58 581F3514 EE19A704 8CF096A3
    E9B139D9 C0A2C067 93104140 73C104E2 F6F8A37C 7C666E11
    FF443933 ABA1CFAD 4C620CDF F5DA8C08 60CEEE80 B8719575
    08538D2D 87A4A3B5 728ADB41 91974A38 4F323D2E 5858695C
    152F99D0 E8CF4CB4 1BC2A612 955B4C48 38B98081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Hash(counter||no_of_bits_to_return||input_string) is
                      6BDA0EED A45C794A 18B04CED 7E8AFAAE
    88B743FE 0833735F C59704C4 3252DAC6 76A4C91B 8D3E78DC
    41782C01 96D73DFD 11C631F3 7B382D42 D0F77A4A A040E727
```

```
    temp =
                            04F0F3 B89552F8 C0006FE2 BA33D069
        A408885E B0AE9A96 18F8381C 832B8A6F D81FFFFF 525C4BD7
        E2E3EDE6 ED7AC02D ED66DFBF A050134D 3B1A828D A2D48184
        826BDA0E EDA45C79 4A18B04C ED7E8AFA AE88B743 FE083373
        5FC59704 C43252DA C676A4C9 1B8D3E78 DC41782C 0196D73D


  V is
                            04F0F3 B89552F8 C0006FE2 BA33D069
        A408885E B0AE9A96 18F8381C 832B8A6F D81FFFFF 525C4BD7
        E2E3EDE6 ED7AC02D ED66DFBF A050134D 3B1A828D A2D48184
        826BDA0E EDA45C79 4A18B04C ED7E8AFA AE88B743 FE083373
        5FC59704 C43252DA C676A4C9 1B8D3E78 DC41782C 0196D73D


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           0004F0F3 B89552F8 C0006FE2 BA33D069
        A408885E B0AE9A96 18F8381C 832B8A6F D81FFFFF 525C4BD7
        E2E3EDE6 ED7AC02D ED66DFBF A050134D 3B1A828D A2D48184
        826BDA0E EDA45C79 4A18B04C ED7E8AFA AE88B743 FE083373
        5FC59704 C43252DA C676A4C9 1B8D3E78 DC41782C 0196D73D


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 0004F0F3 B89552F8 C0006FE2 BA33D069
        A408885E B0AE9A96 18F8381C 832B8A6F D81FFFFF 525C4BD7
        E2E3EDE6 ED7AC02D ED66DFBF A050134D 3B1A828D A2D48184
        826BDA0E EDA45C79 4A18B04C ED7E8AFA AE88B743 FE083373
        5FC59704 C43252DA C676A4C9 1B8D3E78 DC41782C 0196D73D


    Hash(counter||no_of_bits_to_return||input_string) is
                           76878CDA 0362CAD7 DB3F3D92 17093D29
        602FF901 5D2D87A1 8EE4B2F2 88947D33 4565E066 F7E104AC
        DDBC773B 1486541E D12488D3 B70FCD34 AE68F5AD 78464189
```

```
    temp =
                          76878CDA 0362CAD7 DB3F3D92 17093D29
        602FF901 5D2D87A1 8EE4B2F2 88947D33 4565E066 F7E104AC
        DDBC773B 1486541E D12488D3 B70FCD34 AE68F5AD 78464189


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
              02 00000378 0004F0F3 B89552F8 C0006FE2 BA33D069
        A408885E B0AE9A96 18F8381C 832B8A6F D81FFFFF 525C4BD7
        E2E3EDE6 ED7AC02D ED66DFBF A050134D 3B1A828D A2D48184
        826BDA0E EDA45C79 4A18B04C ED7E8AFA AE88B743 FE083373
        5FC59704 C43252DA C676A4C9 1B8D3E78 DC41782C 0196D73D


    Hash(counter||no_of_bits_to_return||input_string) is
                          A8053FAF A58CA32F EA5C4F5C 7F3AEF74
        D699AD57 13E64377 430E4528 E54B6EE6 CE4DB441 907CA52A
        3F90A768 7AA90E89 4E60E54B C1E4E3E5 101AD0F5 CC8DD1E0


    temp =
                            76878C DA0362CA D7DB3F3D 9217093D
        29602FF9 015D2D87 A18EE4B2 F288947D 334565E0 66F7E104
        ACDDBC77 3B148654 1ED12488 D3B70FCD 34AE68F5 AD784641
        89A8053F AFA58CA3 2FEA5C4F 5C7F3AEF 74D699AD 5713E643
        77430E45 28E54B6E E6CE4DB4 41907CA5 2A3F90A7 687AA90E


  C is
                            76878C DA0362CA D7DB3F3D 9217093D
        29602FF9 015D2D87 A18EE4B2 F288947D 334565E0 66F7E104
        ACDDBC77 3B148654 1ED12488 D3B70FCD 34AE68F5 AD784641
        89A8053F AFA58CA3 2FEA5C4F 5C7F3AEF 74D699AD 5713E643
        77430E45 28E54B6E E6CE4DB4 41907CA5 2A3F90A7 687AA90E


**************************************************************

Hash_DRBG_Generate_algorithm
```

```
  requested_number_of_bits = 1024

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                           04F0F3 B89552F8 C0006FE2 BA33D069
        A408885E B0AE9A96 18F8381C 832B8A6F D81FFFFF 525C4BD7
        E2E3EDE6 ED7AC02D ED66DFBF A050134D 3B1A828D A2D48184
        826BDA0E EDA45C79 4A18B04C ED7E8AFA AE88B743 FE083373
        5FC59704 C43252DA C676A4C9 1B8D3E78 DC41782C 0196D73D


    w_i is
                          7596A763 72308BD5 A5613439 934678B3
        5521A94D 81ABFE63 A21ACF61 ABB88B61 E86A12C3 7F308F2B
        BBE32BE4 B38D03AE 80838649 4D70EF52 E9E1365D D18B7784


    W is
                          7596A763 72308BD5 A5613439 934678B3
        5521A94D 81ABFE63 A21ACF61 ABB88B61 E86A12C3 7F308F2B
        BBE32BE4 B38D03AE 80838649 4D70EF52 E9E1365D D18B7784


    ------------

    i = 2

    data is
                           04F0F3 B89552F8 C0006FE2 BA33D069
        A408885E B0AE9A96 18F8381C 832B8A6F D81FFFFF 525C4BD7
        E2E3EDE6 ED7AC02D ED66DFBF A050134D 3B1A828D A2D48184
        826BDA0E EDA45C79 4A18B04C ED7E8AFA AE88B743 FE083373
        5FC59704 C43252DA C676A4C9 1B8D3E78 DC41782C 0196D73E
```

```
    w_i is
                          CAB826F3 1D47579E 4D57F69D 8BF3152B
        95741946 CEBE5857 1DF58ED3 9980D9AF 44E69F01 E8989759
        8E401711 01A0E330 2838E0AD 9E849C01 988993CF 9F6E5263


    W is
                                               7596A763 72308BD5
        A5613439 934678B3 5521A94D 81ABFE63 A21ACF61 ABB88B61
        E86A12C3 7F308F2B BBE32BE4 B38D03AE 80838649 4D70EF52
        E9E1365D D18B7784 CAB826F3 1D47579E 4D57F69D 8BF3152B
        95741946 CEBE5857 1DF58ED3 9980D9AF 44E69F01 E8989759
        8E401711 01A0E330 2838E0AD 9E849C01 988993CF 9F6E5263


  returned_bits is
                                               7596A763 72308BD5
        A5613439 934678B3 5521A94D 81ABFE63 A21ACF61 ABB88B61
        E86A12C3 7F308F2B BBE32BE4 B38D03AE 80838649 4D70EF52
        E9E1365D D18B7784 CAB826F3 1D47579E 4D57F69D 8BF3152B
        95741946 CEBE5857 1DF58ED3 9980D9AF 44E69F01 E8989759
        8E401711 01A0E330 2838E0AD 9E849C01 988993CF 9F6E5263


--------------------------

  Update V

    0x03||V is
                          0304F0F3 B89552F8 C0006FE2 BA33D069
        A408885E B0AE9A96 18F8381C 832B8A6F D81FFFFF 525C4BD7
        E2E3EDE6 ED7AC02D ED66DFBF A050134D 3B1A828D A2D48184
        826BDA0E EDA45C79 4A18B04C ED7E8AFA AE88B743 FE083373
        5FC59704 C43252DA C676A4C9 1B8D3E78 DC41782C 0196D73D


    H is
                          570B7582 C7A57D2D 0D1631DD 208A507A
        9B9BE4AE 3676F474 C31F49B0 AE96CD64 33D19AEB 51584CEA
        F532A3C7 9E0C7208 17510AAB 6AF67458 9AB9180B 51620620


  Updated values

  V is
                             7B7880 9298B5C3 97DBAF20 4C4AD9A6
```

```
        CD68B857 B20BC81D BA871CCF 75B41EED 0B6565DF B9542CDC
        8FC1AA5E 288F4682 634379CB 3BACA047 7CDF1D60 70D71840
        A7AFC3FC D3C0DD91 3D22564C F894934E 5730EBDC A67466A1
        CC3B4911 8B241051 C495FD28 C8142F76 A13A20DE BB73866C


  reseed_counter is
                                                0000 00000002


rnd_val is
                                             7596A763 72308BD5
        A5613439 934678B3 5521A94D 81ABFE63 A21ACF61 ABB88B61
        E86A12C3 7F308F2B BBE32BE4 B38D03AE 80838649 4D70EF52
        E9E1365D D18B7784 CAB826F3 1D47579E 4D57F69D 8BF3152B
        95741946 CEBE5857 1DF58ED3 9980D9AF 44E69F01 E8989759
        8E401711 01A0E330 2838E0AD 9E849C01 988993CF 9F6E5263


----------------------------------------------------------------

Second call to Generate

****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Generate FAILED: Reseed is required
----------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                           C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
```

```
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  additional_input
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            017B 78809298 B5C397DB AF204C4A D9A6CD68 B857B20B
        C81DBA87 1CCF75B4 1EED0B65 65DFB954 2CDC8FC1 AA5E288F
        46826343 79CB3BAC A0477CDF 1D6070D7 1840A7AF C3FCD3C0
        DD913D22 564CF894 934E5730 EBDCA674 66A1CC3B 49118B24
        1051C495 FD28C814 2F76A13A 20DEBB73 866CC0C1 C2C3C4C5
        C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
        DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                          010000
        0378017B 78809298 B5C397DB AF204C4A D9A6CD68 B857B20B
        C81DBA87 1CCF75B4 1EED0B65 65DFB954 2CDC8FC1 AA5E288F
        46826343 79CB3BAC A0477CDF 1D6070D7 1840A7AF C3FCD3C0
        DD913D22 564CF894 934E5730 EBDCA674 66A1CC3B 49118B24
        1051C495 FD28C814 2F76A13A 20DEBB73 866CC0C1 C2C3C4C5
```

```
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Hash(counter||no_of_bits_to_return||input_string) is
                    913CA013 D788EAD1 4EDFA1A5 7857414B
    1D68E30D 85930C99 4EC8DEEE 1B2F7E74 4CAC3288 A442A4CD
    55A41FD1 A0B265B4 90812D90 00FFCC62 82474D78 8DFB3781


temp =
                    913CA013 D788EAD1 4EDFA1A5 7857414B
    1D68E30D 85930C99 4EC8DEEE 1B2F7E74 4CAC3288 A442A4CD
    55A41FD1 A0B265B4 90812D90 00FFCC62 82474D78 8DFB3781


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
    0378017B 78809298 B5C397DB AF204C4A D9A6CD68 B857B20B
    C81DBA87 1CCF75B4 1EED0B65 65DFB954 2CDC8FC1 AA5E288F
    46826343 79CB3BAC A0477CDF 1D6070D7 1840A7AF C3FCD3C0
    DD913D22 564CF894 934E5730 EBDCA674 66A1CC3B 49118B24
    1051C495 FD28C814 2F76A13A 20DEBB73 866CC0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Hash(counter||no_of_bits_to_return||input_string) is
```

```
                        E7F19451 0674954D 9E49CEAC 2FD98109
        E08BEBBF FBBBA78C 16FEB723 64F49334 6BB916DB 78563AAD
        BD51A07D 55315AFB 4612F770 B4936987 47C3EC71 9C7BF6C0


    temp =
                          913CA0 13D788EA D14EDFA1 A5785741
        4B1D68E3 0D85930C 994EC8DE EE1B2F7E 744CAC32 88A442A4
        CD55A41F D1A0B265 B490812D 9000FFCC 6282474D 788DFB37
        81E7F194 51067495 4D9E49CE AC2FD981 09E08BEB BFFBBBA7
        8C16FEB7 2364F493 346BB916 DB78563A ADBD51A0 7D55315A


  V is
                          913CA0 13D788EA D14EDFA1 A5785741
        4B1D68E3 0D85930C 994EC8DE EE1B2F7E 744CAC32 88A442A4
        CD55A41F D1A0B265 B490812D 9000FFCC 6282474D 788DFB37
        81E7F194 51067495 4D9E49CE AC2FD981 09E08BEB BFFBBBA7
        8C16FEB7 2364F493 346BB916 DB78563A ADBD51A0 7D55315A


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                        00913CA0 13D788EA D14EDFA1 A5785741
        4B1D68E3 0D85930C 994EC8DE EE1B2F7E 744CAC32 88A442A4
        CD55A41F D1A0B265 B490812D 9000FFCC 6282474D 788DFB37
        81E7F194 51067495 4D9E49CE AC2FD981 09E08BEB BFFBBBA7
        8C16FEB7 2364F493 346BB916 DB78563A ADBD51A0 7D55315A


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00913CA0 13D788EA D14EDFA1 A5785741
        4B1D68E3 0D85930C 994EC8DE EE1B2F7E 744CAC32 88A442A4
        CD55A41F D1A0B265 B490812D 9000FFCC 6282474D 788DFB37
        81E7F194 51067495 4D9E49CE AC2FD981 09E08BEB BFFBBBA7
        8C16FEB7 2364F493 346BB916 DB78563A ADBD51A0 7D55315A
```

```
  Hash(counter||no_of_bits_to_return||input_string) is
                        9FA80ADB 6DC1CD99 3C00413B A974350B
      49725E33 4A188BEB 0A992B22 5C49DE64 CFE92B47 8B7589B6
      0649255A 304CA2EB 11BF7BB7 9021A86B A4F7BCD9 3679B8F7


  temp =
                        9FA80ADB 6DC1CD99 3C00413B A974350B
      49725E33 4A188BEB 0A992B22 5C49DE64 CFE92B47 8B7589B6
      0649255A 304CA2EB 11BF7BB7 9021A86B A4F7BCD9 3679B8F7


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
            02 00000378 00913CA0 13D788EA D14EDFA1 A5785741
      4B1D68E3 0D85930C 994EC8DE EE1B2F7E 744CAC32 88A442A4
      CD55A41F D1A0B265 B490812D 9000FFCC 6282474D 788DFB37
      81E7F194 51067495 4D9E49CE AC2FD981 09E08BEB BFFBBBA7
      8C16FEB7 2364F493 346BB916 DB78563A ADBD51A0 7D55315A


  Hash(counter||no_of_bits_to_return||input_string) is
                        356ED503 70D4A92A 84F44891 788408BE
      D41B4F3C 71B4FD1F 90D1480E 506B96A4 180D945C E02C4369
      876C3994 CA9463D6 887B6B27 457709FF FFCA9CE8 CE90D484


  temp =
                          9FA80A DB6DC1CD 993C0041 3BA97435
      0B49725E 334A188B EB0A992B 225C49DE 64CFE92B 478B7589
      B6064925 5A304CA2 EB11BF7B B79021A8 6BA4F7BC D93679B8
      F7356ED5 0370D4A9 2A84F448 91788408 BED41B4F 3C71B4FD
      1F90D148 0E506B96 A4180D94 5CE02C43 69876C39 94CA9463


C is
                          9FA80A DB6DC1CD 993C0041 3BA97435
      0B49725E 334A188B EB0A992B 225C49DE 64CFE92B 478B7589
      B6064925 5A304CA2 EB11BF7B B79021A8 6BA4F7BC D93679B8
      F7356ED5 0370D4A9 2A84F448 91788408 BED41B4F 3C71B4FD
      1F90D148 0E506B96 A4180D94 5CE02C43 69876C39 94CA9463
```

```
*************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                            913CA0 13D788EA D14EDFA1 A5785741
        4B1D68E3 0D85930C 994EC8DE EE1B2F7E 744CAC32 88A442A4
        CD55A41F D1A0B265 B490812D 9000FFCC 6282474D 788DFB37
        81E7F194 51067495 4D9E49CE AC2FD981 09E08BEB BFFBBBA7
        8C16FEB7 2364F493 346BB916 DB78563A ADBD51A0 7D55315A


    w_i is
                          DBE5EE36 FCD85301 303E1C36 17C1AC5E
        23C08885 D0BEFAAD 0C85A0D8 9F85B9F1 6ECE3D88 A24EB965
        04F2F13E FA704962 1782F5DE 2C416A0D 294CCFE5 3545C4E3


    W is
                          DBE5EE36 FCD85301 303E1C36 17C1AC5E
        23C08885 D0BEFAAD 0C85A0D8 9F85B9F1 6ECE3D88 A24EB965
        04F2F13E FA704962 1782F5DE 2C416A0D 294CCFE5 3545C4E3


    ------------

    i = 2

    data is
                            913CA0 13D788EA D14EDFA1 A5785741
        4B1D68E3 0D85930C 994EC8DE EE1B2F7E 744CAC32 88A442A4
```

```
        CD55A41F D1A0B265 B490812D 9000FFCC 6282474D 788DFB37
        81E7F194 51067495 4D9E49CE AC2FD981 09E08BEB BFFBBBA7
        8C16FEB7 2364F493 346BB916 DB78563A ADBD51A0 7D55315B


    w_i is
                         09C48E1E 285A2B82 9A574B72 B3C2FBE1
        34D01E37 06B486F2 401B9820 E17298A3 42666918 E15B8462
        87F8C5AF 2D96B20F AF3D0BB3 92E15F4A 06CDB0DE CD1B6AD7


    W is
                                           DBE5EE36 FCD85301
        303E1C36 17C1AC5E 23C08885 D0BEFAAD 0C85A0D8 9F85B9F1
        6ECE3D88 A24EB965 04F2F13E FA704962 1782F5DE 2C416A0D
        294CCFE5 3545C4E3 09C48E1E 285A2B82 9A574B72 B3C2FBE1
        34D01E37 06B486F2 401B9820 E17298A3 42666918 E15B8462
        87F8C5AF 2D96B20F AF3D0BB3 92E15F4A 06CDB0DE CD1B6AD7


  returned_bits is
                                           DBE5EE36 FCD85301
        303E1C36 17C1AC5E 23C08885 D0BEFAAD 0C85A0D8 9F85B9F1
        6ECE3D88 A24EB965 04F2F13E FA704962 1782F5DE 2C416A0D
        294CCFE5 3545C4E3 09C48E1E 285A2B82 9A574B72 B3C2FBE1
        34D01E37 06B486F2 401B9820 E17298A3 42666918 E15B8462
        87F8C5AF 2D96B20F AF3D0BB3 92E15F4A 06CDB0DE CD1B6AD7


---------------------------

  Update V

    0x03||V is
                         03913CA0 13D788EA D14EDFA1 A5785741
        4B1D68E3 0D85930C 994EC8DE EE1B2F7E 744CAC32 88A442A4
        CD55A41F D1A0B265 B490812D 9000FFCC 6282474D 788DFB37
        81E7F194 51067495 4D9E49CE AC2FD981 09E08BEB BFFBBBA7
        8C16FEB7 2364F493 346BB916 DB78563A ADBD51A0 7D55315A


    H is
                         73FD2839 3EFADC11 1ADBC674 E19D8341
        76345539 6AC56861 F86260C7 4918A450 5D41B9D7 5FC254C0
        2EE70292 ED511374 3F2C179A A23149FC 18F27654 98319719
```

Updated values

V is

```
                          30E4AA EF454AB8 6A8ADFE2 E121CB76
       5666DB41 40CFAB98 8459620A 1077795C D91C955D D02FB82E
       835BED45 2BD0FF09 139F68E2 868BFD85 E903057F 3361F831
       EF51B5A2 BF3CB1A0 70859EDE 86C101DA 25F66112 5C2FC564
       DA8ED292 1F06739E 17AFDE45 DA89CC7A 3037342E AA515CD7
```

reseed_counter is

```
                                                0000 00000002
```

rnd_val is

```
                                           DBE5EE36 FCD85301
       303E1C36 17C1AC5E 23C08885 D0BEFAAD 0C85A0D8 9F85B9F1
       6ECE3D88 A24EB965 04F2F13E FA704962 1782F5DE 2C416A0D
       294CCFE5 3545C4E3 09C48E1E 285A2B82 9A574B72 B3C2FBE1
       34D01E37 06B486F2 401B9820 E17298A3 42666918 E15B8462
       87F8C5AF 2D96B20F AF3D0BB3 92E15F4A 06CDB0DE CD1B6AD7
```

```
###############################################################

HMAC_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                      20 21222324


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    nonce is
                                                        20 21222324


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                                     00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


  Key is
                 00000000 00000000 00000000 00000000 00000000


  V is
                 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                                     00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    ------------

    V || 0x00 || provided_data is
                                           01 01010101 01010101
        01010101 01010101 01010100 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    K = HMAC(K, V || 0x00 || provided_data) is
                 C11B066D 8601D7F1 10C65AE7 750C4937 052014A1
```

```
    V = HMAC(K, V) is
                FB07A09C 7E6E4644 39B497DD F3293B58 35819502


    ------------

    V || 0x01 || provided_data is
                                          FB 07A09C7E 6E464439
        B497DDF3 293B5835 81950201 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    K = HMAC(K, V || 0x01 || provided_data) is
                AB160DD2 1C30980C A3CA5A9C 77B7BDF0 50E64EE9


    V = HMAC(K, V) is
                614499EA 980CFB3D AA2CA86D 65A46BF4 488D8CC5


  Update (Key, V):

    Key is
                AB160DD2 1C30980C A3CA5A9C 77B7BDF0 50E64EE9


    V is
                614499EA 980CFB3D AA2CA86D 65A46BF4 488D8CC5


---------------------------------------------------------------

First call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
```

```
                5A7D3B44 9F481CB3 8DF79AD2 B1FCC01E 57F8135E


    temp is
                5A7D3B44 9F481CB3 8DF79AD2 B1FCC01E 57F8135E


  ------------

    V = HMAC(K, V) is
                8C0B22CD 0630BFB0 127FB540 8C8EFC17 A929896E


    temp is
                           5A7D3B44 9F481CB3 8DF79AD2 B1FCC01E
        57F8135E 8C0B22CD 0630BFB0 127FB540 8C8EFC17 A929896E


---------------------------

  returned_bits is
                           5A7D3B44 9F481CB3 8DF79AD2 B1FCC01E
        57F8135E 8C0B22CD 0630BFB0 127FB540 8C8EFC17 A929896E


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
              8C 0B22CD06 30BFB012 7FB5408C 8EFC17A9 29896E00


    K = HMAC(K, V || 0x00 || provided_data) is
                7BB18028 E01D0342 DF4F54DA 5122FA5F 2C3A05E4


    V = HMAC(K, V) is
                2F894F28 CC2F5382 9640643A D17B84B0 CD3C7979
```

```
rnd_val is
                          5A7D3B44 9F481CB3 8DF79AD2 B1FCC01E
        57F8135E 8C0B22CD 0630BFB0 127FB540 8C8EFC17 A929896E


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                  82CF772E C3E84B00 FC74F5DF 104EFBFB 2428554E


    temp is
                  82CF772E C3E84B00 FC74F5DF 104EFBFB 2428554E


  ------------

    V = HMAC(K, V) is
                  9CE367D0 3AEADE37 827FA8E9 CB6A0819 6115D948


    temp is
                          82CF772E C3E84B00 FC74F5DF 104EFBFB
        2428554E 9CE367D0 3AEADE37 827FA8E9 CB6A0819 6115D948


---------------------------

  returned_bits is
                          82CF772E C3E84B00 FC74F5DF 104EFBFB
        2428554E 9CE367D0 3AEADE37 827FA8E9 CB6A0819 6115D948


  call Update(additional_input, K, V)
```

```
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
              9C E367D03A EADE3782 7FA8E9CB 6A081961 15D94800


    K = HMAC(K, V || 0x00 || provided_data) is
                 3D4D7377 E9172AAF A776B0DD CB894200 4A44B7FD


    V = HMAC(K, V) is
                 1A26BD9B FC9744BD 29F6AEBE 2437E209 F1F71625


rnd_val is
                          82CF772E C3E84B00 FC74F5DF 104EFBFB
         2428554E 9CE367D0 3AEADE37 827FA8E9 CB6A0819 6115D948


################################################################

HMAC_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

```
    EntropyInput2 (for Reseed2) =
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                    20 21222324


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                    20 21222324


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                                    00010203 04050607 08090A0B
```

```
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


  Key is
                00000000 00000000 00000000 00000000 00000000


  V is
                01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                                    00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    ------------

    V || 0x00 || provided_data is
                                          01 01010101 01010101
        01010101 01010101 01010100 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    K = HMAC(K, V || 0x00 || provided_data) is
                C11B066D 8601D7F1 10C65AE7 750C4937 052014A1


    V = HMAC(K, V) is
                FB07A09C 7E6E4644 39B497DD F3293B58 35819502


    ------------

    V || 0x01 || provided_data is
                                          FB 07A09C7E 6E464439
        B497DDF3 293B5835 81950201 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324
```

```
    K = HMAC(K, V || 0x01 || provided_data) is
                 AB160DD2 1C30980C A3CA5A9C 77B7BDF0 50E64EE9


    V = HMAC(K, V) is
                 614499EA 980CFB3D AA2CA86D 65A46BF4 488D8CC5


  Update (Key, V):

    Key is
                 AB160DD2 1C30980C A3CA5A9C 77B7BDF0 50E64EE9


    V is
                 614499EA 980CFB3D AA2CA86D 65A46BF4 488D8CC5


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
```

```
  ------------

  V || 0x00 || provided_data is
                                                      614499EA
      980CFB3D AA2CA86D 65A46BF4 488D8CC5 00606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  K = HMAC(K, V || 0x00 || provided_data) is
               E8C6B0A1 D480E7D6 C3B41065 EBED069A E157CBC3


  V = HMAC(K, V) is
               CBEDC05C 2C54CA75 334BD647 06FC3EF8 7B4E328E


  ------------

  V || 0x01 || provided_data is
                                                      CBEDC05C
      2C54CA75 334BD647 06FC3EF8 7B4E328E 01606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  K = HMAC(K, V || 0x01 || provided_data) is
               48B3AD2B 21D8EF7E A766C6B5 21A2FC3F B1E42935


  V = HMAC(K, V) is
               C5B984AC 3985C236 0E73B018 2F9FBDC7 3251FFD3


------------

  V = HMAC(K, V) is
               C7AAAC58 3C6EF630 0714C2CC 5D06C148 CFFB4044


  temp is
               C7AAAC58 3C6EF630 0714C2CC 5D06C148 CFFB4044


------------
```

```
    V = HMAC(K, V) is
                 9AD0BB26 FAC0497B 5C57E161 E36681BC C930CE80


    temp is
                          C7AAAC58 3C6EF630 0714C2CC 5D06C148
         CFFB4044 9AD0BB26 FAC0497B 5C57E161 E36681BC C930CE80


---------------------------

  returned_bits is
                          C7AAAC58 3C6EF630 0714C2CC 5D06C148
         CFFB4044 9AD0BB26 FAC0497B 5C57E161 E36681BC C930CE80


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                606162 63646566
         6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
         7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                                                          9AD0BB26
         FAC0497B 5C57E161 E36681BC C930CE80 00606162 63646566
         6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
         7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                 AC235DC4 2E53D55A 20FAA9F0 6543E29A 799D3DE2


    V = HMAC(K, V) is
                 5106A127 D021DB3E 76AAEC1D 24D4DAAE 7BA91FF2


    ------------
```

```
    V || 0x01 || provided_data is
                                                        5106A127
        D021DB3E 76AAEC1D 24D4DAAE 7BA91FF2 01606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
                 3A062E6B 79FE70DB FFEB3A2B 6BE80323 F7D674C5


    V = HMAC(K, V) is
                 BD363128 BF580D7A 54429DDD 58E8193B 9843BD2B


rnd_val is
                          C7AAAC58 3C6EF630 0714C2CC 5D06C148
        CFFB4044 9AD0BB26 FAC0497B 5C57E161 E36681BC C930CE80


------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
```

```
  ------------

  V || 0x00 || provided_data is
                                                        BD363128
      BF580D7A 54429DDD 58E8193B 9843BD2B 00A0A1A2 A3A4A5A6
      A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
      BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  K = HMAC(K, V || 0x00 || provided_data) is
                D7CDFD76 F19B373F E9FEBC06 115278C8 5DD14375


  V = HMAC(K, V) is
                D06F8199 E16826AF 9EC3486F B76DA833 E2BB11E5


  ------------

  V || 0x01 || provided_data is
                                                        D06F8199
      E16826AF 9EC3486F B76DA833 E2BB11E5 01A0A1A2 A3A4A5A6
      A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
      BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  K = HMAC(K, V || 0x01 || provided_data) is
                D1B575BC 767410DB B5E2F7F7 586BB421 CCCD5E22


  V = HMAC(K, V) is
                C4BB579E 7E2A0A94 5A408C61 28446BFF DD211A16


------------

  V = HMAC(K, V) is
                6EBD2B7B 5E0A2AD7 A24B1BF9 A1DBA47D 43271719


  temp is
                6EBD2B7B 5E0A2AD7 A24B1BF9 A1DBA47D 43271719
```

```
  ------------

    V = HMAC(K, V) is
                B9C37B7F E81BA940 45A14A7C B514B446 666EA5A7


    temp is
                           6EBD2B7B 5E0A2AD7 A24B1BF9 A1DBA47D
        43271719 B9C37B7F E81BA940 45A14A7C B514B446 666EA5A7


---------------------------

  returned_bits is
                           6EBD2B7B 5E0A2AD7 A24B1BF9 A1DBA47D
        43271719 B9C37B7F E81BA940 45A14A7C B514B446 666EA5A7


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                                                         B9C37B7F
        E81BA940 45A14A7C B514B446 666EA5A7 00A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                7FDB1E3A A4B1368E 03C63FC8 F4A05A88 E7A9A11A


    V = HMAC(K, V) is
                D48C4E59 EDA3F929 3282AD19 29A854ED FA128BB7
```

```
    ------------

    V || 0x01 || provided_data is
                                                          D48C4E59
        EDA3F929 3282AD19 29A854ED FA128BB7 01A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
                 8AD7E347 72B5FC7C 3B3B2762 4F0B9177 6A8A7112


    V = HMAC(K, V) is
                 D71376A4 6D764B17 C3B73934 7B384E51 51E87E88


rnd_val is
                           6EBD2B7B 5E0A2AD7 A24B1BF9 A1DBA47D
        43271719 B9C37B7F E81BA940 45A14A7C B514B446 666EA5A7


################################################################

HMAC_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                 C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
```

DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6

Nonce =
20 21222324

PersonalizationString =
404142 43444546
4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576

AdditionalInput = <empty>

##

****

HMAC_DRBG_Instantiate_algorithm

entropy_input is
000102 03040506
0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536

nonce is
20 21222324

personal_str is
404142 43444546
4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576

prediction_resistance_flag = "No PredictionResistance"

Seed_Material is
000102 03040506 0708090A 0B0C0D0E 0F101112
13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576

```
  Key is
                00000000 00000000 00000000 00000000 00000000

  V is
                01010101 01010101 01010101 01010101 01010101

--------------------------

  Update

    provided_data
                  000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    ------------

    V || 0x00 || provided_data is
                         01010101 01010101 01010101 01010101
        01010101 00000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x00 || provided_data) is
                3F7A620C 6BED0A29 2CB8E7D7 6DCEA617 67E060D5


    V = HMAC(K, V) is
                5848B848 182B6499 F6348807 E3CFE186 EE05FE25


    ------------

    V || 0x01 || provided_data is
                         5848B848 182B6499 F6348807 E3CFE186
        EE05FE25 01000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
```

```
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x01 || provided_data) is
                B7D966D7 0D4E27A7 FA838F7D 61126C0E DC84761C


    V = HMAC(K, V) is
                DAB2A718 83F1005C 5DD03932 4D3C364D 6E18F954


  Update (Key, V):

    Key is
                B7D966D7 0D4E27A7 FA838F7D 61126C0E DC84761C


    V is
                DAB2A718 83F1005C 5DD03932 4D3C364D 6E18F954


-----------------------------------------------------------

First call to Generate

***********************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                B3BD0524 6CBA12A6 4735A4E3 FDE599BC 1BE30F43


    temp is
                B3BD0524 6CBA12A6 4735A4E3 FDE599BC 1BE30F43


  ------------
```

```
    V = HMAC(K, V) is
                  9BD06020 8EEA7D71 F9D123DF 47B3CE06 9D98EDE6


    temp is
                            B3BD0524 6CBA12A6 4735A4E3 FDE599BC
         1BE30F43 9BD06020 8EEA7D71 F9D123DF 47B3CE06 9D98EDE6


---------------------------

  returned_bits is
                            B3BD0524 6CBA12A6 4735A4E3 FDE599BC
         1BE30F43 9BD06020 8EEA7D71 F9D123DF 47B3CE06 9D98EDE6


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
              9B D060208E EA7D71F9 D123DF47 B3CE069D 98EDE600


    K = HMAC(K, V || 0x00 || provided_data) is
                  87D3828B E03A807D D3402941 BED6DE98 6EE7A286


    V = HMAC(K, V) is
                  6AE1D008 6F53B1B7 63A4515B 1906FEE4 7661FD47


rnd_val is
                            B3BD0524 6CBA12A6 4735A4E3 FDE599BC
         1BE30F43 9BD06020 8EEA7D71 F9D123DF 47B3CE06 9D98EDE6


---------------------------------------------------------------

Second call to Generate
```

```
***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                 B5DADA38 0E2872DF 935BCA55 B882C8C9 376902AB


    temp is
                 B5DADA38 0E2872DF 935BCA55 B882C8C9 376902AB


  ------------

    V = HMAC(K, V) is
                 63976547 2B71ACEB E2EA8B1B 6B49629C B67317E0


    temp is
                           B5DADA38 0E2872DF 935BCA55 B882C8C9
        376902AB 63976547 2B71ACEB E2EA8B1B 6B49629C B67317E0


---------------------------

  returned_bits is
                           B5DADA38 0E2872DF 935BCA55 B882C8C9
        376902AB 63976547 2B71ACEB E2EA8B1B 6B49629C B67317E0


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------
```

```
    V || 0x00 || provided_data is
              63 9765472B 71ACEBE2 EA8B1B6B 49629CB6 7317E000


    K = HMAC(K, V || 0x00 || provided_data) is
                 26ABBF54 B28B93FF 9008670E BFEE86CD D7228ED5


    V = HMAC(K, V) is
                 E9254729 E00204A1 B6C02158 A6C72786 4714F1F7


rnd_val is
                           B5DADA38 0E2872DF 935BCA55 B882C8C9
        376902AB 63976547 2B71ACEB E2EA8B1B 6B49629C B67317E0


################################################################

HMAC_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                 C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                       20 21222324
```

```
    PersonalizationString =
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                    20 21222324


    personal_str is
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                  000102 03040506 0708090A 0B0C0D0E 0F101112
```

```
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                00000000 00000000 00000000 00000000 00000000


  V is
                01010101 01010101 01010101 01010101 01010101


----------------------------

  Update

    provided_data
                 000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    ------------

    V || 0x00 || provided_data is
                         01010101 01010101 01010101 01010101
        01010101 00000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x00 || provided_data) is
                3F7A620C 6BED0A29 2CB8E7D7 6DCEA617 67E060D5


    V = HMAC(K, V) is
                5848B848 182B6499 F6348807 E3CFE186 EE05FE25


    ------------
```

```
    V || 0x01 || provided_data is
                          5848B848 182B6499 F6348807 E3CFE186
        EE05FE25 01000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x01 || provided_data) is
                 B7D966D7 0D4E27A7 FA838F7D 61126C0E DC84761C


    V = HMAC(K, V) is
                 DAB2A718 83F1005C 5DD03932 4D3C364D 6E18F954


  Update (Key, V):

    Key is
                 B7D966D7 0D4E27A7 FA838F7D 61126C0E DC84761C


    V is
                 DAB2A718 83F1005C 5DD03932 4D3C364D 6E18F954


-----------------------------------------------------------

First call to Generate

***********************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is
                                              606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  additional_input <> NULL, call Update(additional_input, K, V)
--------------------------
```

```
Update

  provided_data
                                                606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  ------------

  V || 0x00 || provided_data is
                                                        DAB2A718
      83F1005C 5DD03932 4D3C364D 6E18F954 00606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  K = HMAC(K, V || 0x00 || provided_data) is
              94FF0C25 4EAFC7D7 EA314E83 780A09DF 46A5F1A3


  V = HMAC(K, V) is
              7A8FE422 EE665D07 1F63841D CE347CED A6CC07AE


  ------------

  V || 0x01 || provided_data is
                                                        7A8FE422
      EE665D07 1F63841D CE347CED A6CC07AE 01606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  K = HMAC(K, V || 0x01 || provided_data) is
              92AF76A0 7C0A556E 579044B6 A1F19ED9 52727FB6


  V = HMAC(K, V) is
              21BE014B CE5FFB6A 569DDEB6 4F0901F8 469BA704


------------

  V = HMAC(K, V) is
```

```
                1F8FEC7B C7CFA9A8 80345D28 0B13C632 B852770A


    temp is
                1F8FEC7B C7CFA9A8 80345D28 0B13C632 B852770A


  ------------

    V = HMAC(K, V) is
                6DFC302E AD4CE3F5 54C79B0D 44239EBA 56A7EA2D


    temp is
                           1F8FEC7B C7CFA9A8 80345D28 0B13C632
        B852770A 6DFC302E AD4CE3F5 54C79B0D 44239EBA 56A7EA2D


---------------------------

  returned_bits is
                           1F8FEC7B C7CFA9A8 80345D28 0B13C632
        B852770A 6DFC302E AD4CE3F5 54C79B0D 44239EBA 56A7EA2D


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                                                         6DFC302E
        AD4CE3F5 54C79B0D 44239EBA 56A7EA2D 00606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
```

```
                E5B19979 A077728F A891F907 57A39527 1BA998E2


    V = HMAC(K, V) is
                330D2882 2736520F B8C295D8 B853CF90 E6A7F04E


    ------------

    V || 0x01 || provided_data is
                                                        330D2882
        2736520F B8C295D8 B853CF90 E6A7F04E 01606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
                17A5D79F 0767876F 3A45E0C9 C33EC88B 03CEEA13


    V = HMAC(K, V) is
                4D2F3BC7 77505C45 F7E17DCD 3D86BF37 9CB6025E


rnd_val is
                          1F8FEC7B C7CFA9A8 80345D28 0B13C632
        B852770A 6DFC302E AD4CE3F5 54C79B0D 44239EBA 56A7EA2D


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  additional_input <> NULL, call Update(additional_input, K, V)
```

```
---------------------------

  Update

    provided_data
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                                                          4D2F3BC7
        77505C45 F7E17DCD 3D86BF37 9CB6025E 00A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                 7024EBA2 2F9EFDF9 43CCD4A5 3C3E3EBE 1C328E49


    V = HMAC(K, V) is
                 6EF6820D D3C9BB9C 42D91D32 AC3CF56A 59A7A161


    ------------

    V || 0x01 || provided_data is
                                                          6EF6820D
        D3C9BB9C 42D91D32 AC3CF56A 59A7A161 01A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
                 41EDB8EA 2E6E4A25 D9E1A3BC DB40CF35 7976422B


    V = HMAC(K, V) is
                 0E8B49B1 D57E64FE F896BCDB C08920FC 58AC87F8


  ------------
```

```
    V = HMAC(K, V) is
                 AF97CDE1 E8AB322A 2EACA8E6 F4E5BF78 A11BDEF7


    temp is
                 AF97CDE1 E8AB322A 2EACA8E6 F4E5BF78 A11BDEF7


  ------------

    V = HMAC(K, V) is
                 DC91215D 44B107B4 D5A77901 59250976 5280F969


    temp is
                          AF97CDE1 E8AB322A 2EACA8E6 F4E5BF78
        A11BDEF7 DC91215D 44B107B4 D5A77901 59250976 5280F969


---------------------------

  returned_bits is
                          AF97CDE1 E8AB322A 2EACA8E6 F4E5BF78
        A11BDEF7 DC91215D 44B107B4 D5A77901 59250976 5280F969


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                                                       DC91215D
        44B107B4 D5A77901 59250976 5280F969 00A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
```

```
    K = HMAC(K, V || 0x00 || provided_data) is
                 2CCF0DC9 D717135E 3D52BEC8 82B48902 B559A2B5


    V = HMAC(K, V) is
                 16609755 A8B2C412 E44C47F5 891FBAF6 645505E8


    ------------

    V || 0x01 || provided_data is
                                                        16609755
        A8B2C412 E44C47F5 891FBAF6 645505E8 01A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
                 079B57D9 406E11C2 F87C8C82 8C8C6FA7 6E40EA01


    V = HMAC(K, V) is
                 A654FE72 F8A77BB8 F03DFF07 C79A5153 009EDDDA


rnd_val is
                          AF97CDE1 E8AB322A 2EACA8E6 F4E5BF78
        A11BDEF7 DC91215D 44B107B4 D5A77901 59250976 5280F969


################################################################

HMAC_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                               000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
```

```
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                      20 21222324


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                      20 21222324


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                                    00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


  Key is
```

```
                00000000 00000000 00000000 00000000 00000000

  V is
                01010101 01010101 01010101 01010101 01010101

---------------------------

  Update

    provided_data
                                    00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    ------------

    V || 0x00 || provided_data is
                                           01 01010101 01010101
        01010101 01010101 01010100 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    K = HMAC(K, V || 0x00 || provided_data) is
                C11B066D 8601D7F1 10C65AE7 750C4937 052014A1


    V = HMAC(K, V) is
                FB07A09C 7E6E4644 39B497DD F3293B58 35819502


    ------------

    V || 0x01 || provided_data is
                                           FB 07A09C7E 6E464439
        B497DDF3 293B5835 81950201 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    K = HMAC(K, V || 0x01 || provided_data) is
                AB160DD2 1C30980C A3CA5A9C 77B7BDF0 50E64EE9
```

```
    V = HMAC(K, V) is
                614499EA 980CFB3D AA2CA86D 65A46BF4 488D8CC5


  Update (Key, V):

    Key is
                AB160DD2 1C30980C A3CA5A9C 77B7BDF0 50E64EE9


    V is
                614499EA 980CFB3D AA2CA86D 65A46BF4 488D8CC5


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                              808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    additional_input is  <empty>

  Seed_Material is
                                              808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

Key is
AB160DD2 1C30980C A3CA5A9C 77B7BDF0 50E64EE9

V is
614499EA 980CFB3D AA2CA86D 65A46BF4 488D8CC5

Update

provided_data
808182 83848586
8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6

V || 0x00 || provided_data is
614499EA
980CFB3D AA2CA86D 65A46BF4 488D8CC5 00808182 83848586
8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6

K = HMAC(K, V || 0x00 || provided_data) is
B365E8D2 ABCB06AE EF8094A3 768F6FA5 8402966D

V = HMAC(K, V) is
91EC2556 8078AA94 0A447074 33004BB0 A388B056

V || 0x01 || provided_data is
91EC2556
8078AA94 0A447074 33004BB0 A388B056 01808182 83848586
8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6

K = HMAC(K, V || 0x01 || provided_data) is
CD4CAB38 C8AD6571 22BF5D3D 00D0AC9B 13D629BB

```
    V = HMAC(K, V) is
                F660E23E 91006B62 C6543AB1 344D23A3 1AB4CF2C


  Update (Key, V):

    Key is
                CD4CAB38 C8AD6571 22BF5D3D 00D0AC9B 13D629BB


    V is
                F660E23E 91006B62 C6543AB1 344D23A3 1AB4CF2C

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                FEC4597F 06A3A8CC 8529D595 57B9E661 053809C0


    temp is
                FEC4597F 06A3A8CC 8529D595 57B9E661 053809C0


  ------------

    V = HMAC(K, V) is
                BC0EFC28 2ABD8760 5CC90CBA 9B8633DC B1DAE02E


    temp is
                          FEC4597F 06A3A8CC 8529D595 57B9E661
        053809C0 BC0EFC28 2ABD8760 5CC90CBA 9B8633DC B1DAE02E


--------------------------
```

```
  returned_bits is
                          FEC4597F 06A3A8CC 8529D595 57B9E661
        053809C0 BC0EFC28 2ABD8760 5CC90CBA 9B8633DC B1DAE02E


  call Update(additional_input, K, V)
----------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
              BC 0EFC282A BD87605C C90CBA9B 8633DCB1 DAE02E00


    K = HMAC(K, V || 0x00 || provided_data) is
                587FD821 EF6C9DA4 A83C1921 1F1056CA CD23FC1A


    V = HMAC(K, V) is
                848FD14C 13B7EA93 720CCFDE 71F2F644 39DB795D


rnd_val is
                          FEC4597F 06A3A8CC 8529D595 57B9E661
        053809C0 BC0EFC28 2ABD8760 5CC90CBA 9B8633DC B1DAE02E


------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

Generate FAILED: Reseed is required
************************************************************
```

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6

    additional_input is <empty>

  Seed_Material is
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6

  Key is
                587FD821 EF6C9DA4 A83C1921 1F1056CA CD23FC1A

  V is
                848FD14C 13B7EA93 720CCFDE 71F2F644 39DB795D

  Update

    provided_data
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6

    V || 0x00 || provided_data is
                                                            848FD14C
        13B7EA93 720CCFDE 71F2F644 39DB795D 00C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6

    K = HMAC(K, V || 0x00 || provided_data) is
                E99B2A74 468B6877 0F2F00C0 9C1F5850 BE543344

```
    V = HMAC(K, V) is
                42138429 41CC9219 A1D0C6D0 E0C96DA3 DF303937


    ------------

    V || 0x01 || provided_data is
                                                        42138429
        41CC9219 A1D0C6D0 E0C96DA3 DF303937 01C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    K = HMAC(K, V || 0x01 || provided_data) is
                DBA1CFF4 879546A0 38A559B2 A24DF2C0 30089A41


    V = HMAC(K, V) is
                2F883C46 48E131E8 6DDF9DCA 0D74F30C A1CE6EFB


  Update (Key, V):

    Key is
                DBA1CFF4 879546A0 38A559B2 A24DF2C0 30089A41


    V is
                2F883C46 48E131E8 6DDF9DCA 0D74F30C A1CE6EFB


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                84ADD5E2 D2041C01 723A4DE4 335B13EF DF16B0E5
```

```
    temp is
                 84ADD5E2 D2041C01 723A4DE4 335B13EF DF16B0E5


  ------------

    V = HMAC(K, V) is
                 1A0AD39B D15E862E 644F31E4 A2D7D843 E57C5968


    temp is
                           84ADD5E2 D2041C01 723A4DE4 335B13EF
        DF16B0E5 1A0AD39B D15E862E 644F31E4 A2D7D843 E57C5968


----------------------------

  returned_bits is
                           84ADD5E2 D2041C01 723A4DE4 335B13EF
        DF16B0E5 1A0AD39B D15E862E 644F31E4 A2D7D843 E57C5968


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
              1A 0AD39BD1 5E862E64 4F31E4A2 D7D843E5 7C596800


    K = HMAC(K, V || 0x00 || provided_data) is
                 F939A5AB 08A39F23 1070B0D4 C96DC237 90BA0153


    V = HMAC(K, V) is
                 CE6D08B4 AE2CE383 FDABB01E AAFC9C8E 76A0D472


rnd_val is
                           84ADD5E2 D2041C01 723A4DE4 335B13EF
```

DF16B0E5 1A0AD39B D15E862E 644F31E4 A2D7D843 E57C5968

##

HMAC_DRBG

Requested Security Strength = 80

Requested Hash Algorithm = SHA-1

prediction_resistance_flag = "ENABLED"
EntropyInput =
000102 03040506
0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536

EntropyInput1 (for Reseed1) =
808182 83848586
8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6

EntropyInput2 (for Reseed2) =
C0C1C2 C3C4C5C6
C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6

Nonce =
20 21222324

PersonalizationString = <empty>

AdditionalInput1 =
606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596

AdditionalInput2 =
A0A1A2 A3A4A5A6
A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6

```
###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                       20 21222324


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                                    00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


  Key is
                00000000 00000000 00000000 00000000 00000000


  V is
                01010101 01010101 01010101 01010101 01010101


--------------------------

  Update

    provided_data
                                    00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324
```

```
    ------------

    V || 0x00 || provided_data is
                                          01 01010101 01010101
        01010101 01010101 01010100 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    K = HMAC(K, V || 0x00 || provided_data) is
                 C11B066D 8601D7F1 10C65AE7 750C4937 052014A1


    V = HMAC(K, V) is
                 FB07A09C 7E6E4644 39B497DD F3293B58 35819502


    ------------

    V || 0x01 || provided_data is
                                          FB 07A09C7E 6E464439
        B497DDF3 293B5835 81950201 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    K = HMAC(K, V || 0x01 || provided_data) is
                 AB160DD2 1C30980C A3CA5A9C 77B7BDF0 50E64EE9


    V = HMAC(K, V) is
                 614499EA 980CFB3D AA2CA86D 65A46BF4 488D8CC5


  Update (Key, V):

    Key is
                 AB160DD2 1C30980C A3CA5A9C 77B7BDF0 50E64EE9


    V is
                 614499EA 980CFB3D AA2CA86D 65A46BF4 488D8CC5


-----------------------------------------------------------------
```

```
First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Seed_Material is
                             8081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Key is
                AB160DD2 1C30980C A3CA5A9C 77B7BDF0 50E64EE9


  V is
                614499EA 980CFB3D AA2CA86D 65A46BF4 488D8CC5
```

```
---------------------------

  Update

    provided_data
                                8081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                                      614499 EA980CFB 3DAA2CA8
        6D65A46B F4488D8C C5008081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                 580F7D3D 738FBF1C 8D9ACE0D 52CB00C4 B490CE86


    V = HMAC(K, V) is
                 1F06F616 E7D08B5B F2947CB1 DC295B71 46ED65CE


    ------------

    V || 0x01 || provided_data is
                                      1F06F6 16E7D08B 5BF2947C
        B1DC295B 7146ED65 CE018081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
                 5228A4B6 A4469290 5EC044BF F0BB4E25 A387CAC1
```

```
    V = HMAC(K, V) is
                  247732D0 4CB84ED4 1ADD95A4 B78B50CD 9B3D3F32


  Update (Key, V):

    Key is
                  5228A4B6 A4469290 5EC044BF F0BB4E25 A387CAC1


    V is
                  247732D0 4CB84ED4 1ADD95A4 B78B50CD 9B3D3F32


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                  A1BA8FA5 8BB5013F 43F7B6ED 52B4539F A16DC779


    temp is
                  A1BA8FA5 8BB5013F 43F7B6ED 52B4539F A16DC779


  ------------

    V = HMAC(K, V) is
                  57AEE815 B9C07004 C7E992EB 8C7E5919 64AFEEA2


    temp is
                           A1BA8FA5 8BB5013F 43F7B6ED 52B4539F
        A16DC779 57AEE815 B9C07004 C7E992EB 8C7E5919 64AFEEA2


---------------------------
```

```
  returned_bits is
                           A1BA8FA5 8BB5013F 43F7B6ED 52B4539F
        A16DC779 57AEE815 B9C07004 C7E992EB 8C7E5919 64AFEEA2


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
              57 AEE815B9 C07004C7 E992EB8C 7E591964 AFEEA200


    K = HMAC(K, V || 0x00 || provided_data) is
                 AB3DD489 5BC8CD22 71DEBA5F 3C136352 6B8B7452


    V = HMAC(K, V) is
                 A866C5EF F2AF042B 11864494 45237F9C 02449864


rnd_val is
                           A1BA8FA5 8BB5013F 43F7B6ED 52B4539F
        A16DC779 57AEE815 B9C07004 C7E992EB 8C7E5919 64AFEEA2


-------------------------------------------------------------

Second call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is
                                              A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
```

```
Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Seed_Material is
                             C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Key is
                AB3DD489 5BC8CD22 71DEBA5F 3C136352 6B8B7452


  V is
                A866C5EF F2AF042B 11864494 45237F9C 02449864


---------------------------

  Update

    provided_data
                             C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
```

```
  ------------

  V || 0x00 || provided_data is
                                    A866C5 EFF2AF04 2B118644
      9445237F 9C024498 6400C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
      CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
      E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
      A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
      BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  K = HMAC(K, V || 0x00 || provided_data) is
                C908BF7E 4FC908C3 17B20887 77CC961F 8173EACB


  V = HMAC(K, V) is
                915C0615 0BC71C0D 01B8B479 3E01367E 59F8BE44


  ------------

  V || 0x01 || provided_data is
                                    915C06 150BC71C 0D01B8B4
      793E0136 7E59F8BE 4401C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
      CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
      E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
      A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
      BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  K = HMAC(K, V || 0x01 || provided_data) is
                E5739F9C F7FF4384 D1273E02 6B453121 36494F41


  V = HMAC(K, V) is
                30C34305 C2C648B0 57A64022 1B5C5657 26CD32B2


Update (Key, V):

  Key is
                E5739F9C F7FF4384 D1273E02 6B453121 36494F41


  V is
                30C34305 C2C648B0 57A64022 1B5C5657 26CD32B2
```

```
*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                 84264A73 A818C95C 2F424B37 D3CC990B 046FB50C


    temp is
                 84264A73 A818C95C 2F424B37 D3CC990B 046FB50C


  ------------

    V = HMAC(K, V) is
                 2DC64A16 4211889A 010F2471 A0912FFE A1BF0195


    temp is
                           84264A73 A818C95C 2F424B37 D3CC990B
        046FB50C 2DC64A16 4211889A 010F2471 A0912FFE A1BF0195


---------------------------

  returned_bits is
                           84264A73 A818C95C 2F424B37 D3CC990B
        046FB50C 2DC64A16 4211889A 010F2471 A0912FFE A1BF0195


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------
```

```
    V || 0x00 || provided_data is
              2D C64A1642 11889A01 0F2471A0 912FFEA1 BF019500


    K = HMAC(K, V || 0x00 || provided_data) is
                 6191CA9B F000D10A 71690AC1 0E09FFC8 92ABDE9A


    V = HMAC(K, V) is
                 1EC0490F A0B76552 7E5EA18B 5322B28B DD0E7BC0


rnd_val is
                           84264A73 A818C95C 2F424B37 D3CC990B
        046FB50C 2DC64A16 4211889A 010F2471 A0912FFE A1BF0195


################################################################

HMAC_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                 C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
```

```
                                                    20 21222324


    PersonalizationString =
                                                   404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                   000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                    20 21222324


    personal_str is
                                                   404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                  000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                00000000 00000000 00000000 00000000 00000000
```

```
  V is
                01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                   000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    ------------

    V || 0x00 || provided_data is
                          01010101 01010101 01010101 01010101
        01010101 00000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x00 || provided_data) is
                3F7A620C 6BED0A29 2CB8E7D7 6DCEA617 67E060D5


    V = HMAC(K, V) is
                5848B848 182B6499 F6348807 E3CFE186 EE05FE25


    ------------

    V || 0x01 || provided_data is
                          5848B848 182B6499 F6348807 E3CFE186
        EE05FE25 01000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576
```

```
    K = HMAC(K, V || 0x01 || provided_data) is
                B7D966D7 0D4E27A7 FA838F7D 61126C0E DC84761C

    V = HMAC(K, V) is
                DAB2A718 83F1005C 5DD03932 4D3C364D 6E18F954

  Update (Key, V):

    Key is
                B7D966D7 0D4E27A7 FA838F7D 61126C0E DC84761C

    V is
                DAB2A718 83F1005C 5DD03932 4D3C364D 6E18F954

-----------------------------------------------------------------

First call to Generate

*****************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

Generate FAILED: Reseed is required
*****************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                              808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6

    additional_input is  <empty>

  Seed_Material is
                                              808182 83848586
```

```
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  Key is
                B7D966D7 0D4E27A7 FA838F7D 61126C0E DC84761C


  V is
                DAB2A718 83F1005C 5DD03932 4D3C364D 6E18F954


---------------------------

  Update

    provided_data
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    ------------

    V || 0x00 || provided_data is
                                                        DAB2A718
        83F1005C 5DD03932 4D3C364D 6E18F954 00808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    K = HMAC(K, V || 0x00 || provided_data) is
                F5044986 F825EB14 7DB35FE8 0666DB09 A7773C4C


    V = HMAC(K, V) is
                9C4D0729 7D6631D9 504721BD 21C8A102 C632306C


    ------------

    V || 0x01 || provided_data is
                                                        9C4D0729
        7D6631D9 504721BD 21C8A102 C632306C 01808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

```
    K = HMAC(K, V || 0x01 || provided_data) is
                 B9254D8A ACBA43FB DAE6394F 2B3AFC5D 580800BF


    V = HMAC(K, V) is
                 28403B60 3638D07D 7966661E F67B9D39 05F46DB9


  Update (Key, V):

    Key is
                 B9254D8A ACBA43FB DAE6394F 2B3AFC5D 580800BF


    V is
                 28403B60 3638D07D 7966661E F67B9D39 05F46DB9


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                 6C37FDD7 29AA40F8 0BC6AB08 CA7CC649 794F6998


    temp is
                 6C37FDD7 29AA40F8 0BC6AB08 CA7CC649 794F6998


  ------------

    V = HMAC(K, V) is
                 B57081E4 220F22C5 C283E2C9 1B8E305A B869C625


    temp is
                         6C37FDD7 29AA40F8 0BC6AB08 CA7CC649
```

```
        794F6998 B57081E4 220F22C5 C283E2C9 1B8E305A B869C625


---------------------------

  returned_bits is
                          6C37FDD7 29AA40F8 0BC6AB08 CA7CC649
        794F6998 B57081E4 220F22C5 C283E2C9 1B8E305A B869C625


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
              B5 7081E422 0F22C5C2 83E2C91B 8E305AB8 69C62500


    K = HMAC(K, V || 0x00 || provided_data) is
                64FE074A 6E7797D1 A435DA89 64484D6C F8BDC01B


    V = HMAC(K, V) is
                43E0C052 1586E947 3B060D87 D08A2325 FAE149D1


rnd_val is
                          6C37FDD7 29AA40F8 0BC6AB08 CA7CC649
        794F6998 B57081E4 220F22C5 C283E2C9 1B8E305A B869C625


------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320
```

```
    additional_input is  <empty>

Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is  <empty>

  Seed_Material is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  Key is
                64FE074A 6E7797D1 A435DA89 64484D6C F8BDC01B


  V is
                43E0C052 1586E947 3B060D87 D08A2325 FAE149D1


---------------------------

  Update

    provided_data
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    ------------

    V || 0x00 || provided_data is
                                                        43E0C052
        1586E947 3B060D87 D08A2325 FAE149D1 00C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
```

```
    K = HMAC(K, V || 0x00 || provided_data) is
                C25BF4F6 DF4271AC 796CC694 F61D7EEF 0BA4B13F


    V = HMAC(K, V) is
                E1A4863E 97118850 8DD8413B 07610B55 EFCFE0C2


    ------------

    V || 0x01 || provided_data is
                                                        E1A4863E
        97118850 8DD8413B 07610B55 EFCFE0C2 01C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    K = HMAC(K, V || 0x01 || provided_data) is
                02BC577F D10EF719 3C1DB098 BD5B75C7 C4B67959


    V = HMAC(K, V) is
                BCBDF052 E0E02AE8 9A776794 3F9865B8 B722902D


  Update (Key, V):

    Key is
                02BC577F D10EF719 3C1DB098 BD5B75C7 C4B67959


    V is
                BCBDF052 E0E02AE8 9A776794 3F9865B8 B722902D

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------
```

```
    V = HMAC(K, V) is
                 CAF57DCF EA393B92 36BF691F A456FEA7 FDF1DF83


    temp is
                 CAF57DCF EA393B92 36BF691F A456FEA7 FDF1DF83


  ------------

    V = HMAC(K, V) is
                 61482CA5 4D5FA723 F4C88B4F A504BF03 277FA783


    temp is
                           CAF57DCF EA393B92 36BF691F A456FEA7
        FDF1DF83 61482CA5 4D5FA723 F4C88B4F A504BF03 277FA783


---------------------------

  returned_bits is
                           CAF57DCF EA393B92 36BF691F A456FEA7
        FDF1DF83 61482CA5 4D5FA723 F4C88B4F A504BF03 277FA783


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
              61 482CA54D 5FA723F4 C88B4FA5 04BF0327 7FA78300


    K = HMAC(K, V || 0x00 || provided_data) is
                 1AA4241C 695E29C0 A59AD18A 6070E338 A548BE92


    V = HMAC(K, V) is
                 0347359B C9C7F88C C8330D4F 59FBC770 B0B77B03
```

```
rnd_val is
                          CAF57DCF EA393B92 36BF691F A456FEA7
        FDF1DF83 61482CA5 4D5FA723 F4C88B4F A504BF03 277FA783


################################################################

HMAC_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                 C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                     20 21222324


    PersonalizationString =
                                                 404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                 606162 63646566
```

6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596

AdditionalInput2 =
A0A1A2 A3A4A5A6
A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6

##

****

HMAC_DRBG_Instantiate_algorithm

entropy_input is
000102 03040506
0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536

nonce is
20 21222324

personal_str is
404142 43444546
4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576

prediction_resistance_flag = "PredictionResistance"

Seed_Material is
000102 03040506 0708090A 0B0C0D0E 0F101112
13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576

Key is
00000000 00000000 00000000 00000000 00000000

```
  V is
                01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                  000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    ------------

    V || 0x00 || provided_data is
                           01010101 01010101 01010101 01010101
        01010101 00000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x00 || provided_data) is
                3F7A620C 6BED0A29 2CB8E7D7 6DCEA617 67E060D5


    V = HMAC(K, V) is
                5848B848 182B6499 F6348807 E3CFE186 EE05FE25


    ------------

    V || 0x01 || provided_data is
                           5848B848 182B6499 F6348807 E3CFE186
        EE05FE25 01000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576
```

```
    K = HMAC(K, V || 0x01 || provided_data) is
                 B7D966D7 0D4E27A7 FA838F7D 61126C0E DC84761C


    V = HMAC(K, V) is
                 DAB2A718 83F1005C 5DD03932 4D3C364D 6E18F954


  Update (Key, V):

    Key is
                 B7D966D7 0D4E27A7 FA838F7D 61126C0E DC84761C


    V is
                 DAB2A718 83F1005C 5DD03932 4D3C364D 6E18F954


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is
                                              606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                              808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    additional_input is
```

```
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Seed_Material is
                               8081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Key is
                B7D966D7 0D4E27A7 FA838F7D 61126C0E DC84761C


  V is
                DAB2A718 83F1005C 5DD03932 4D3C364D 6E18F954


--------------------------

  Update

    provided_data
                               8081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                                     DAB2A7 1883F100 5C5DD039
        324D3C36 4D6E18F9 54008081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                B02FB0AE F02B9D35 01597640 32641425 F7AB0780
```

```
    V = HMAC(K, V) is
                0D23D81F 8626C01D FA230E23 B6AD0A2C CAEA3180


    ------------

    V || 0x01 || provided_data is
                                      0D23D8 1F8626C0 1DFA230E
        23B6AD0A 2CCAEA31 80018081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
                C09548C0 D3C861D7 40F2837D 72B50723 5C26DB82


    V = HMAC(K, V) is
                174B3F84 C3531F7C 0A2E5421 234EA16B 708DDF0D


  Update (Key, V):

    Key is
                C09548C0 D3C861D7 40F2837D 72B50723 5C26DB82


    V is
                174B3F84 C3531F7C 0A2E5421 234EA16B 708DDF0D


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
```

```
                BD07C25C FD7C5E3A 4EAA6E2E DC5AB7EA 4942A091


    temp is
                BD07C25C FD7C5E3A 4EAA6E2E DC5AB7EA 4942A091


  ------------

    V = HMAC(K, V) is
                3471FDA5 5C6DDD2C 03EFA3B9 643AB3BB 22F6C9F2


    temp is
                           BD07C25C FD7C5E3A 4EAA6E2E DC5AB7EA
        4942A091 3471FDA5 5C6DDD2C 03EFA3B9 643AB3BB 22F6C9F2


---------------------------

  returned_bits is
                           BD07C25C FD7C5E3A 4EAA6E2E DC5AB7EA
        4942A091 3471FDA5 5C6DDD2C 03EFA3B9 643AB3BB 22F6C9F2


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
              34 71FDA55C 6DDD2C03 EFA3B964 3AB3BB22 F6C9F200


    K = HMAC(K, V || 0x00 || provided_data) is
                603F0949 279C70E8 C66C0F56 37C0F375 6007E5AC


    V = HMAC(K, V) is
                F2B33B21 151FAF61 20018310 F44E4CD0 BFE368EA
```

```
rnd_val is
                          BD07C25C FD7C5E3A 4EAA6E2E DC5AB7EA
        4942A091 3471FDA5 5C6DDD2C 03EFA3B9 643AB3BB 22F6C9F2


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
***************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                 C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Seed_Material is
                             C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
```

Key is
603F0949 279C70E8 C66C0F56 37C0F375 6007E5AC

V is
F2B33B21 151FAF61 20018310 F44E4CD0 BFE368EA

Update

provided_data
C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6

V || 0x00 || provided_data is
F2B33B 21151FAF 61200183
10F44E4C D0BFE368 EA00C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6

K = HMAC(K, V || 0x00 || provided_data) is
66638E61 B8F0D692 C5D300BA 7D0237DD CE94F587

V = HMAC(K, V) is
80EFA2CF 6DB37996 B4147204 724649BF CB0C6C79

V || 0x01 || provided_data is
80EFA2 CF6DB379 96B41472
04724649 BFCB0C6C 7901C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6

```
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
                 8942A54F 349E281B 84AA4695 87FBDDAF 9D114082


    V = HMAC(K, V) is
                 07730E3C BFFD3CAF D7A8AAE2 BF01D601 4301E24D


  Update (Key, V):

    Key is
                 8942A54F 349E281B 84AA4695 87FBDDAF 9D114082


    V is
                 07730E3C BFFD3CAF D7A8AAE2 BF01D601 4301E24D

**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                 D1A9C1A2 2C84FC23 FF2227EF 98EC8BA9 DF2A209B


    temp is
                 D1A9C1A2 2C84FC23 FF2227EF 98EC8BA9 DF2A209B


  ------------

    V = HMAC(K, V) is
                 A1DB0980 9F57BFEA E5B3E5F1 46C75F2D 8DBB5E4A
```

```
    temp is
                           D1A9C1A2 2C84FC23 FF2227EF 98EC8BA9
         DF2A209B A1DB0980 9F57BFEA E5B3E5F1 46C75F2D 8DBB5E4A


---------------------------

  returned_bits is
                           D1A9C1A2 2C84FC23 FF2227EF 98EC8BA9
         DF2A209B A1DB0980 9F57BFEA E5B3E5F1 46C75F2D 8DBB5E4A


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
              A1 DB09809F 57BFEAE5 B3E5F146 C75F2D8D BB5E4A00


    K = HMAC(K, V || 0x00 || provided_data) is
                 BDE1B46C DC5413B3 D9F735AC DB80B13C 57BFE473


    V = HMAC(K, V) is
                 725A3C78 20DE1A06 D095819C CF6F2C9B 3A67F2CE


rnd_val is
                           D1A9C1A2 2C84FC23 FF2227EF 98EC8BA9
         DF2A209B A1DB0980 9F57BFEA E5B3E5F1 46C75F2D 8DBB5E4A
```

```
################################################################

HMAC_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    nonce is
                                                202122 23242526


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                               0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


  Key is
                                                        00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                        01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                               0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    ------------

    V || 0x00 || provided_data is
                    010101 01010101 01010101 01010101 01010101
        01010101 01010101 01000001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        B1F7F90A
```

```
        6FFA27B5 34FB2454 58934840 532A856D 5FC3E322 5AD0C4EE


    V = HMAC(K, V) is
                                                        F679095D
        7D62ED32 D35CC35C F8209B48 BA2463EF E19F5416 4825ADB5


    ------------

    V || 0x01 || provided_data is
                   F67909 5D7D62ED 32D35CC3 5CF8209B 48BA2463
        EFE19F54 164825AD B5010001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    K = HMAC(K, V || 0x01 || provided_data) is
                                                        69E16A0D
        59DD6B13 0C941512 AFAE8492 C4ECFAA0 95B89282 5E814FF1


    V = HMAC(K, V) is
                                                        BE23F2F3
        66C83C79 D6A17791 99855104 4B6479EB 3C1F18E6 E3975E06


  Update (Key, V):

    Key is
                                                        69E16A0D
        59DD6B13 0C941512 AFAE8492 C4ECFAA0 95B89282 5E814FF1


    V is
                                                        BE23F2F3
        66C83C79 D6A17791 99855104 4B6479EB 3C1F18E6 E3975E06


----------------------------------------------------------------

First call to Generate

****************************************************************

HMAC_DRBG_Generate
```

```
  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                          2444F876
        2695FE82 C2CA72C9 C5834B94 8C9C334C C922A81A EABC53D9


    temp is
                                                          2444F876
        2695FE82 C2CA72C9 C5834B94 8C9C334C C922A81A EABC53D9


  ------------

    V = HMAC(K, V) is
                                                          4962FF27
        345EF1E3 E199DDE5 E586800E 40C4B369 8F84FFE1 580EA6A9


    temp is
                                                 2444F876 2695FE82
        C2CA72C9 C5834B94 8C9C334C C922A81A EABC53D9 4962FF27
        345EF1E3 E199DDE5 E586800E 40C4B369 8F84FFE1 580EA6A9


---------------------------

  returned_bits is
                                                 2444F876 2695FE82
        C2CA72C9 C5834B94 8C9C334C C922A81A EABC53D9 4962FF27
        345EF1E3 E199DDE5 E586800E 40C4B369 8F84FFE1 580EA6A9


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------
```

```
    V || 0x00 || provided_data is
                                                        49 62FF2734
        5EF1E3E1 99DDE5E5 86800E40 C4B3698F 84FFE158 0EA6A900


    K = HMAC(K, V || 0x00 || provided_data) is
                                                          CB3DFDD4
        13A75233 0768D47A 0F63EC98 E5A16D2D 8DA28CD6 ABC9BEE0


    V = HMAC(K, V) is
                                                          43F9FE36
        663484FF 28F83061 90496111 1D919505 0C6268CE 07F86D55


rnd_val is
                                              2444F876 2695FE82
        C2CA72C9 C5834B94 8C9C334C C922A81A EABC53D9 4962FF27
        345EF1E3 E199DDE5 E586800E 40C4B369 8F84FFE1 580EA6A9


----------------------------------------------------------------

Second call to Generate

****************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                          C2FD2E69
        DD13C1AB 0B9E4182 4109E257 22DC2248 3ADFE7C1 C556D924


    temp is
                                                          C2FD2E69
        DD13C1AB 0B9E4182 4109E257 22DC2248 3ADFE7C1 C556D924
```

```
  ------------

    V = HMAC(K, V) is
                                                          45EDDEB3
        C98DC11C 51F59F2A A00F9DC2 C22DC9BD 3050F06E B516B98D


    temp is
                                              C2FD2E69 DD13C1AB
        0B9E4182 4109E257 22DC2248 3ADFE7C1 C556D924 45EDDEB3
        C98DC11C 51F59F2A A00F9DC2 C22DC9BD 3050F06E B516B98D


---------------------------

  returned_bits is
                                              C2FD2E69 DD13C1AB
        0B9E4182 4109E257 22DC2248 3ADFE7C1 C556D924 45EDDEB3
        C98DC11C 51F59F2A A00F9DC2 C22DC9BD 3050F06E B516B98D


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                       45 EDDEB3C9
        8DC11C51 F59F2AA0 0F9DC2C2 2DC9BD30 50F06EB5 16B98D00


    K = HMAC(K, V || 0x00 || provided_data) is
                                                          0D7D695F
        79040A7D B6A96BB9 CAB37A2D B22D43D6 E96FCDA2 581B6D4E


    V = HMAC(K, V) is
                                                          BDB549A1
        495B54BB 36F670C6 2DCD0699 903211BE 4A3506B9 5EE8F8C7


rnd_val is
```

```
                                                C2FD2E69 DD13C1AB
        0B9E4182 4109E257 22DC2248 3ADFE7C1 C556D924 45EDDEB3
        C98DC11C 51F59F2A A00F9DC2 C22DC9BD 3050F06E B516B98D


##############################################################

HMAC_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                  A0A1A2 A3A4A5A6
```

```
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                 202122 23242526


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                              0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


  Key is
                                                       00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                       01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                              0001 02030405 06070809 0A0B0C0D
```

```
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


  ------------

  V || 0x00 || provided_data is
                 010101 01010101 01010101 01010101 01010101
    01010101 01010101 01000001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


  K = HMAC(K, V || 0x00 || provided_data) is
                                                    B1F7F90A
    6FFA27B5 34FB2454 58934840 532A856D 5FC3E322 5AD0C4EE


  V = HMAC(K, V) is
                                                    F679095D
    7D62ED32 D35CC35C F8209B48 BA2463EF E19F5416 4825ADB5


  ------------

  V || 0x01 || provided_data is
                 F67909 5D7D62ED 32D35CC3 5CF8209B 48BA2463
    EFE19F54 164825AD B5010001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


  K = HMAC(K, V || 0x01 || provided_data) is
                                                    69E16A0D
    59DD6B13 0C941512 AFAE8492 C4ECFAA0 95B89282 5E814FF1


  V = HMAC(K, V) is
                                                    BE23F2F3
    66C83C79 D6A17791 99855104 4B6479EB 3C1F18E6 E3975E06


Update (Key, V):

  Key is
                                                    69E16A0D
```

```
        59DD6B13 0C941512 AFAE8492 C4ECFAA0 95B89282 5E814FF1


    V is
                                                          BE23F2F3
        66C83C79 D6A17791 99855104 4B6479EB 3C1F18E6 E3975E06


---------------------------------------------------------------

First call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                                   BE23F2F3 66C83C79 D6A17791
        99855104 4B6479EB 3C1F18E6 E3975E06 00606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                                                          C2B0B628
```

```
      4B609F8C F9C532F2 3A4FBC51 80B893E9 9377214A 14029FE4


  V = HMAC(K, V) is
                                                        B574BE90
      67E03706 A28C8AA4 B2C5E0C0 95434964 2439A2DD 5E8DB295


  ------------

  V || 0x01 || provided_data is
                                  B574BE90 67E03706 A28C8AA4
      B2C5E0C0 95434964 2439A2DD 5E8DB295 01606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  K = HMAC(K, V || 0x01 || provided_data) is
                                                        7FF56354
      5662FD74 EA9F2E45 9C5685A8 258DFEE3 5420638C 333617E0


  V = HMAC(K, V) is
                                                        EA32E139
      1A80FD6F 6CD28207 C229C386 E68499F3 9A1D432A B303BAC0


------------

  V = HMAC(K, V) is
                                                        F9CA2486
      FCBED54C F88DFAA8 B87959D7 0BD1048E CD01FA2E B4375028


  temp is
                                                        F9CA2486
      FCBED54C F88DFAA8 B87959D7 0BD1048E CD01FA2E B4375028


------------

  V = HMAC(K, V) is
                                                        8860ACC0
      1EF2DC2C 47D29FD9 9B353754 EA45EF0F 45074520 B4591045
```

```
    temp is
                                                F9CA2486 FCBED54C
        F88DFAA8 B87959D7 0BD1048E CD01FA2E B4375028 8860ACC0
        1EF2DC2C 47D29FD9 9B353754 EA45EF0F 45074520 B4591045


---------------------------

  returned_bits is
                                                F9CA2486 FCBED54C
        F88DFAA8 B87959D7 0BD1048E CD01FA2E B4375028 8860ACC0
        1EF2DC2C 47D29FD9 9B353754 EA45EF0F 45074520 B4591045


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                                    8860ACC0 1EF2DC2C 47D29FD9
        9B353754 EA45EF0F 45074520 B4591045 00606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                                                          279D1B68
        E24558AE 38BF95EC A2095AB3 32520665 0571DC01 D727770E


    V = HMAC(K, V) is
                                                          BBDADA2A
        0BAFC0AB 43FF2F3E F8323A11 1C06AA01 CB4AE54C 6522409D


    ------------
```

```
    V || 0x01 || provided_data is
                                    BBDADA2A 0BAFC0AB 43FF2F3E
        F8323A11 1C06AA01 CB4AE54C 6522409D 01606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
                                                        8F137BBC
        45EB987E 7610C142 7E0A42CC 9DE74BAC F04B8E7B AB144EC0


    V = HMAC(K, V) is
                                                        CC72D1CB
        867CBE33 96B27783 6C3DA456 6D01E5C3 F9B37262 1C3C4094


rnd_val is
                                               F9CA2486 FCBED54C
        F88DFAA8 B87959D7 0BD1048E CD01FA2E B4375028 8860ACC0
        1EF2DC2C 47D29FD9 9B353754 EA45EF0F 45074520 B4591045


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                 A0A1A2 A3A4A5A6
```

```
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  ------------

  V || 0x00 || provided_data is
                                CC72D1CB 867CBE33 96B27783
    6C3DA456 6D01E5C3 F9B37262 1C3C4094 00A0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  K = HMAC(K, V || 0x00 || provided_data) is
                                                    BADF9387
    FF7212EE DAE531DD F1D69F9E 2938BB4D 837DF2AD 07E3F89B


  V = HMAC(K, V) is
                                                    36FB6EAE
    622876D7 DE3E66B1 D3295F5E 373419CF 11FF31C6 568E00B5


  ------------

  V || 0x01 || provided_data is
                                36FB6EAE 622876D7 DE3E66B1
    D3295F5E 373419CF 11FF31C6 568E00B5 01A0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  K = HMAC(K, V || 0x01 || provided_data) is
                                                    83EF49A7
    A1758EAE 37E40BE9 F7A87929 C2702BC2 AB7244DD 527B86AC


  V = HMAC(K, V) is
                                                    C2E02384
    8D14026B 8CC97914 E9E9DA72 298F6334 AA012B34 9A8D4792


------------

  V = HMAC(K, V) is
                                                    96D23972
```

```
        60FA9F7D 085F9CDC B3EBAA39 A0B2E4B4 8C5858B9 88357FE6


    temp is
                                                        96D23972
        60FA9F7D 085F9CDC B3EBAA39 A0B2E4B4 8C5858B9 88357FE6


  ------------

    V = HMAC(K, V) is
                                                        32985C91
        FC3A8A58 3441856D 0C1B1059 C7153B91 1DE34048 425E3A42


    temp is
                                                96D23972 60FA9F7D
        085F9CDC B3EBAA39 A0B2E4B4 8C5858B9 88357FE6 32985C91
        FC3A8A58 3441856D 0C1B1059 C7153B91 1DE34048 425E3A42


--------------------------

  returned_bits is
                                                96D23972 60FA9F7D
        085F9CDC B3EBAA39 A0B2E4B4 8C5858B9 88357FE6 32985C91
        FC3A8A58 3441856D 0C1B1059 C7153B91 1DE34048 425E3A42


  call Update(additional_input, K, V)
--------------------------

  Update

    provided_data
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                                    32985C91 FC3A8A58 3441856D
        0C1B1059 C7153B91 1DE34048 425E3A42 00A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
```

```
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        47D94E6B
        04AFC62D 1F5C2D66 C423787F 3117AAFE BE0A1DDE 420377DC


    V = HMAC(K, V) is
                                                        ECAF7807
        CD949FD7 30B12F60 927CCFA1 F3EBE260 DE99E007 E49FEF48


    ------------

    V || 0x01 || provided_data is
                                    ECAF7807 CD949FD7 30B12F60
        927CCFA1 F3EBE260 DE99E007 E49FEF48 01A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
                                                        BC8C708C
        E66DA5EC D09AD5C5 75A56079 EF34217A FBC4CD18 697C739A


    V = HMAC(K, V) is
                                                        D8B3E4BE
        638D71E2 D7B691E8 81680E60 69B3E4D9 9FCA0557 6D0203F7


rnd_val is
                                               96D23972 60FA9F7D
        085F9CDC B3EBAA39 A0B2E4B4 8C5858B9 88357FE6 32985C91
        FC3A8A58 3441856D 0C1B1059 C7153B91 1DE34048 425E3A42


################################################################

HMAC_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224
```

```
    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString =
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                  202122 23242526
```

```
    personal_str is
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                                                        00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                        01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    ------------

    V || 0x00 || provided_data is
                                                          0101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010000 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
```

```
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        B45032CF
        6A06E937 50DBD791 1C1F7701 11FA85E4 522863CA 4B8B66E7


    V = HMAC(K, V) is
                                                        A00F5F20
        C0D5BC5D CCDFDEC7 8839E0D5 376D22CC A1ABEB9A 2FC53CAC


    ------------

    V || 0x01 || provided_data is
                                                            A00F
        5F20C0D5 BC5DCCDF DEC78839 E0D5376D 22CCA1AB EB9A2FC5
        3CAC0100 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x01 || provided_data) is
                                                        4F7FCBA2
        3A6D7557 A0D657F7 57E3EBA4 6093D3BD F5D86BCF D941B53A


    V = HMAC(K, V) is
                                                        D0DE6F99
        D9E7DF8C 07E9F4D7 5E05B73E FDE0834B 2E19CC1F DC0FC853


Update (Key, V):

    Key is
                                                        4F7FCBA2
        3A6D7557 A0D657F7 57E3EBA4 6093D3BD F5D86BCF D941B53A


    V is
                                                        D0DE6F99
```

```
        D9E7DF8C 07E9F4D7 5E05B73E FDE0834B 2E19CC1F DC0FC853


--------------------------------------------------------------

First call to Generate

**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                        CC52B803
        A2BE29C1 3669C492 60C80FAB A2C8079E 12D929B0 19A229A2


    temp is
                                                        CC52B803
        A2BE29C1 3669C492 60C80FAB A2C8079E 12D929B0 19A229A2


  ------------

    V = HMAC(K, V) is
                                                        3EBC03FA
        0962232F 6D92E3E4 432DCD20 B62A1F3B AC98B7C2 5A85A1C9


    temp is
                                               CC52B803 A2BE29C1
        3669C492 60C80FAB A2C8079E 12D929B0 19A229A2 3EBC03FA
        0962232F 6D92E3E4 432DCD20 B62A1F3B AC98B7C2 5A85A1C9


---------------------------

  returned_bits is
                                               CC52B803 A2BE29C1
        3669C492 60C80FAB A2C8079E 12D929B0 19A229A2 3EBC03FA
        0962232F 6D92E3E4 432DCD20 B62A1F3B AC98B7C2 5A85A1C9
```

```
  call Update(additional_input, K, V)
--------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                        3E BC03FA09
        62232F6D 92E3E443 2DCD20B6 2A1F3BAC 98B7C25A 85A1C900


    K = HMAC(K, V || 0x00 || provided_data) is
                                                       BE844670
        9C81C7A0 818B6639 84595EC1 EDCCA3F7 C6205C42 2A32061F


    V = HMAC(K, V) is
                                                       F6A634C4
        8CA0EA19 687D5438 656915AF CF76AC73 B3386CBC BD093016


rnd_val is
                                               CC52B803 A2BE29C1
        3669C492 60C80FAB A2C8079E 12D929B0 19A229A2 3EBC03FA
        0962232F 6D92E3E4 432DCD20 B62A1F3B AC98B7C2 5A85A1C9


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------
```

```
    V = HMAC(K, V) is
                                                          1A6131F5
        FBE23C94 750185A4 F496EFB4 108F5125 CEBDCF02 746B32FD


    temp is
                                                          1A6131F5
        FBE23C94 750185A4 F496EFB4 108F5125 CEBDCF02 746B32FD


  ------------

    V = HMAC(K, V) is
                                                          952AEC16
        BD2538AB E16C2C99 245C8B3C 3A2E77CC 8BC86FAC 26CE278F


    temp is
                                                 1A6131F5 FBE23C94
        750185A4 F496EFB4 108F5125 CEBDCF02 746B32FD 952AEC16
        BD2538AB E16C2C99 245C8B3C 3A2E77CC 8BC86FAC 26CE278F


---------------------------

  returned_bits is
                                                 1A6131F5 FBE23C94
        750185A4 F496EFB4 108F5125 CEBDCF02 746B32FD 952AEC16
        BD2538AB E16C2C99 245C8B3C 3A2E77CC 8BC86FAC 26CE278F


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                       95 2AEC16BD
        2538ABE1 6C2C9924 5C8B3C3A 2E77CC8B C86FAC26 CE278F00


    K = HMAC(K, V || 0x00 || provided_data) is
```

                                                    2E7B1838
        458F0B0B 989DD5C1 6E4CAC18 25A5D73B 6B957C70 6F3B9941

    V = HMAC(K, V) is
                                                    81046D3D
        D2F3DFA4 5BD97475 49EB1880 7CA55CE0 1F3FEB35 837C2530

rnd_val is
                                            1A6131F5 FBE23C94
        750185A4 F496EFB4 108F5125 CEBDCF02 746B32FD 952AEC16
        BD2538AB E16C2C99 245C8B3C 3A2E77CC 8BC86FAC 26CE278F

##

HMAC_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                              000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536

    EntropyInput1 (for Reseed1) =
                                              808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6

    EntropyInput2 (for Reseed2) =
                                              C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6

    Nonce =
                                              202122 23242526

```
    PersonalizationString =
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                202122 23242526


    personal_str is
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
```

```
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                                                          00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                          01010101
        01010101 01010101 01010101 01010101 01010101 01010101


----------------------------

  Update

    provided_data
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    ------------

    V || 0x00 || provided_data is
                                                            0101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010000 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x00 || provided_data) is
                                                          B45032CF
        6A06E937 50DBD791 1C1F7701 11FA85E4 522863CA 4B8B66E7


    V = HMAC(K, V) is
                                                          A00F5F20
        C0D5BC5D CCDFDEC7 8839E0D5 376D22CC A1ABEB9A 2FC53CAC
```

```
    ------------

    V || 0x01 || provided_data is
                                                              A00F
        5F20C0D5 BC5DCCDF DEC78839 E0D5376D 22CCA1AB EB9A2FC5
        3CAC0100 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x01 || provided_data) is
                                                          4F7FCBA2
        3A6D7557 A0D657F7 57E3EBA4 6093D3BD F5D86BCF D941B53A


    V = HMAC(K, V) is
                                                          D0DE6F99
        D9E7DF8C 07E9F4D7 5E05B73E FDE0834B 2E19CC1F DC0FC853


  Update (Key, V):

    Key is
                                                          4F7FCBA2
        3A6D7557 A0D657F7 57E3EBA4 6093D3BD F5D86BCF D941B53A


    V is
                                                          D0DE6F99
        D9E7DF8C 07E9F4D7 5E05B73E FDE0834B 2E19CC1F DC0FC853


-----------------------------------------------------------

First call to Generate

***********************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448
```

```
    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                                  D0DE6F99 D9E7DF8C 07E9F4D7
        5E05B73E FDE0834B 2E19CC1F DC0FC853 00606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        DBA3E0DA
        7D398C32 BA5CB4CE FEC678BC 42C2E23F 51458216 227EDD6E


    V = HMAC(K, V) is
                                                        D20CD00C
        4C59B384 24D4421A 4294D0CC 4946A992 42B842B8 467D7C74


    ------------

    V || 0x01 || provided_data is
                                  D20CD00C 4C59B384 24D4421A
        4294D0CC 4946A992 42B842B8 467D7C74 01606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
```

```
                                                        36EAE5C0
        D729D9D4 37311A3D 9E412E01 E3B10E2C E727C770 2DCFD9ED


    V = HMAC(K, V) is
                                                        D1CFC04F
        A80E88F6 849054F3 20CB84E5 DB77F3B7 EBBE820A F16F006A


  ------------

    V = HMAC(K, V) is
                                                        499A959D
        E618773D F17A5372 074DA0AA 7A7B121C D31DA444 F65F9782


    temp is
                                                        499A959D
        E618773D F17A5372 074DA0AA 7A7B121C D31DA444 F65F9782


  ------------

    V = HMAC(K, V) is
                                                        801EAFE1
        ED3A3D40 06C3A321 C5FA1261 CA596C75 E25CBC26 23189FC4


    temp is
                                            499A959D E618773D
        F17A5372 074DA0AA 7A7B121C D31DA444 F65F9782 801EAFE1
        ED3A3D40 06C3A321 C5FA1261 CA596C75 E25CBC26 23189FC4


---------------------------

  returned_bits is
                                            499A959D E618773D
        F17A5372 074DA0AA 7A7B121C D31DA444 F65F9782 801EAFE1
        ED3A3D40 06C3A321 C5FA1261 CA596C75 E25CBC26 23189FC4


  call Update(additional_input, K, V)
---------------------------

  Update
```

```
    provided_data
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                                   801EAFE1 ED3A3D40 06C3A321
        C5FA1261 CA596C75 E25CBC26 23189FC4 00606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        3CCE29FF
        4BB898B5 F67EFC0B 1D967D19 8D39C0C8 E7B4AB49 2C5B17D9


    V = HMAC(K, V) is
                                                        3E97F0F4
        27AF7B10 F40CC786 0E9A5E04 1B1CC7EB D670E8A9 55BCFEC8


    ------------

    V || 0x01 || provided_data is
                                   3E97F0F4 27AF7B10 F40CC786
        0E9A5E04 1B1CC7EB D670E8A9 55BCFEC8 01606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
                                                        F433D100
        3FBFAB7B 3708531F 206D93EB 0A4F9FD8 43F3BF00 9D9815A1


    V = HMAC(K, V) is
                                                        2F61B62E
        88FDA431 B829880A DC472F8B 44BAA571 D27878F0 36D72ED2


rnd_val is
```

```
                                                499A959D E618773D
        F17A5372 074DA0AA 7A7B121C D31DA444 F65F9782 801EAFE1
        ED3A3D40 06C3A321 C5FA1261 CA596C75 E25CBC26 23189FC4


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                                  2F61B62E 88FDA431 B829880A
        DC472F8B 44BAA571 D27878F0 36D72ED2 00A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        5F2F354C
        E2992DAF E9FF8612 013C50B3 A38F5AED E8B88F87 84EAD08C
```

```
  V = HMAC(K, V) is
                                                      8C5574C7
      9376296E E2463C2B CB39BB3D 85F80542 BE686350 2C0AC1F8


  ------------

  V || 0x01 || provided_data is
                                  8C5574C7 9376296E E2463C2B
      CB39BB3D 85F80542 BE686350 2C0AC1F8 01A0A1A2 A3A4A5A6
      A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
      BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  K = HMAC(K, V || 0x01 || provided_data) is
                                                      3D854845
      99F8D48D A11C61F6 E954A100 DA4149D9 DCA75625 911A42A5


  V = HMAC(K, V) is
                                                      15536D25
      35361578 6B563F02 64CFF800 00D75389 4C5A23AE 34403B13


------------

  V = HMAC(K, V) is
                                                      0AD161E1
      9C70E4F5 29A31D94 D4913162 9A24E77B 5545AE91 F23A7D1C


  temp is
                                                      0AD161E1
      9C70E4F5 29A31D94 D4913162 9A24E77B 5545AE91 F23A7D1C


------------

  V = HMAC(K, V) is
                                                      6FFB0C00
      19640D0F 75B62D31 431557E9 A87A6714 0F9C1BA3 917A510C


  temp is
                                              0AD161E1 9C70E4F5
      29A31D94 D4913162 9A24E77B 5545AE91 F23A7D1C 6FFB0C00
```

```
        19640D0F 75B62D31 431557E9 A87A6714 0F9C1BA3 917A510C


--------------------------

  returned_bits is
                                                0AD161E1 9C70E4F5
        29A31D94 D4913162 9A24E77B 5545AE91 F23A7D1C 6FFB0C00
        19640D0F 75B62D31 431557E9 A87A6714 0F9C1BA3 917A510C


  call Update(additional_input, K, V)
--------------------------

  Update

    provided_data
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                                    6FFB0C00 19640D0F 75B62D31
        431557E9 A87A6714 0F9C1BA3 917A510C 00A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        E7CB8EB0
        7E6A6CA3 1F44AB18 B09D9772 C8D0C54E 1909B375 BA3FE64F


    V = HMAC(K, V) is
                                                        C5CDA955
        5D4E8307 1F0DDC95 9D996CB1 88DCF23A 41953C90 28196F9E


    ------------

    V || 0x01 || provided_data is
                                    C5CDA955 5D4E8307 1F0DDC95
        9D996CB1 88DCF23A 41953C90 28196F9E 01A0A1A2 A3A4A5A6
```

```
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
                                                        BFB6AFF8
        B2F1096D 92E05777 68B85EB7 32037CC1 B8775A71 3A0CE3BA


    V = HMAC(K, V) is
                                                        71BA6980
        76B9E948 8636D427 7A382EA7 D6774CE2 BE10F390 DA3F92D6


rnd_val is
                                              0AD161E1 9C70E4F5
        29A31D94 D4913162 9A24E77B 5545AE91 F23A7D1C 6FFB0C00
        19640D0F 75B62D31 431557E9 A87A6714 0F9C1BA3 917A510C


##############################################################

HMAC_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
```

```
    Nonce =
                                                202122 23242526


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                202122 23242526


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                              0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


  Key is
                                                        00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                        01010101
        01010101 01010101 01010101 01010101 01010101 01010101


--------------------------
```

Update

provided_data
                          0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526

V || 0x00 || provided_data is
              010101 01010101 01010101 01010101 01010101
    01010101 01010101 01000001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526

K = HMAC(K, V || 0x00 || provided_data) is
                                                    B1F7F90A
    6FFA27B5 34FB2454 58934840 532A856D 5FC3E322 5AD0C4EE

V = HMAC(K, V) is
                                                    F679095D
    7D62ED32 D35CC35C F8209B48 BA2463EF E19F5416 4825ADB5

V || 0x01 || provided_data is
                F67909 5D7D62ED 32D35CC3 5CF8209B 48BA2463
    EFE19F54 164825AD B5010001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526

K = HMAC(K, V || 0x01 || provided_data) is
                                                    69E16A0D
    59DD6B13 0C941512 AFAE8492 C4ECFAA0 95B89282 5E814FF1

V = HMAC(K, V) is
                                                    BE23F2F3
    66C83C79 D6A17791 99855104 4B6479EB 3C1F18E6 E3975E06

```
  Update (Key, V):

    Key is
                                                        69E16A0D
        59DD6B13 0C941512 AFAE8492 C4ECFAA0 95B89282 5E814FF1


    V is
                                                        BE23F2F3
        66C83C79 D6A17791 99855104 4B6479EB 3C1F18E6 E3975E06


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    additional_input is  <empty>

  Seed_Material is
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  Key is
                                                        69E16A0D
```

```
        59DD6B13 0C941512 AFAE8492 C4ECFAA0 95B89282 5E814FF1


  V is
                                                          BE23F2F3
        66C83C79 D6A17791 99855104 4B6479EB 3C1F18E6 E3975E06


---------------------------

  Update

    provided_data
                                                   808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    ------------

    V || 0x00 || provided_data is
                                  BE23F2F3 66C83C79 D6A17791
        99855104 4B6479EB 3C1F18E6 E3975E06 00808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                          2216735C
        C98E7189 2680E0C4 13B68700 5752DBFF E5AEA7A0 BCFA0244


    V = HMAC(K, V) is
                                                          3776E0E0
        CFF312C1 5551DC10 FA8B40E3 226C9C02 48544531 020DC532


    ------------

    V || 0x01 || provided_data is
                                  3776E0E0 CFF312C1 5551DC10
        FA8B40E3 226C9C02 48544531 020DC532 01808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

```
    K = HMAC(K, V || 0x01 || provided_data) is
                                                          95603C76
        4BC3CB23 7C2FC6B0 651F858F 2DB9378A B26ADB6E 2632437C


    V = HMAC(K, V) is
                                                          7DC1DD01
        33C30D6B 4862D627 09514D76 DD15699C 598C173B BB7F8129


  Update (Key, V):

    Key is
                                                          95603C76
        4BC3CB23 7C2FC6B0 651F858F 2DB9378A B26ADB6E 2632437C


    V is
                                                          7DC1DD01
        33C30D6B 4862D627 09514D76 DD15699C 598C173B BB7F8129


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                          A07AA4CC
        1716E214 96DB43E3 05B00400 578D3227 E224ED5F 08D881B7


    temp is
                                                          A07AA4CC
        1716E214 96DB43E3 05B00400 578D3227 E224ED5F 08D881B7


  ------------

    V = HMAC(K, V) is
                                                          04CA6EFF
```

```
        3E9CA847 C90660DF 36517813 AC13913B AC1E822B 5883281A


    temp is
                                                A07AA4CC 1716E214
        96DB43E3 05B00400 578D3227 E224ED5F 08D881B7 04CA6EFF
        3E9CA847 C90660DF 36517813 AC13913B AC1E822B 5883281A


---------------------------

  returned_bits is
                                                A07AA4CC 1716E214
        96DB43E3 05B00400 578D3227 E224ED5F 08D881B7 04CA6EFF
        3E9CA847 C90660DF 36517813 AC13913B AC1E822B 5883281A


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                      04 CA6EFF3E
        9CA847C9 0660DF36 517813AC 13913BAC 1E822B58 83281A00


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        707AB325
        EC6269F7 8B43B0CB B6D18E20 B78944EF 3028763E 3C9D6486


    V = HMAC(K, V) is
                                                        0494DEDA
        33EE314C 09879164 4E23201A 8AC6D0CB 6085548C B89260B8


rnd_val is
                                                A07AA4CC 1716E214
        96DB43E3 05B00400 578D3227 E224ED5F 08D881B7 04CA6EFF
        3E9CA847 C90660DF 36517813 AC13913B AC1E822B 5883281A
```

```
------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is  <empty>

  Seed_Material is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  Key is
                                                        707AB325
        EC6269F7 8B43B0CB B6D18E20 B78944EF 3028763E 3C9D6486


  V is
                                                        0494DEDA
        33EE314C 09879164 4E23201A 8AC6D0CB 6085548C B89260B8


---------------------------

  Update
```

```
  provided_data
                                                  C0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  ------------

  V || 0x00 || provided_data is
                                0494DEDA 33EE314C 09879164
      4E23201A 8AC6D0CB 6085548C B89260B8 00C0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  K = HMAC(K, V || 0x00 || provided_data) is
                                                        4EABCEE2
      A40FED76 141D2FF2 77F6B4C4 F16BF785 DC98CE03 8D8634C6


  V = HMAC(K, V) is
                                                        E0493CBD
      0E533288 16113396 BF703F25 B9AD4748 19E1D904 5D4540FA


  ------------

  V || 0x01 || provided_data is
                                E0493CBD 0E533288 16113396
      BF703F25 B9AD4748 19E1D904 5D4540FA 01C0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  K = HMAC(K, V || 0x01 || provided_data) is
                                                        61ED54C4
      6DE78330 A4E25662 8A1F8417 70C049F7 F9DE7C39 040ADA10


  V = HMAC(K, V) is
                                                        D0758ED6
      5D5C2F3D BFA33CD2 408125FA 8AB1C03F 0A4DB8C7 3D607F53


Update (Key, V):
```

```
    Key is
                                                        61ED54C4
        6DE78330 A4E25662 8A1F8417 70C049F7 F9DE7C39 040ADA10


    V is
                                                        D0758ED6
        5D5C2F3D BFA33CD2 408125FA 8AB1C03F 0A4DB8C7 3D607F53


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                        1FCC850D
        8F3E8B56 98D03900 F3D6BE3F 3EAD1260 09BCE060 4D0B60DF


    temp is
                                                        1FCC850D
        8F3E8B56 98D03900 F3D6BE3F 3EAD1260 09BCE060 4D0B60DF


  ------------

    V = HMAC(K, V) is
                                                        CE17F743
        CE0913AB CAF36FC3 082F89D2 F8AD52A8 A0DF633F A3C108A7


    temp is
                                                1FCC850D 8F3E8B56
        98D03900 F3D6BE3F 3EAD1260 09BCE060 4D0B60DF CE17F743
        CE0913AB CAF36FC3 082F89D2 F8AD52A8 A0DF633F A3C108A7


---------------------------

  returned_bits is
```

```
                                                1FCC850D 8F3E8B56
        98D03900 F3D6BE3F 3EAD1260 09BCE060 4D0B60DF CE17F743
        CE0913AB CAF36FC3 082F89D2 F8AD52A8 A0DF633F A3C108A7


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                      CE 17F743CE
        0913ABCA F36FC308 2F89D2F8 AD52A8A0 DF633FA3 C108A700


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        B4838859
        F3630EFF 7568590A 01D2E40C 42EABF47 43C03872 682F5B64


    V = HMAC(K, V) is
                                                        074F3021
        F6A0D2FF 03FAEA1C 94F63BD1 8CB9F9E0 5058DDE6 7D81AE13


rnd_val is
                                                1FCC850D 8F3E8B56
        98D03900 F3D6BE3F 3EAD1260 09BCE060 4D0B60DF CE17F743
        CE0913AB CAF36FC3 082F89D2 F8AD52A8 A0DF633F A3C108A7


##############################################################

HMAC_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                  000102 03040506
```

```
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                202122 23242526


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    nonce is
                                                202122 23242526


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                               0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


  Key is
                                                        00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                        01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                               0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    ------------

    V || 0x00 || provided_data is
                    010101 01010101 01010101 01010101 01010101
        01010101 01010101 01000001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        B1F7F90A
        6FFA27B5 34FB2454 58934840 532A856D 5FC3E322 5AD0C4EE
```

```
    V = HMAC(K, V) is
                                                          F679095D
        7D62ED32 D35CC35C F8209B48 BA2463EF E19F5416 4825ADB5


    ------------

    V || 0x01 || provided_data is
                   F67909 5D7D62ED 32D35CC3 5CF8209B 48BA2463
        EFE19F54 164825AD B5010001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    K = HMAC(K, V || 0x01 || provided_data) is
                                                          69E16A0D
        59DD6B13 0C941512 AFAE8492 C4ECFAA0 95B89282 5E814FF1


    V = HMAC(K, V) is
                                                          BE23F2F3
        66C83C79 D6A17791 99855104 4B6479EB 3C1F18E6 E3975E06


  Update (Key, V):

    Key is
                                                          69E16A0D
        59DD6B13 0C941512 AFAE8492 C4ECFAA0 95B89282 5E814FF1


    V is
                                                          BE23F2F3
        66C83C79 D6A17791 99855104 4B6479EB 3C1F18E6 E3975E06


-----------------------------------------------------------------

First call to Generate

*****************************************************************

HMAC_DRBG_Generate
```

```
  requested_number_of_bits = 448

    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Seed_Material is
                             8081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Key is
                                                      69E16A0D
        59DD6B13 0C941512 AFAE8492 C4ECFAA0 95B89282 5E814FF1


  V is
                                                      BE23F2F3
        66C83C79 D6A17791 99855104 4B6479EB 3C1F18E6 E3975E06


---------------------------

  Update
```

```
provided_data
                          8081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


------------

V || 0x00 || provided_data is
               BE23F2 F366C83C 79D6A177 91998551 044B6479
    EB3C1F18 E6E3975E 06008081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


K = HMAC(K, V || 0x00 || provided_data) is
                                                    FA5BDF71
    2EB399A3 81F352A3 D22DFFD5 47F205D4 9C4D85C2 8433BE8D


V = HMAC(K, V) is
                                                    EAB91B1F
    72E91DCC 52F897BD 0725D58E 8761300A 8ADBF928 67325DFC


------------

V || 0x01 || provided_data is
               EAB91B 1F72E91D CC52F897 BD0725D5 8E876130
    0A8ADBF9 2867325D FC018081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


K = HMAC(K, V || 0x01 || provided_data) is
                                                    091ED0A7
    D134660B 75769A07 F26DAD14 5CB66631 C18A01FB BFB92C60
```

```
    V = HMAC(K, V) is
                                                        994C10C0
        F06B1287 0E8AEE05 D92245DB FCCB6067 21E3D98A 00B74C0C

  Update (Key, V):

    Key is
                                                        091ED0A7
        D134660B 75769A07 F26DAD14 5CB66631 C18A01FB BFB92C60

    V is
                                                        994C10C0
        F06B1287 0E8AEE05 D92245DB FCCB6067 21E3D98A 00B74C0C

**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                        E28DA53A
        461C412D 7E57C3A2 E4A93A82 13EFC9E7 A9BD99CD F8624A25

    temp is
                                                        E28DA53A
        461C412D 7E57C3A2 E4A93A82 13EFC9E7 A9BD99CD F8624A25

  ------------

    V = HMAC(K, V) is
                                                        1EE9B715
        33C5D916 05FA2C6B 14C50A75 2DF39B9B 0DE877B7 645A3D2F

    temp is
                                              E28DA53A 461C412D
```

```
        7E57C3A2 E4A93A82 13EFC9E7 A9BD99CD F8624A25 1EE9B715
        33C5D916 05FA2C6B 14C50A75 2DF39B9B 0DE877B7 645A3D2F


---------------------------

  returned_bits is
                                              E28DA53A 461C412D
        7E57C3A2 E4A93A82 13EFC9E7 A9BD99CD F8624A25 1EE9B715
        33C5D916 05FA2C6B 14C50A75 2DF39B9B 0DE877B7 645A3D2F


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                    1E E9B71533
        C5D91605 FA2C6B14 C50A752D F39B9B0D E877B764 5A3D2F00


    K = HMAC(K, V || 0x00 || provided_data) is
                                                      D3CE8637
        D87C38FB 1ABC374D E9CDDC6A A77892F2 FAD5D8A6 F008A917


    V = HMAC(K, V) is
                                                      45C6F054
        BBC02940 DE40A451 F276E995 CBC10660 AB1658B6 6B89B1C6


rnd_val is
                                              E28DA53A 461C412D
        7E57C3A2 E4A93A82 13EFC9E7 A9BD99CD F8624A25 1EE9B715
        33C5D916 05FA2C6B 14C50A75 2DF39B9B 0DE877B7 645A3D2F


-------------------------------------------------------------

Second call to Generate
```

```
************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Seed_Material is
                             C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Key is
                                                        D3CE8637
        D87C38FB 1ABC374D E9CDDC6A A77892F2 FAD5D8A6 F008A917


  V is
                                                        45C6F054
        BBC02940 DE40A451 F276E995 CBC10660 AB1658B6 6B89B1C6
```

```
---------------------------

  Update

    provided_data
                              C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                   45C6F0 54BBC029 40DE40A4 51F276E9 95CBC106
        60AB1658 B66B89B1 C600C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        7AA2ABB4
        10E64C6A 30A48CEC 96A95766 F0CB5574 709B6540 EB41ED8F


    V = HMAC(K, V) is
                                                        0C27DF08
        5E23EC39 6E5D6D06 EED6B0FE 2F9A24E8 7E52F526 B15E2633


    ------------

    V || 0x01 || provided_data is
                   0C27DF 085E23EC 396E5D6D 06EED6B0 FE2F9A24
        E87E52F5 26B15E26 3301C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
```

```
                                                        159FA328
        4A1E65D9 0AD889A0 9BAD44DA D0197935 E66C772E 68F2A468


    V = HMAC(K, V) is
                                                        FC104C95
        577F4259 7113809C 66AADAD8 998A788D E93B937F 70746973


  Update (Key, V):

    Key is
                                                        159FA328
        4A1E65D9 0AD889A0 9BAD44DA D0197935 E66C772E 68F2A468


    V is
                                                        FC104C95
        577F4259 7113809C 66AADAD8 998A788D E93B937F 70746973


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                        0A2E074D
        FF196BD8 2B8CC309 1A1C99C7 2220B0D2 154594EE 103398B8


    temp is
                                                        0A2E074D
        FF196BD8 2B8CC309 1A1C99C7 2220B0D2 154594EE 103398B8


  ------------

    V = HMAC(K, V) is
                                                        774050F6
        87EE6090 D0B415DD 1D3D9027 E9CB59AE 831EF109 C415BB4A
```

```
    temp is
                                                0A2E074D FF196BD8
        2B8CC309 1A1C99C7 2220B0D2 154594EE 103398B8 774050F6
        87EE6090 D0B415DD 1D3D9027 E9CB59AE 831EF109 C415BB4A


----------------------------

  returned_bits is
                                                0A2E074D FF196BD8
        2B8CC309 1A1C99C7 2220B0D2 154594EE 103398B8 774050F6
        87EE6090 D0B415DD 1D3D9027 E9CB59AE 831EF109 C415BB4A


  call Update(additional_input, K, V)
----------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                      77 4050F687
        EE6090D0 B415DD1D 3D9027E9 CB59AE83 1EF109C4 15BB4A00


    K = HMAC(K, V || 0x00 || provided_data) is
                                                         36767608
        2B1FCB6D 186B60A2 BE241915 AB140381 7E759FAD F64064AC


    V = HMAC(K, V) is
                                                         FCB677C9
        D39629C3 EE57FA1D 81938307 A2AFFC50 7713068A 6F8F7BB4


rnd_val is
                                                0A2E074D FF196BD8
        2B8CC309 1A1C99C7 2220B0D2 154594EE 103398B8 774050F6
        87EE6090 D0B415DD 1D3D9027 E9CB59AE 831EF109 C415BB4A
```

```
###############################################################

HMAC_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString =
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
```

```
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                  202122 23242526


    personal_str is
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                                                        00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                        01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576
```

```
  ------------

  V || 0x00 || provided_data is
                                                              0101
      01010101 01010101 01010101 01010101 01010101 01010101
      01010000 01020304 05060708 090A0B0C 0D0E0F10 11121314
      15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
      2D2E2F30 31323334 35362021 22232425 26404142 43444546
      4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
      5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  K = HMAC(K, V || 0x00 || provided_data) is
                                                            B45032CF
      6A06E937 50DBD791 1C1F7701 11FA85E4 522863CA 4B8B66E7


  V = HMAC(K, V) is
                                                            A00F5F20
      C0D5BC5D CCDFDEC7 8839E0D5 376D22CC A1ABEB9A 2FC53CAC


  ------------

  V || 0x01 || provided_data is
                                                              A00F
      5F20C0D5 BC5DCCDF DEC78839 E0D5376D 22CCA1AB EB9A2FC5
      3CAC0100 01020304 05060708 090A0B0C 0D0E0F10 11121314
      15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
      2D2E2F30 31323334 35362021 22232425 26404142 43444546
      4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
      5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  K = HMAC(K, V || 0x01 || provided_data) is
                                                            4F7FCBA2
      3A6D7557 A0D657F7 57E3EBA4 6093D3BD F5D86BCF D941B53A


  V = HMAC(K, V) is
                                                            D0DE6F99
      D9E7DF8C 07E9F4D7 5E05B73E FDE0834B 2E19CC1F DC0FC853


Update (Key, V):
```

```
    Key is
                                                          4F7FCBA2
        3A6D7557 A0D657F7 57E3EBA4 6093D3BD F5D86BCF D941B53A


    V is
                                                          D0DE6F99
        D9E7DF8C 07E9F4D7 5E05B73E FDE0834B 2E19CC1F DC0FC853


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                              808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    additional_input is  <empty>

  Seed_Material is
                                              808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  Key is
                                                          4F7FCBA2
        3A6D7557 A0D657F7 57E3EBA4 6093D3BD F5D86BCF D941B53A
```

```
  V is
                                                          D0DE6F99
       D9E7DF8C 07E9F4D7 5E05B73E FDE0834B 2E19CC1F DC0FC853


---------------------------

  Update

    provided_data
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    ------------

    V || 0x00 || provided_data is
                                  D0DE6F99 D9E7DF8C 07E9F4D7
        5E05B73E FDE0834B 2E19CC1F DC0FC853 00808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                          AC86F578
        BC8A381E D3D91289 BA72063E 7567F07D 8C7D2A0F 879FBD32


    V = HMAC(K, V) is
                                                          6AC3E086
        9913D864 5EA47BBD 8891ECC9 F41F7ED4 B129B9D3 E85995D6


    ------------

    V || 0x01 || provided_data is
                                  6AC3E086 9913D864 5EA47BBD
        8891ECC9 F41F7ED4 B129B9D3 E85995D6 01808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    K = HMAC(K, V || 0x01 || provided_data) is
                                                          5F540144
```

```
        2A22561B 2611D127 F6A18BEE FE11289D E4BF06A7 C9EA1E8F


    V = HMAC(K, V) is
                                                        1F7D5CBC
        DFFB3585 91ABDF03 42EBAF04 399A4D0B 3CB047FF 0179FA4D


  Update (Key, V):

    Key is
                                                        5F540144
        2A22561B 2611D127 F6A18BEE FE11289D E4BF06A7 C9EA1E8F


    V is
                                                        1F7D5CBC
        DFFB3585 91ABDF03 42EBAF04 399A4D0B 3CB047FF 0179FA4D


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                        ACD797A0
        7B378D0A D9A8FBE2 1683E7BB 8A3DF9CB 1346FF43 2EA75B47


    temp is
                                                        ACD797A0
        7B378D0A D9A8FBE2 1683E7BB 8A3DF9CB 1346FF43 2EA75B47


  ------------

    V = HMAC(K, V) is
                                                        66B7C754
        C4D06F4C 257537CC D9A399E5 986BBD30 085EEC86 01582911
```

```
    temp is
                                                ACD797A0 7B378D0A
        D9A8FBE2 1683E7BB 8A3DF9CB 1346FF43 2EA75B47 66B7C754
        C4D06F4C 257537CC D9A399E5 986BBD30 085EEC86 01582911


---------------------------

  returned_bits is
                                                ACD797A0 7B378D0A
        D9A8FBE2 1683E7BB 8A3DF9CB 1346FF43 2EA75B47 66B7C754
        C4D06F4C 257537CC D9A399E5 986BBD30 085EEC86 01582911


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                      66 B7C754C4
        D06F4C25 7537CCD9 A399E598 6BBD3008 5EEC8601 58291100


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        DF30730C
        59996936 44B98F12 22B7F33A E6856E8E 13F74BBD BF9D1F48


    V = HMAC(K, V) is
                                                        92C3122C
        4EF67B98 1F418241 3D718E9B A800A2D7 A45F9E6E 07C9C86B


rnd_val is
                                                ACD797A0 7B378D0A
        D9A8FBE2 1683E7BB 8A3DF9CB 1346FF43 2EA75B47 66B7C754
        C4D06F4C 257537CC D9A399E5 986BBD30 085EEC86 01582911


-------------------------------------------------------------
```

```
Second call to Generate

*****************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

Generate FAILED: Reseed is required
*****************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is  <empty>

  Seed_Material is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  Key is
                                                        DF30730C
        59996936 44B98F12 22B7F33A E6856E8E 13F74BBD BF9D1F48


  V is
                                                        92C3122C
        4EF67B98 1F418241 3D718E9B A800A2D7 A45F9E6E 07C9C86B


---------------------------

  Update

    provided_data
                                                C0C1C2 C3C4C5C6
```

```
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  ------------

  V || 0x00 || provided_data is
                                92C3122C 4EF67B98 1F418241
    3D718E9B A800A2D7 A45F9E6E 07C9C86B 00C0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  K = HMAC(K, V || 0x00 || provided_data) is
                                                  4F2B28A0
    087B3D6D 2547F378 D7F9C755 9964D055 1645831E 741B6BA5


  V = HMAC(K, V) is
                                                  4C5DB5ED
    89B9E3C3 35D79EFB 4EF5B0F4 A1F4E9D0 F3EFA1D1 D086A7BE


  ------------

  V || 0x01 || provided_data is
                                4C5DB5ED 89B9E3C3 35D79EFB
    4EF5B0F4 A1F4E9D0 F3EFA1D1 D086A7BE 01C0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  K = HMAC(K, V || 0x01 || provided_data) is
                                                  4B1DC621
    0B96E8E4 2657BF25 CC14B415 9F740014 2491860B D9AA7A00


  V = HMAC(K, V) is
                                                  ED0C4699
    3DDFEB91 A7EF6E4E E9EDB613 9A4C283C 5D493EDB 482390D7


Update (Key, V):

  Key is
                                                  4B1DC621
```

```
        0B96E8E4 2657BF25 CC14B415 9F740014 2491860B D9AA7A00


    V is
                                                           ED0C4699
        3DDFEB91 A7EF6E4E E9EDB613 9A4C283C 5D493EDB 482390D7


***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                           3531CEE9
        F51FBCA7 361CD991 0AD3A973 416EA587 4A5E5868 3E81BA3B


    temp is
                                                           3531CEE9
        F51FBCA7 361CD991 0AD3A973 416EA587 4A5E5868 3E81BA3B


  ------------

    V = HMAC(K, V) is
                                                           A36A191C
        0B74EDCF 25803D0F 046B3071 738648A8 DC0D4ABC 8C3E5A20


    temp is
                                                 3531CEE9 F51FBCA7
        361CD991 0AD3A973 416EA587 4A5E5868 3E81BA3B A36A191C
        0B74EDCF 25803D0F 046B3071 738648A8 DC0D4ABC 8C3E5A20


---------------------------

  returned_bits is
                                                 3531CEE9 F51FBCA7
        361CD991 0AD3A973 416EA587 4A5E5868 3E81BA3B A36A191C
```

```
        0B74EDCF 25803D0F 046B3071 738648A8 DC0D4ABC 8C3E5A20


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                      A3 6A191C0B
        74EDCF25 803D0F04 6B307173 8648A8DC 0D4ABC8C 3E5A2000


    K = HMAC(K, V || 0x00 || provided_data) is
                                                     CC792D62
        9EC9C4C8 C7983EFA B1E76661 57D43B4F 2CE63DC9 7AE979B3


    V = HMAC(K, V) is
                                                     00EBEB5A
        D8543B8E 5070F6FE 05CB7072 F7D30B47 29B2F718 6841DCB5


rnd_val is
                                                3531CEE9 F51FBCA7
        361CD991 0AD3A973 416EA587 4A5E5868 3E81BA3B A36A191C
        0B74EDCF 25803D0F 046B3071 738648A8 DC0D4ABC 8C3E5A20


###############################################################

HMAC_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    EntropyInput1 (for Reseed1) =
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                202122 23242526


    PersonalizationString =
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    nonce is
                                                202122 23242526


    personal_str is
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                                                        00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                        01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    ------------
```

```
  V || 0x00 || provided_data is
                                                              0101
      01010101 01010101 01010101 01010101 01010101 01010101
      01010000 01020304 05060708 090A0B0C 0D0E0F10 11121314
      15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
      2D2E2F30 31323334 35362021 22232425 26404142 43444546
      4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
      5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  K = HMAC(K, V || 0x00 || provided_data) is
                                                            B45032CF
      6A06E937 50DBD791 1C1F7701 11FA85E4 522863CA 4B8B66E7


  V = HMAC(K, V) is
                                                            A00F5F20
      C0D5BC5D CCDFDEC7 8839E0D5 376D22CC A1ABEB9A 2FC53CAC


  ------------

  V || 0x01 || provided_data is
                                                              A00F
      5F20C0D5 BC5DCCDF DEC78839 E0D5376D 22CCA1AB EB9A2FC5
      3CAC0100 01020304 05060708 090A0B0C 0D0E0F10 11121314
      15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
      2D2E2F30 31323334 35362021 22232425 26404142 43444546
      4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
      5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  K = HMAC(K, V || 0x01 || provided_data) is
                                                            4F7FCBA2
      3A6D7557 A0D657F7 57E3EBA4 6093D3BD F5D86BCF D941B53A


  V = HMAC(K, V) is
                                                            D0DE6F99
      D9E7DF8C 07E9F4D7 5E05B73E FDE0834B 2E19CC1F DC0FC853


Update (Key, V):

  Key is
                                                            4F7FCBA2
```

```
        3A6D7557 A0D657F7 57E3EBA4 6093D3BD F5D86BCF D941B53A


    V is
                                                          D0DE6F99
        D9E7DF8C 07E9F4D7 5E05B73E FDE0834B 2E19CC1F DC0FC853


---------------------------------------------------------------

First call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
***************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Seed_Material is
                             8081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
```

```
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Key is
                                                          4F7FCBA2
        3A6D7557 A0D657F7 57E3EBA4 6093D3BD F5D86BCF D941B53A


  V is
                                                          D0DE6F99
        D9E7DF8C 07E9F4D7 5E05B73E FDE0834B 2E19CC1F DC0FC853


---------------------------

  Update

    provided_data
                              8081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                   D0DE6F 99D9E7DF 8C07E9F4 D75E05B7 3EFDE083
        4B2E19CC 1FDC0FC8 53008081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                                                          7B84E441
        10AEB20F 7E6B716C C1CC579B 83DD4D9E 8ECB38BF 5F6525C3


    V = HMAC(K, V) is
                                                          A027489C
        623DFED2 455551AC 37A813AD 12D21A5D 0E886088 883BC831
```

```
    ------------

    V || 0x01 || provided_data is
                  A02748 9C623DFE D2455551 AC37A813 AD12D21A
        5D0E8860 88883BC8 31018081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
                                                       56C32756
        61E13129 CBB88B5D 29C98DD9 FC5FC3E1 68A84827 0A1AF27E


    V = HMAC(K, V) is
                                                       A62217F1
        E0DDF482 4D64B43D 8A2493B8 7E366BCE 3688E103 059FC6A3


  Update (Key, V):

    Key is
                                                       56C32756
        61E13129 CBB88B5D 29C98DD9 FC5FC3E1 68A84827 0A1AF27E


    V is
                                                       A62217F1
        E0DDF482 4D64B43D 8A2493B8 7E366BCE 3688E103 059FC6A3


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                       C1DA29D0
        48DDBED3 DCCE1040 DCF74E66 0FC2D883 269E65B4 9DBFAD8E
```

```
    temp is
                                                          C1DA29D0
        48DDBED3 DCCE1040 DCF74E66 0FC2D883 269E65B4 9DBFAD8E


  ------------

    V = HMAC(K, V) is
                                                          C99CECB6
        5C4EE17A BC3E3A93 342750DC 623A92A8 2A12A05F 0E59B714


    temp is
                                                C1DA29D0 48DDBED3
        DCCE1040 DCF74E66 0FC2D883 269E65B4 9DBFAD8E C99CECB6
        5C4EE17A BC3E3A93 342750DC 623A92A8 2A12A05F 0E59B714


---------------------------

  returned_bits is
                                                C1DA29D0 48DDBED3
        DCCE1040 DCF74E66 0FC2D883 269E65B4 9DBFAD8E C99CECB6
        5C4EE17A BC3E3A93 342750DC 623A92A8 2A12A05F 0E59B714


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                       C9 9CECB65C
        4EE17ABC 3E3A9334 2750DC62 3A92A82A 12A05F0E 59B71400


    K = HMAC(K, V || 0x00 || provided_data) is
                                                          B2AA116E
        3C7B57EC 08806FC0 3A223326 0A5EA550 D83F0AFB 2390C539
```

```
    V = HMAC(K, V) is
                                                          B96A8DB8
        006DAF12 C4D23EAF 36935AB7 8FE914FD DD0D79BF A33D7465


rnd_val is
                                              C1DA29D0 48DDBED3
        DCCE1040 DCF74E66 0FC2D883 269E65B4 9DBFAD8E C99CECB6
        5C4EE17A BC3E3A93 342750DC 623A92A8 2A12A05F 0E59B714


------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Seed_Material is
```

```
                            C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Key is
                                                    B2AA116E
        3C7B57EC 08806FC0 3A223326 0A5EA550 D83F0AFB 2390C539


  V is
                                                    B96A8DB8
        006DAF12 C4D23EAF 36935AB7 8FE914FD DD0D79BF A33D7465


---------------------------

  Update

    provided_data
                            C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                  B96A8D B8006DAF 12C4D23E AF36935A B78FE914
        FDDD0D79 BFA33D74 6500C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                    8D7799DF
        5B9F1037 ED8D020E BCE90603 FCEE0235 01078635 04B69414


    V = HMAC(K, V) is
```

```
                                                          8DDAAFC4
        6B81D406 918BD1EF CB37742E 43077C81 4D4D5879 2FB8B8FA


    ------------

    V || 0x01 || provided_data is
                   8DDAAF C46B81D4 06918BD1 EFCB3774 2E43077C
        814D4D58 792FB8B8 FA01C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
                                                          2C50D3C3
        468AAE25 80069E95 CEA6AE36 9F46D9FA 42DBCFA1 78599093


    V = HMAC(K, V) is
                                                          DC2EAE8F
        7B370072 D450D431 86813E8A CA306B16 A27F5A2C 51464A0E


  Update (Key, V):

    Key is
                                                          2C50D3C3
        468AAE25 80069E95 CEA6AE36 9F46D9FA 42DBCFA1 78599093


    V is
                                                          DC2EAE8F
        7B370072 D450D431 86813E8A CA306B16 A27F5A2C 51464A0E


************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------
```

```
    V = HMAC(K, V) is
                                                          62CB0F78
        6098110C 817975BA 4AAB395E 2E7D2B7F B0CDD094 59693A1A


    temp is
                                                          62CB0F78
        6098110C 817975BA 4AAB395E 2E7D2B7F B0CDD094 59693A1A


  ------------

    V = HMAC(K, V) is
                                                          952AD057
        CA66E306 F283E5F8 AAAB2087 B0B8A2E1 6DEDF4C3 C5EE8B71


    temp is
                                                 62CB0F78 6098110C
        817975BA 4AAB395E 2E7D2B7F B0CDD094 59693A1A 952AD057
        CA66E306 F283E5F8 AAAB2087 B0B8A2E1 6DEDF4C3 C5EE8B71


--------------------------

  returned_bits is
                                                 62CB0F78 6098110C
        817975BA 4AAB395E 2E7D2B7F B0CDD094 59693A1A 952AD057
        CA66E306 F283E5F8 AAAB2087 B0B8A2E1 6DEDF4C3 C5EE8B71


  call Update(additional_input, K, V)
--------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                       95 2AD057CA
        66E306F2 83E5F8AA AB2087B0 B8A2E16D EDF4C3C5 EE8B7100
```

```
    K = HMAC(K, V || 0x00 || provided_data) is
                                                        5CE58637
        BE1FD995 D54EA9C7 1C3CFB3F 40709465 40E2C717 BBC70669


    V = HMAC(K, V) is
                                                        577AEE11
        6868CE4D CA699C4D E3276E5F DBAEB601 594E6CF8 27A67EF2


rnd_val is
                                                62CB0F78 6098110C
        817975BA 4AAB395E 2E7D2B7F B0CDD094 59693A1A 952AD057
        CA66E306 F283E5F8 AAAB2087 B0B8A2E1 6DEDF4C3 C5EE8B71
```

```
###############################################################

HMAC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    nonce is
                                                20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                              000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


  Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                              000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    ------------

    V || 0x00 || provided_data is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 00000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    K = HMAC(K, V || 0x00 || provided_data) is
                                                44AD352A 3BEE9247
```

```
        C10F06B0 7EAA3983 C163F7D1 2FD023C7 72F45B84 66477910


    V = HMAC(K, V) is
                                                8E900608 F34F1504
        5D31A80E 9D699577 BF327E45 DBC501BC 4F45BA26 A9B4C4BC


    ------------

    V || 0x01 || provided_data is
        8E900608 F34F1504 5D31A80E 9D699577 BF327E45 DBC501BC
        4F45BA26 A9B4C4BC 01000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    K = HMAC(K, V || 0x01 || provided_data) is
                                                3DDA543E 7EEF14F9
        36237BE6 5D094B4D DC969C0B 2B5EAFB5 D805E86C FA64D741


    V = HMAC(K, V) is
                                                2D02C2F8 22517D54
        B817279A 59491C41 A1989B3E 382DEBE8 0D2C7F66 0F4476C4


  Update (Key, V):

    Key is
                                                3DDA543E 7EEF14F9
        36237BE6 5D094B4D DC969C0B 2B5EAFB5 D805E86C FA64D741


    V is
                                                2D02C2F8 22517D54
        B817279A 59491C41 A1989B3E 382DEBE8 0D2C7F66 0F4476C4


------------------------------------------------------------

First call to Generate

************************************************************

HMAC_DRBG_Generate
```

```
  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                              D67B8C17 34F46FA3
        F763CF57 C6F9F4F2 DC1089BD 8BC1F6F0 23950BFC 56176352


    temp is
                                              D67B8C17 34F46FA3
        F763CF57 C6F9F4F2 DC1089BD 8BC1F6F0 23950BFC 56176352


  ------------

    V = HMAC(K, V) is
                                              08C85012 38AD7A44
        00DEFEE4 6C640B61 AF77C2D1 A3BFAA90 EDE5D207 406E5403


    temp is
                          D67B8C17 34F46FA3 F763CF57 C6F9F4F2
        DC1089BD 8BC1F6F0 23950BFC 56176352 08C85012 38AD7A44
        00DEFEE4 6C640B61 AF77C2D1 A3BFAA90 EDE5D207 406E5403


---------------------------

  returned_bits is
                          D67B8C17 34F46FA3 F763CF57 C6F9F4F2
        DC1089BD 8BC1F6F0 23950BFC 56176352 08C85012 38AD7A44
        00DEFEE4 6C640B61 AF77C2D1 A3BFAA90 EDE5D207 406E5403


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------
```

```
    V || 0x00 || provided_data is
                                          08 C8501238 AD7A4400
        DEFEE46C 640B61AF 77C2D1A3 BFAA90ED E5D20740 6E540300


    K = HMAC(K, V || 0x00 || provided_data) is
                                          DD309579 353802CC
        DD4399C3 691C9DD9 09DD3B2D D003CCD5 9D6F08D8 5F2E3509


    V = HMAC(K, V) is
                                          A1C20FF2 70A39D2B
        8D03D659 B9DDD011 C2CCDF24 48557EF6 A1A915D1 8940A688


rnd_val is
                         D67B8C17 34F46FA3 F763CF57 C6F9F4F2
        DC1089BD 8BC1F6F0 23950BFC 56176352 08C85012 38AD7A44
        00DEFEE4 6C640B61 AF77C2D1 A3BFAA90 EDE5D207 406E5403


----------------------------------------------------------------

Second call to Generate

****************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                          8FDAEC20 F8B42140
        7059E358 8920DA7E DA9DCE3C F8274DFA 1C59C108 C1D0AA9B


    temp is
                                          8FDAEC20 F8B42140
        7059E358 8920DA7E DA9DCE3C F8274DFA 1C59C108 C1D0AA9B
```

```
  ------------

    V = HMAC(K, V) is
                                                0FA38DA5 C792037C
        4D33CD07 0CA7CD0C 5608DBA8 B8856546 39DE2187 B74CB263


    temp is
                            8FDAEC20 F8B42140 7059E358 8920DA7E
        DA9DCE3C F8274DFA 1C59C108 C1D0AA9B 0FA38DA5 C792037C
        4D33CD07 0CA7CD0C 5608DBA8 B8856546 39DE2187 B74CB263


---------------------------

  returned_bits is
                            8FDAEC20 F8B42140 7059E358 8920DA7E
        DA9DCE3C F8274DFA 1C59C108 C1D0AA9B 0FA38DA5 C792037C
        4D33CD07 0CA7CD0C 5608DBA8 B8856546 39DE2187 B74CB263


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                           0F A38DA5C7 92037C4D
        33CD070C A7CD0C56 08DBA8B8 85654639 DE2187B7 4CB26300


    K = HMAC(K, V || 0x00 || provided_data) is
                                                5CD5E50A 3E448A07
        C3D2F2A3 F9DEBCC0 465F9CF1 1CA136E9 B504B4D3 1C7FF1B8


    V = HMAC(K, V) is
                                                33B309F2 FF01CE10
        4B4429B6 75FAFA19 011E348B 2812715A 7637F6A6 E63B5D57


rnd_val is
```

```
                        8FDAEC20 F8B42140 7059E358 8920DA7E
        DA9DCE3C F8274DFA 1C59C108 C1D0AA9B 0FA38DA5 C792037C
        4D33CD07 0CA7CD0C 5608DBA8 B8856546 39DE2187 B74CB263


##############################################################

HMAC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                              000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                              808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                              C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                            20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput1 =
                                              606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                              A0A1A2 A3A4A5A6
```

```
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                               20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


  Key is
                                               00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                               01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                            000102 03040506 0708090A 0B0C0D0E
```

```
    0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
    2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


  ------------

  V || 0x00 || provided_data is
    01010101 01010101 01010101 01010101 01010101 01010101
    01010101 01010101 00000102 03040506 0708090A 0B0C0D0E
    0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
    2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


  K = HMAC(K, V || 0x00 || provided_data) is
                                         44AD352A 3BEE9247
    C10F06B0 7EAA3983 C163F7D1 2FD023C7 72F45B84 66477910


  V = HMAC(K, V) is
                                         8E900608 F34F1504
    5D31A80E 9D699577 BF327E45 DBC501BC 4F45BA26 A9B4C4BC


  ------------

  V || 0x01 || provided_data is
    8E900608 F34F1504 5D31A80E 9D699577 BF327E45 DBC501BC
    4F45BA26 A9B4C4BC 01000102 03040506 0708090A 0B0C0D0E
    0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
    2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


  K = HMAC(K, V || 0x01 || provided_data) is
                                         3DDA543E 7EEF14F9
    36237BE6 5D094B4D DC969C0B 2B5EAFB5 D805E86C FA64D741


  V = HMAC(K, V) is
                                         2D02C2F8 22517D54
    B817279A 59491C41 A1989B3E 382DEBE8 0D2C7F66 0F4476C4


Update (Key, V):

  Key is
                                         3DDA543E 7EEF14F9
```

```
        36237BE6 5D094B4D DC969C0B 2B5EAFB5 D805E86C FA64D741


    V is
                                                2D02C2F8 22517D54
        B817279A 59491C41 A1989B3E 382DEBE8 0D2C7F66 0F4476C4


---------------------------------------------------------------

First call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                          2D02C2F8 22517D54 B817279A 59491C41
        A1989B3E 382DEBE8 0D2C7F66 0F4476C4 00606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                                                BC43CACB 4AFF5D2D
```

```
      A0C65825 D013B674 E6950B8D 926F5E57 18F8D9BA 839FC4EE


  V = HMAC(K, V) is
                                                 C5FF9271 0AE3ECB8
      6D76A3EB 1C5100C3 B79F8E19 B943E1E6 C76ABB92 756B59BC


  ------------

  V || 0x01 || provided_data is
                         C5FF9271 0AE3ECB8 6D76A3EB 1C5100C3
      B79F8E19 B943E1E6 C76ABB92 756B59BC 01606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  K = HMAC(K, V || 0x01 || provided_data) is
                                                 08B5732C FC2C5F8C
      9EA915AE 8F6419AB 5383373E 6EE0DBF0 37325E82 1C548A66


  V = HMAC(K, V) is
                                                 CD58D9B9 850EB9DD
      1EC6C827 5A41F6AF 0153AB5E 5C0E3654 0FB4D618 BBFE0640


------------

  V = HMAC(K, V) is
                                                 41878735 8135419B
      93813353 5306176A FB251CDD 2BA37988 59B566A0 5CFB1D68


  temp is
                                                 41878735 8135419B
      93813353 5306176A FB251CDD 2BA37988 59B566A0 5CFB1D68


------------

  V = HMAC(K, V) is
                                                 0EA92585 6D5B84D5
      6ADAE870 45A6BA28 D2C908AB 75B7CC41 431FAC59 F38918A3
```

```
    temp is
                          41878735 8135419B 93813353 5306176A
        FB251CDD 2BA37988 59B566A0 5CFB1D68 0EA92585 6D5B84D5
        6ADAE870 45A6BA28 D2C908AB 75B7CC41 431FAC59 F38918A3


---------------------------

  returned_bits is
                          41878735 8135419B 93813353 5306176A
        FB251CDD 2BA37988 59B566A0 5CFB1D68 0EA92585 6D5B84D5
        6ADAE870 45A6BA28 D2C908AB 75B7CC41 431FAC59 F38918A3


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                 606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                          0EA92585 6D5B84D5 6ADAE870 45A6BA28
        D2C908AB 75B7CC41 431FAC59 F38918A3 00606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                                                 19D384D9 A9A7F8F5
        401C181E BDEDD94E 297AC090 5FD44A97 5AB78132 36CB8D2A


    V = HMAC(K, V) is
                                                 06461517 E829ADA4
        E5AB4523 EBA1514B 56A141D7 94C3877F EFAA7CB2 07C2BBC7


    ------------
```

```
    V || 0x01 || provided_data is
                            06461517 E829ADA4 E5AB4523 EBA1514B
        56A141D7 94C3877F EFAA7CB2 07C2BBC7 01606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
                                               791D3144 B302AD6C
        E4324134 4210AAD0 D399EDB7 B5906FB2 51DB1CB6 0004EA51


    V = HMAC(K, V) is
                                               58FD965F 4F99893C
        17E6A33C B8E90415 B516D006 14A449D4 06E03C68 5BD859BD


rnd_val is
                            41878735 8135419B 93813353 5306176A
        FB251CDD 2BA37988 59B566A0 5CFB1D68 0EA92585 6D5B84D5
        6ADAE870 45A6BA28 D2C908AB 75B7CC41 431FAC59 F38918A3


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                 A0A1A2 A3A4A5A6
```

```
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  ------------

  V || 0x00 || provided_data is
                       58FD965F 4F99893C 17E6A33C B8E90415
    B516D006 14A449D4 06E03C68 5BD859BD 00A0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  K = HMAC(K, V || 0x00 || provided_data) is
                                          FC15C8FD 1A937961
    D6880278 84E31C1A 679694A2 4543B65E CDAA24A5 457AFF6E


  V = HMAC(K, V) is
                                          F72F8818 3AFCE0AE
    B1B53151 962AFAB7 D2C87E51 97B1E21C 25D2CC83 C2F20801


  ------------

  V || 0x01 || provided_data is
                       F72F8818 3AFCE0AE B1B53151 962AFAB7
    D2C87E51 97B1E21C 25D2CC83 C2F20801 01A0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  K = HMAC(K, V || 0x01 || provided_data) is
                                          36A2F9CE A0B5E314
    CBE70BD5 E8D81916 2498C734 4F50FB34 D8879990 E2985CDA


  V = HMAC(K, V) is
                                          1FAF36AE BAFF731D
    99921019 DB901FBC 62C562AF E1C535A6 7EE281D3 8CF1FA40


------------

  V = HMAC(K, V) is
                                          7C067BDD CA817248
```

```
        23D64C69 829285BD BFF53771 6102C188 2E202250 E0FA5EF3


    temp is
                                                7C067BDD CA817248
        23D64C69 829285BD BFF53771 6102C188 2E202250 E0FA5EF3


  ------------

    V = HMAC(K, V) is
                                               A384CD34 A20FFD1F
        BC91E0C5 32A8A421 BC4AFE3C D47F2232 3EB4BAE1 A0078981


    temp is
                           7C067BDD CA817248 23D64C69 829285BD
        BFF53771 6102C188 2E202250 E0FA5EF3 A384CD34 A20FFD1F
        BC91E0C5 32A8A421 BC4AFE3C D47F2232 3EB4BAE1 A0078981


---------------------------

  returned_bits is
                           7C067BDD CA817248 23D64C69 829285BD
        BFF53771 6102C188 2E202250 E0FA5EF3 A384CD34 A20FFD1F
        BC91E0C5 32A8A421 BC4AFE3C D47F2232 3EB4BAE1 A0078981


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                           A384CD34 A20FFD1F BC91E0C5 32A8A421
        BC4AFE3C D47F2232 3EB4BAE1 A0078981 00A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
```

```
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                                              F7EE5EE9 3CE673E2
        48886523 A03B5F16 580ADD46 C62F4CC9 2B6F870E E6F503F2


    V = HMAC(K, V) is
                                              721BE504 190DBE91
        CD17E519 1C0885FC 8B7C9060 352B08EB FEB1DB58 55B4B040


    ------------

    V || 0x01 || provided_data is
                           721BE504 190DBE91 CD17E519 1C0885FC
        8B7C9060 352B08EB FEB1DB58 55B4B040 01A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
                                              E7458FB4 4A369A65
        3F2F8F57 7BF975C4 B362C4FE 618B2F1F F6769B13 C94DECF4


    V = HMAC(K, V) is
                                              19334B8C 31B74932
        DDD7B2A4 68F6436D F92E100D 39D3ACB3 68C7029C B883EC89


rnd_val is
                           7C067BDD CA817248 23D64C69 829285BD
        BFF53771 6102C188 2E202250 E0FA5EF3 A384CD34 A20FFD1F
        BC91E0C5 32A8A421 BC4AFE3C D47F2232 3EB4BAE1 A0078981


################################################################

HMAC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256
```

```
    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                              20212223 24252627


    PersonalizationString =
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

##################################################################

**********************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                              20212223 24252627
```

```
    personal_str is
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                                               00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                               01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    ------------

    V || 0x00 || provided_data is
                                                010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01000001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
```

```
    2E2F3031 32333435 36202122 23242526 27404142 43444546
    4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
    5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  K = HMAC(K, V || 0x00 || provided_data) is
                                          E48294AE A5171B5D
    6A091450 868B39C4 B14D4E1A 9B29F128 416E1E14 81D10F69


  V = HMAC(K, V) is
                                          40987A58 C3E1346C
    0023F00F 417FA7BD 09C72FED A9738670 993392DF 490E94E2


  ------------

  V || 0x01 || provided_data is
                                            40987A 58C3E134
    6C0023F0 0F417FA7 BD09C72F EDA97386 70993392 DF490E94
    E2010001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36202122 23242526 27404142 43444546
    4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
    5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  K = HMAC(K, V || 0x01 || provided_data) is
                                          65673C34 8E51CFAC
    C410BD20 0249A59A 9D6BAE77 6904271B B1F718DA 1D182042


  V = HMAC(K, V) is
                                          E0F91AC9 9630EEE6
    7CF830CF D5044FEB F55C0C11 5007997A DA11296F C4164A9A


Update (Key, V):

  Key is
                                          65673C34 8E51CFAC
    C410BD20 0249A59A 9D6BAE77 6904271B B1F718DA 1D182042


  V is
                                          E0F91AC9 9630EEE6
```

```
        7CF830CF D5044FEB F55C0C11 5007997A DA11296F C4164A9A


------------------------------------------------------------

First call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                0DD9C855 89F357C3
        89D6AF8D E9D734A9 17C771EF 2D8816B9 82596ED1 2DB45D73


    temp is
                                                0DD9C855 89F357C3
        89D6AF8D E9D734A9 17C771EF 2D8816B9 82596ED1 2DB45D73


  ------------

    V = HMAC(K, V) is
                                                4A626808 35C02FDA
        66B08E1A 369AE218 F26D5210 AD564248 872D7A28 784159C3


    temp is
                           0DD9C855 89F357C3 89D6AF8D E9D734A9
        17C771EF 2D8816B9 82596ED1 2DB45D73 4A626808 35C02FDA
        66B08E1A 369AE218 F26D5210 AD564248 872D7A28 784159C3


---------------------------

  returned_bits is
                           0DD9C855 89F357C3 89D6AF8D E9D734A9
        17C771EF 2D8816B9 82596ED1 2DB45D73 4A626808 35C02FDA
        66B08E1A 369AE218 F26D5210 AD564248 872D7A28 784159C3
```

```
  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                          4A 62680835 C02FDA66
        B08E1A36 9AE218F2 6D5210AD 56424887 2D7A2878 4159C300


    K = HMAC(K, V || 0x00 || provided_data) is
                                            F0B2F242 CAD992A7
        24F7E559 1D2F3B0C 2157AE70 D5327899 40F16445 9B00C749


    V = HMAC(K, V) is
                                            1A03F91C 5120BACA
        2BF6C64D D73AB11D F6FD3FF1 AC3B5720 A3F7FBE3 9E7E7FE9


rnd_val is
                         0DD9C855 89F357C3 89D6AF8D E9D734A9
        17C771EF 2D8816B9 82596ED1 2DB45D73 4A626808 35C02FDA
        66B08E1A 369AE218 F26D5210 AD564248 872D7A28 784159C3


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------
```

```
    V = HMAC(K, V) is
                                                46B4F475 6AE715E0
        E51681AB 2932DE15 23BE5D13 BAF0F458 8B11FE37 2FDA37AB


    temp is
                                                46B4F475 6AE715E0
        E51681AB 2932DE15 23BE5D13 BAF0F458 8B11FE37 2FDA37AB


  ------------

    V = HMAC(K, V) is
                                                E3683173 41BC8BA9
        1FC5D85B 7FB8CA8F BC309A75 8FD6FCA9 DF43C766 0B221322


    temp is
                            46B4F475 6AE715E0 E51681AB 2932DE15
        23BE5D13 BAF0F458 8B11FE37 2FDA37AB E3683173 41BC8BA9
        1FC5D85B 7FB8CA8F BC309A75 8FD6FCA9 DF43C766 0B221322


---------------------------

  returned_bits is
                            46B4F475 6AE715E0 E51681AB 2932DE15
        23BE5D13 BAF0F458 8B11FE37 2FDA37AB E3683173 41BC8BA9
        1FC5D85B 7FB8CA8F BC309A75 8FD6FCA9 DF43C766 0B221322


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                              E3 68317341 BC8BA91F
        C5D85B7F B8CA8FBC 309A758F D6FCA9DF 43C7660B 22132200


    K = HMAC(K, V || 0x00 || provided_data) is
```

```
                                                5C0DEC09 3708C17C
        A76B57C0 CB60CF88 9DCC47AD 10BD64BC 6A14B23F 2026078A


    V = HMAC(K, V) is
                                                456752A5 11B848BD
        05F1819B 9F6B1542 C7D5ECF9 32733926 7A0C7723 5B87DC5A


rnd_val is
                           46B4F475 6AE715E0 E51681AB 2932DE15
        23BE5D13 BAF0F458 8B11FE37 2FDA37AB E3683173 41BC8BA9
        1FC5D85B 7FB8CA8F BC309A75 8FD6FCA9 DF43C766 0B221322


################################################################

HMAC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                20212223 24252627
```

```
    PersonalizationString =
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                              20212223 24252627


    personal_str is
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
```

```
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                                                 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


----------------------------

  Update

    provided_data
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    ------------

    V || 0x00 || provided_data is
                                                   010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01000001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x00 || provided_data) is
                                                 E48294AE A5171B5D
        6A091450 868B39C4 B14D4E1A 9B29F128 416E1E14 81D10F69


    V = HMAC(K, V) is
                                                 40987A58 C3E1346C
        0023F00F 417FA7BD 09C72FED A9738670 993392DF 490E94E2
```

```
    ------------

    V || 0x01 || provided_data is
                                                40987A 58C3E134
        6C0023F0 0F417FA7 BD09C72F EDA97386 70993392 DF490E94
        E2010001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x01 || provided_data) is
                                               65673C34 8E51CFAC
        C410BD20 0249A59A 9D6BAE77 6904271B B1F718DA 1D182042


    V = HMAC(K, V) is
                                               E0F91AC9 9630EEE6
        7CF830CF D5044FEB F55C0C11 5007997A DA11296F C4164A9A


  Update (Key, V):

    Key is
                                               65673C34 8E51CFAC
        C410BD20 0249A59A 9D6BAE77 6904271B B1F718DA 1D182042


    V is
                                               E0F91AC9 9630EEE6
        7CF830CF D5044FEB F55C0C11 5007997A DA11296F C4164A9A


-----------------------------------------------------------

First call to Generate

***********************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512
```

```
    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                           E0F91AC9 9630EEE6 7CF830CF D5044FEB
        F55C0C11 5007997A DA11296F C4164A9A 00606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                                               AEC2D8F1 47E486D9
        02BFCBD5 3348C149 1E4D2FFB 1926867A ACA29FD0 C71DCFB7


    V = HMAC(K, V) is
                                               E6C969EE 096C8EE7
        B90A0AB5 587F435F DE8C4AFB 657910D4 B7B5E522 23C31FC1


    ------------

    V || 0x01 || provided_data is
                           E6C969EE 096C8EE7 B90A0AB5 587F435F
        DE8C4AFB 657910D4 B7B5E522 23C31FC1 01606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
```

```
                                                80B2F215 13E4279D
        F0A8C63F 985E14CE D2DEB415 821EA82A 716AAB4C 2552C49D


    V = HMAC(K, V) is
                                                4C16A0FC 00C35B53
        B152AA1E 430F241D 63B4F167 DF65CC92 FC3F4821 F0FBF71C


  ------------

    V = HMAC(K, V) is
                                                1478F29E 94B02CB4
        0D3AAB86 245557CE 13A8CA2F DB657D98 EFC19234 6B9FAC33


    temp is
                                                1478F29E 94B02CB4
        0D3AAB86 245557CE 13A8CA2F DB657D98 EFC19234 6B9FAC33


  ------------

    V = HMAC(K, V) is
                                                EA58ADA2 CCA432CC
        DEFBCDAA 8B82F553 EF966134 E2CD139F 15F01CAD 568565A8


    temp is
                            1478F29E 94B02CB4 0D3AAB86 245557CE
        13A8CA2F DB657D98 EFC19234 6B9FAC33 EA58ADA2 CCA432CC
        DEFBCDAA 8B82F553 EF966134 E2CD139F 15F01CAD 568565A8


---------------------------

  returned_bits is
                            1478F29E 94B02CB4 0D3AAB86 245557CE
        13A8CA2F DB657D98 EFC19234 6B9FAC33 EA58ADA2 CCA432CC
        DEFBCDAA 8B82F553 EF966134 E2CD139F 15F01CAD 568565A8


  call Update(additional_input, K, V)
---------------------------

  Update
```

```
    provided_data
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                           EA58ADA2 CCA432CC DEFBCDAA 8B82F553
        EF966134 E2CD139F 15F01CAD 568565A8 00606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                                               584491D3 53B81040
        53EA0BD3 F436510C 5FD38433 939A1951 F4983744 A6C8E5AB


    V = HMAC(K, V) is
                                               E625EAF3 5BB58168
        F208A9EE 65A4A531 F3072BA6 7921D2F3 6838C3E1 6B4B7A69


    ------------

    V || 0x01 || provided_data is
                           E625EAF3 5BB58168 F208A9EE 65A4A531
        F3072BA6 7921D2F3 6838C3E1 6B4B7A69 01606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
                                               572C0374 C1A10125
        BFA6AECD 7CEBFE32 F752C3FB 316731B7 CFDBDEC2 6356932B


    V = HMAC(K, V) is
                                               D68BF041 F3EB5088
        088D8B8E 712C36AE 9583BB08 FD1F9034 A4E942E9 A6747CE7


rnd_val is
```

```
                        1478F29E 94B02CB4 0D3AAB86 245557CE
        13A8CA2F DB657D98 EFC19234 6B9FAC33 EA58ADA2 CCA432CC
        DEFBCDAA 8B82F553 EF966134 E2CD139F 15F01CAD 568565A8


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                        D68BF041 F3EB5088 088D8B8E 712C36AE
        9583BB08 FD1F9034 A4E942E9 A6747CE7 00A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                 39B0DA85 112EE543
        27721EEA A7A16965 F6E0975F F81F312A 7C88E79B 8F0F98E9
```

```
  V = HMAC(K, V) is
                                                B189B4DF 841734E7
      8B3D482E 9A082D36 16F5D674 23EADAE7 ED966B72 8EA10C56


  ------------

  V || 0x01 || provided_data is
                          B189B4DF 841734E7 8B3D482E 9A082D36
      16F5D674 23EADAE7 ED966B72 8EA10C56 01A0A1A2 A3A4A5A6
      A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
      BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  K = HMAC(K, V || 0x01 || provided_data) is
                                                D88F4E3B DAB9404B
      817B0EBD 27330511 E2B4C257 753CF527 CDA90871 4C73BC0D


  V = HMAC(K, V) is
                                                9CE06AB1 8AEC3612
      5C6E9029 156DDDD0 936072E1 78168681 1A6B57DE D8473E04


------------

  V = HMAC(K, V) is
                                                497C7A16 E88A6411
      F8FCE10E F56763C6 1025801D 8F51A743 52D682CC 23A0A8E6


  temp is
                                                497C7A16 E88A6411
      F8FCE10E F56763C6 1025801D 8F51A743 52D682CC 23A0A8E6


------------

  V = HMAC(K, V) is
                                                73CAE032 28939064
      7DC683B7 342885D6 B76AB1DA 696D3E97 E22DFFDD FFFD8DF0


  temp is
                          497C7A16 E88A6411 F8FCE10E F56763C6
      1025801D 8F51A743 52D682CC 23A0A8E6 73CAE032 28939064
```

```
        7DC683B7 342885D6 B76AB1DA 696D3E97 E22DFFDD FFFD8DF0


--------------------------

  returned_bits is
                         497C7A16 E88A6411 F8FCE10E F56763C6
        1025801D 8F51A743 52D682CC 23A0A8E6 73CAE032 28939064
        7DC683B7 342885D6 B76AB1DA 696D3E97 E22DFFDD FFFD8DF0


  call Update(additional_input, K, V)
--------------------------

  Update

    provided_data
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                         73CAE032 28939064 7DC683B7 342885D6
        B76AB1DA 696D3E97 E22DFFDD FFFD8DF0 00A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                 F8F5E360 854BAA38
        A7F3F443 12D2475A 0752C0CA 57643724 CFF0431C 0F93BD61


    V = HMAC(K, V) is
                                                 DC2F83C9 DA2605D2
        1E026EF0 6E008D53 34B51534 3CA1E918 472E7F81 D7E37EF5


    ------------

    V || 0x01 || provided_data is
                         DC2F83C9 DA2605D2 1E026EF0 6E008D53
        34B51534 3CA1E918 472E7F81 D7E37EF5 01A0A1A2 A3A4A5A6
```

```
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
                                              282E0734 80809375
        58B1392E 95AB91E7 C1F622B2 4FFB8720 A5F0A5E0 7550C7C2


    V = HMAC(K, V) is
                                              DFC3BDB5 F3BCF1AA
        68298E79 0D720A67 A76E31B9 2B9B35A8 E5471BB1 7E303C6B


rnd_val is
                         497C7A16 E88A6411 F8FCE10E F56763C6
        1025801D 8F51A743 52D682CC 23A0A8E6 73CAE032 28939064
        7DC683B7 342885D6 B76AB1DA 696D3E97 E22DFFDD FFFD8DF0


################################################################

HMAC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
```

```
    Nonce =
                                                20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


  Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


--------------------------
```

```
Update

  provided_data
                           000102 03040506 0708090A 0B0C0D0E
      0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
      2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


  ------------

  V || 0x00 || provided_data is
      01010101 01010101 01010101 01010101 01010101 01010101
      01010101 01010101 00000102 03040506 0708090A 0B0C0D0E
      0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
      2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


  K = HMAC(K, V || 0x00 || provided_data) is
                                           44AD352A 3BEE9247
      C10F06B0 7EAA3983 C163F7D1 2FD023C7 72F45B84 66477910


  V = HMAC(K, V) is
                                           8E900608 F34F1504
      5D31A80E 9D699577 BF327E45 DBC501BC 4F45BA26 A9B4C4BC


  ------------

  V || 0x01 || provided_data is
      8E900608 F34F1504 5D31A80E 9D699577 BF327E45 DBC501BC
      4F45BA26 A9B4C4BC 01000102 03040506 0708090A 0B0C0D0E
      0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
      2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


  K = HMAC(K, V || 0x01 || provided_data) is
                                           3DDA543E 7EEF14F9
      36237BE6 5D094B4D DC969C0B 2B5EAFB5 D805E86C FA64D741


  V = HMAC(K, V) is
                                           2D02C2F8 22517D54
      B817279A 59491C41 A1989B3E 382DEBE8 0D2C7F66 0F4476C4
```

```
  Update (Key, V):

    Key is
                                                3DDA543E 7EEF14F9
        36237BE6 5D094B4D DC969C0B 2B5EAFB5 D805E86C FA64D741


    V is
                                                2D02C2F8 22517D54
        B817279A 59491C41 A1989B3E 382DEBE8 0D2C7F66 0F4476C4


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    additional_input is  <empty>

  Seed_Material is
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  Key is
                                                3DDA543E 7EEF14F9
```

```
        36237BE6 5D094B4D DC969C0B 2B5EAFB5 D805E86C FA64D741


  V is
                                                 2D02C2F8 22517D54
        B817279A 59491C41 A1989B3E 382DEBE8 0D2C7F66 0F4476C4


---------------------------

  Update

    provided_data
                                                   808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    ------------

    V || 0x00 || provided_data is
                          2D02C2F8 22517D54 B817279A 59491C41
        A1989B3E 382DEBE8 0D2C7F66 0F4476C4 00808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                 E7F1346E 1B837375
        0DFF7840 DCD97C74 25F85732 87B91151 CD5C3C2A 37B06B0C


    V = HMAC(K, V) is
                                                 5775A709 1255E890
        3B575A25 6C0DE34E A959CDB4 F8ABEE3E D5C21D59 8243C185


    ------------

    V || 0x01 || provided_data is
                          5775A709 1255E890 3B575A25 6C0DE34E
        A959CDB4 F8ABEE3E D5C21D59 8243C185 01808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

```
    K = HMAC(K, V || 0x01 || provided_data) is
                                                B84007E3 E27F34F9
        A7820B7A B59BBEFC D0C4ACAE DE4B0B36 B147B897 79FD749D


    V = HMAC(K, V) is
                                                A72B8FEE 92392F0A
        9D2D61BF 09A4DFCC 9DE69A16 A5F15022 4C3EF604 2D1521FC


  Update (Key, V):

    Key is
                                                B84007E3 E27F34F9
        A7820B7A B59BBEFC D0C4ACAE DE4B0B36 B147B897 79FD749D


    V is
                                                A72B8FEE 92392F0A
        9D2D61BF 09A4DFCC 9DE69A16 A5F15022 4C3EF604 2D1521FC


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                FABD0AE2 5C69DC2E
        FDEFB7F2 0C5A31B5 7AC938AB 771AA19B F8F5F146 8F665C93


    temp is
                                                FABD0AE2 5C69DC2E
        FDEFB7F2 0C5A31B5 7AC938AB 771AA19B F8F5F146 8F665C93


  ------------

    V = HMAC(K, V) is
                                                8C9A1A5D F0628A56
```

```
        90F15A1A D8A613F3 1BBD65EE AD5457D5 D26947F2 9FE91AA7


    temp is
                            FABD0AE2 5C69DC2E FDEFB7F2 0C5A31B5
        7AC938AB 771AA19B F8F5F146 8F665C93 8C9A1A5D F0628A56
        90F15A1A D8A613F3 1BBD65EE AD5457D5 D26947F2 9FE91AA7


---------------------------

  returned_bits is
                            FABD0AE2 5C69DC2E FDEFB7F2 0C5A31B5
        7AC938AB 771AA19B F8F5F146 8F665C93 8C9A1A5D F0628A56
        90F15A1A D8A613F3 1BBD65EE AD5457D5 D26947F2 9FE91AA7


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                           8C 9A1A5DF0 628A5690
        F15A1AD8 A613F31B BD65EEAD 5457D5D2 6947F29F E91AA700


    K = HMAC(K, V || 0x00 || provided_data) is
                                           4348AF84 20842FA0
        77B9D3DB A8DCE9B3 E1DF734F FCE1BEA5 B9E2B154 DC5EC615


    V = HMAC(K, V) is
                                           D2C1AC27 885D4332
        76713146 32EA6043 3CCA7273 04569EA7 D471FEA7 DB7D315D


rnd_val is
                            FABD0AE2 5C69DC2E FDEFB7F2 0C5A31B5
        7AC938AB 771AA19B F8F5F146 8F665C93 8C9A1A5D F0628A56
        90F15A1A D8A613F3 1BBD65EE AD5457D5 D26947F2 9FE91AA7
```

```
------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is  <empty>

  Seed_Material is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  Key is
                                              4348AF84 20842FA0
        77B9D3DB A8DCE9B3 E1DF734F FCE1BEA5 B9E2B154 DC5EC615


  V is
                                              D2C1AC27 885D4332
        76713146 32EA6043 3CCA7273 04569EA7 D471FEA7 DB7D315D


---------------------------

  Update
```

```
  provided_data
                                                C0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  ------------

  V || 0x00 || provided_data is
                        D2C1AC27 885D4332 76713146 32EA6043
      3CCA7273 04569EA7 D471FEA7 DB7D315D 00C0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  K = HMAC(K, V || 0x00 || provided_data) is
                                               668B28ED 146DAB9E
      561501C6 544536C8 34259891 4A444CDB 484E709A 41E5C10F


  V = HMAC(K, V) is
                                               D19D64C7 941B480A
      C3444F46 A3771FD3 E3D204B1 270F33AD 6482D293 E1300249


  ------------

  V || 0x01 || provided_data is
                        D19D64C7 941B480A C3444F46 A3771FD3
      E3D204B1 270F33AD 6482D293 E1300249 01C0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  K = HMAC(K, V || 0x01 || provided_data) is
                                               BFA02CE7 E92DE92B
      18242886 890E586F 836906AC E9E554F1 B0ED6357 3CB8B503


  V = HMAC(K, V) is
                                               D32403EE A9DCE161
      6E4E1155 B923D884 2CC6E784 C67A9385 B2A637F1 02FA45D5


Update (Key, V):
```

```
    Key is
                                                BFA02CE7 E92DE92B
        18242886 890E586F 836906AC E9E554F1 B0ED6357 3CB8B503


    V is
                                                D32403EE A9DCE161
        6E4E1155 B923D884 2CC6E784 C67A9385 B2A637F1 02FA45D5


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                6BD925B0 E1C232EF
        D67CCD84 F722E927 ECB46AB2 B7400147 77AF14BA 0BBF53A4


    temp is
                                                6BD925B0 E1C232EF
        D67CCD84 F722E927 ECB46AB2 B7400147 77AF14BA 0BBF53A4


  ------------

    V = HMAC(K, V) is
                                                5BDBB62B 3F7D0B9C
        8EEAD057 C0EC754E F8B53E60 A1F434F0 5946A8B6 86AFBC7A


    temp is
                            6BD925B0 E1C232EF D67CCD84 F722E927
        ECB46AB2 B7400147 77AF14BA 0BBF53A4 5BDBB62B 3F7D0B9C
        8EEAD057 C0EC754E F8B53E60 A1F434F0 5946A8B6 86AFBC7A


---------------------------

  returned_bits is
```

```
                          6BD925B0 E1C232EF D67CCD84 F722E927
        ECB46AB2 B7400147 77AF14BA 0BBF53A4 5BDBB62B 3F7D0B9C
        8EEAD057 C0EC754E F8B53E60 A1F434F0 5946A8B6 86AFBC7A


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                          5B DBB62B3F 7D0B9C8E
        EAD057C0 EC754EF8 B53E60A1 F434F059 46A8B686 AFBC7A00


    K = HMAC(K, V || 0x00 || provided_data) is
                                          8121F776 4C081EE9
        D1171ED1 87BAE088 95CAE230 D0A25E37 39C57D54 16109B82


    V = HMAC(K, V) is
                                          3784977C C0E59FBC
        9CDA4E11 92475C6E FAF80720 19862122 CB6BCEAA CC4A175E


rnd_val is
                          6BD925B0 E1C232EF D67CCD84 F722E927
        ECB46AB2 B7400147 77AF14BA 0BBF53A4 5BDBB62B 3F7D0B9C
        8EEAD057 C0EC754E F8B53E60 A1F434F0 5946A8B6 86AFBC7A


##############################################################

HMAC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                            000102 03040506
```

```
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

nonce is
                                                20212223 24252627

personal_str is <empty>

prediction_resistance_flag = "PredictionResistance"

Seed_Material is
                              000102 03040506 0708090A 0B0C0D0E
      0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
      2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627

Key is
                                                00000000 00000000
      00000000 00000000 00000000 00000000 00000000 00000000

V is
                                                01010101 01010101
      01010101 01010101 01010101 01010101 01010101 01010101

Update

provided_data
                              000102 03040506 0708090A 0B0C0D0E
      0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
      2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627

V || 0x00 || provided_data is
      01010101 01010101 01010101 01010101 01010101 01010101
      01010101 01010101 00000102 03040506 0708090A 0B0C0D0E
      0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
      2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627

K = HMAC(K, V || 0x00 || provided_data) is
                                                44AD352A 3BEE9247
      C10F06B0 7EAA3983 C163F7D1 2FD023C7 72F45B84 66477910

```
    V = HMAC(K, V) is
                                                8E900608 F34F1504
        5D31A80E 9D699577 BF327E45 DBC501BC 4F45BA26 A9B4C4BC


    ------------

    V || 0x01 || provided_data is
        8E900608 F34F1504 5D31A80E 9D699577 BF327E45 DBC501BC
        4F45BA26 A9B4C4BC 01000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    K = HMAC(K, V || 0x01 || provided_data) is
                                                3DDA543E 7EEF14F9
        36237BE6 5D094B4D DC969C0B 2B5EAFB5 D805E86C FA64D741


    V = HMAC(K, V) is
                                                2D02C2F8 22517D54
        B817279A 59491C41 A1989B3E 382DEBE8 0D2C7F66 0F4476C4


  Update (Key, V):

    Key is
                                                3DDA543E 7EEF14F9
        36237BE6 5D094B4D DC969C0B 2B5EAFB5 D805E86C FA64D741


    V is
                                                2D02C2F8 22517D54
        B817279A 59491C41 A1989B3E 382DEBE8 0D2C7F66 0F4476C4


------------------------------------------------------------

First call to Generate

************************************************************

HMAC_DRBG_Generate
```

```
  requested_number_of_bits = 512

    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Seed_Material is
                             8081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Key is
                                               3DDA543E 7EEF14F9
        36237BE6 5D094B4D DC969C0B 2B5EAFB5 D805E86C FA64D741


  V is
                                               2D02C2F8 22517D54
        B817279A 59491C41 A1989B3E 382DEBE8 0D2C7F66 0F4476C4


---------------------------

  Update
```

```
provided_data
                          8081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


------------

V || 0x00 || provided_data is
      2D02C2 F822517D 54B81727 9A59491C 41A1989B 3E382DEB
    E80D2C7F 660F4476 C4008081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


K = HMAC(K, V || 0x00 || provided_data) is
                                        A61BAEFD DC0C56E3
    E0851C60 F83FDBB3 C9A8B56F 2B5ADA3B FD70228E FBC8EBCC


V = HMAC(K, V) is
                                        E1C3045A 91B61344
    A9493879 32B94894 A0D41A9D 873F2C61 A897D512 4AE95D27


------------

V || 0x01 || provided_data is
      E1C304 5A91B613 44A94938 7932B948 94A0D41A 9D873F2C
    61A897D5 124AE95D 27018081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


K = HMAC(K, V || 0x01 || provided_data) is
                                        C125EA99 758EBB9A
    6F69AE31 2AC204B5 94C00AB6 8B816E3A 52128E02 78A584AC
```

```
    V = HMAC(K, V) is
                                                B2CB2B89 123F5B4A
        F587B8F6 BDC5427A 991419D3 53077C68 5E707ACD F8E9FDA9


  Update (Key, V):

    Key is
                                                C125EA99 758EBB9A
        6F69AE31 2AC204B5 94C00AB6 8B816E3A 52128E02 78A584AC


    V is
                                                B2CB2B89 123F5B4A
        F587B8F6 BDC5427A 991419D3 53077C68 5E707ACD F8E9FDA9


****************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                085D57AF 6BABCF2B
        9AEEF387 D531650E 6A505C54 406AB37A 52899E0E CAB3632B


    temp is
                                                085D57AF 6BABCF2B
        9AEEF387 D531650E 6A505C54 406AB37A 52899E0E CAB3632B


  ------------

    V = HMAC(K, V) is
                                                7A068A28 14C6DF6A
        E532B658 D0D9741C 84775FEE 45B684CD BDC25FBC B4D8F310


    temp is
                            085D57AF 6BABCF2B 9AEEF387 D531650E
```

```
        6A505C54 406AB37A 52899E0E CAB3632B 7A068A28 14C6DF6A
        E532B658 D0D9741C 84775FEE 45B684CD BDC25FBC B4D8F310


---------------------------

  returned_bits is
                           085D57AF 6BABCF2B 9AEEF387 D531650E
        6A505C54 406AB37A 52899E0E CAB3632B 7A068A28 14C6DF6A
        E532B658 D0D9741C 84775FEE 45B684CD BDC25FBC B4D8F310


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                            7A 068A2814 C6DF6AE5
        32B658D0 D9741C84 775FEE45 B684CDBD C25FBCB4 D8F31000


    K = HMAC(K, V || 0x00 || provided_data) is
                                           C6ED8FED 7157A4D0
        9EA1DDE8 946B5443 3ECC5449 A4A352AF 45764EE6 734BBB04


    V = HMAC(K, V) is
                                           EBC77525 6BB78124
        1E9C70BB CF732BDC 90AD10D9 DD3A896E CC12B92F FB6345AB


rnd_val is
                           085D57AF 6BABCF2B 9AEEF387 D531650E
        6A505C54 406AB37A 52899E0E CAB3632B 7A068A28 14C6DF6A
        E532B658 D0D9741C 84775FEE 45B684CD BDC25FBC B4D8F310


-------------------------------------------------------------

Second call to Generate
```

```
***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
***************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Seed_Material is
                             C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Key is
                                                 C6ED8FED 7157A4D0
        9EA1DDE8 946B5443 3ECC5449 A4A352AF 45764EE6 734BBB04


  V is
                                                 EBC77525 6BB78124
        1E9C70BB CF732BDC 90AD10D9 DD3A896E CC12B92F FB6345AB
```

```
---------------------------

  Update

    provided_data
                              C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
          EBC775 256BB781 241E9C70 BBCF732B DC90AD10 D9DD3A89
        6ECC12B9 2FFB6345 AB00C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                                              EC9957E0 75B59A8B
        ABE0F473 DB8348C7 FDDB3291 39AAA1D9 81E7027A 8BF6F94D


    V = HMAC(K, V) is
                                              5D2D543E 1CB4E397
        FFD81958 E452D31E 951EEBBE 05AD5C68 6958E58B 1961275C


    ------------

    V || 0x01 || provided_data is
          5D2D54 3E1CB4E3 97FFD819 58E452D3 1E951EEB BE05AD5C
        686958E5 8B196127 5C01C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
```

```
                                                FC51DA84 F9696BCC
        84C8F2AC B924BCDF 72F82EA2 CA643F08 3B0C16C3 634EFC62


    V = HMAC(K, V) is
                                                B974E437 0AD576BB
        99C4E49E A680BFF9 8DE9E12F ECD013DE D43C80F6 9A7ADE8A


  Update (Key, V):

    Key is
                                                FC51DA84 F9696BCC
        84C8F2AC B924BCDF 72F82EA2 CA643F08 3B0C16C3 634EFC62


    V is
                                                B974E437 0AD576BB
        99C4E49E A680BFF9 8DE9E12F ECD013DE D43C80F6 9A7ADE8A


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                9B219FD9 0DE2A08E
        493405CF 874417B5 826770F3 94481555 DC668ACD 96B9A3E5


    temp is
                                                9B219FD9 0DE2A08E
        493405CF 874417B5 826770F3 94481555 DC668ACD 96B9A3E5


  ------------

    V = HMAC(K, V) is
                                                6F9D2C32 5E26D47C
        1DFCFC8F BF86126F 40A1E639 60F62749 342ECDB7 1B240DC6
```

```
    temp is
                            9B219FD9 0DE2A08E 493405CF 874417B5
        826770F3 94481555 DC668ACD 96B9A3E5 6F9D2C32 5E26D47C
        1DFCFC8F BF86126F 40A1E639 60F62749 342ECDB7 1B240DC6


----------------------------

  returned_bits is
                            9B219FD9 0DE2A08E 493405CF 874417B5
        826770F3 94481555 DC668ACD 96B9A3E5 6F9D2C32 5E26D47C
        1DFCFC8F BF86126F 40A1E639 60F62749 342ECDB7 1B240DC6


  call Update(additional_input, K, V)
----------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                          6F 9D2C325E 26D47C1D
        FCFC8FBF 86126F40 A1E63960 F6274934 2ECDB71B 240DC600


    K = HMAC(K, V || 0x00 || provided_data) is
                                          56A2B446 32CB8FC3
        A64009BF D6EC95E5 6CEF8E7C 912AA82B 16F61491 5D9CD6E3


    V = HMAC(K, V) is
                                          B5B396A0 1576B0FE
        42F40844 556C4CF4 B6804C94 DE9D6238 F1F7E7AF 5C7257F3


rnd_val is
                            9B219FD9 0DE2A08E 493405CF 874417B5
        826770F3 94481555 DC668ACD 96B9A3E5 6F9D2C32 5E26D47C
        1DFCFC8F BF86126F 40A1E639 60F62749 342ECDB7 1B240DC6
```

```
###############################################################

HMAC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                               20212223 24252627


    PersonalizationString =
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
```

```
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                20212223 24252627


    personal_str is
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576
```

```
  ------------

  V || 0x00 || provided_data is
                                                 010101 01010101
      01010101 01010101 01010101 01010101 01010101 01010101
      01000001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
      16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
      2E2F3031 32333435 36202122 23242526 27404142 43444546
      4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
      5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  K = HMAC(K, V || 0x00 || provided_data) is
                                               E48294AE A5171B5D
      6A091450 868B39C4 B14D4E1A 9B29F128 416E1E14 81D10F69


  V = HMAC(K, V) is
                                               40987A58 C3E1346C
      0023F00F 417FA7BD 09C72FED A9738670 993392DF 490E94E2


  ------------

  V || 0x01 || provided_data is
                                                 40987A 58C3E134
      6C0023F0 0F417FA7 BD09C72F EDA97386 70993392 DF490E94
      E2010001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
      16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
      2E2F3031 32333435 36202122 23242526 27404142 43444546
      4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
      5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  K = HMAC(K, V || 0x01 || provided_data) is
                                               65673C34 8E51CFAC
      C410BD20 0249A59A 9D6BAE77 6904271B B1F718DA 1D182042


  V = HMAC(K, V) is
                                               E0F91AC9 9630EEE6
      7CF830CF D5044FEB F55C0C11 5007997A DA11296F C4164A9A


Update (Key, V):
```

```
    Key is
                                                65673C34 8E51CFAC
        C410BD20 0249A59A 9D6BAE77 6904271B B1F718DA 1D182042


    V is
                                                E0F91AC9 9630EEE6
        7CF830CF D5044FEB F55C0C11 5007997A DA11296F C4164A9A


-----------------------------------------------------------------

First call to Generate

*****************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

Generate FAILED: Reseed is required
*****************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    additional_input is  <empty>

  Seed_Material is
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  Key is
                                                65673C34 8E51CFAC
        C410BD20 0249A59A 9D6BAE77 6904271B B1F718DA 1D182042
```

```
  V is
                                                E0F91AC9 9630EEE6
        7CF830CF D5044FEB F55C0C11 5007997A DA11296F C4164A9A


---------------------------

  Update

    provided_data
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    ------------

    V || 0x00 || provided_data is
                           E0F91AC9 9630EEE6 7CF830CF D5044FEB
        F55C0C11 5007997A DA11296F C4164A9A 00808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                6F9B62E0 F7918FD9
        251248F2 F8EBA1C3 DC736788 8BD5668A 08E773E3 4A197989


    V = HMAC(K, V) is
                                                54C051C9 1B500C9B
        798A021F E4B482AE 5D757F4F DFAA3502 489D1CEB A04D87DB


    ------------

    V || 0x01 || provided_data is
                           54C051C9 1B500C9B 798A021F E4B482AE
        5D757F4F DFAA3502 489D1CEB A04D87DB 01808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    K = HMAC(K, V || 0x01 || provided_data) is
                                                4476C6D1 1FC35D44
```

```
        09D9032E 453B0F0D C3314DB8 62CBDB60 9C560220 8D4C88D8


    V = HMAC(K, V) is
                                                95EF785A 61C2F7B3
        6BC596BA 4BA208A5 2C6DC203 636D8F17 87453B85 2B7E49EC


  Update (Key, V):

    Key is
                                                4476C6D1 1FC35D44
        09D9032E 453B0F0D C3314DB8 62CBDB60 9C560220 8D4C88D8


    V is
                                                95EF785A 61C2F7B3
        6BC596BA 4BA208A5 2C6DC203 636D8F17 87453B85 2B7E49EC


****************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                D8B67130 714194FF
        E5B2A35D BCD5E1A2 9942AD5C 68F3DEB9 4ADD9E9E BAD86067


    temp is
                                                D8B67130 714194FF
        E5B2A35D BCD5E1A2 9942AD5C 68F3DEB9 4ADD9E9E BAD86067


  ------------

    V = HMAC(K, V) is
                                                EDF04915 FB40C391
        EAE70C65 9EAAE7EF 11A3D46A 5B085EDD 90CC72CE A989210B
```

```
    temp is
                           D8B67130 714194FF E5B2A35D BCD5E1A2
         9942AD5C 68F3DEB9 4ADD9E9E BAD86067 EDF04915 FB40C391
         EAE70C65 9EAAE7EF 11A3D46A 5B085EDD 90CC72CE A989210B


---------------------------

  returned_bits is
                           D8B67130 714194FF E5B2A35D BCD5E1A2
         9942AD5C 68F3DEB9 4ADD9E9E BAD86067 EDF04915 FB40C391
         EAE70C65 9EAAE7EF 11A3D46A 5B085EDD 90CC72CE A989210B


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                           ED F04915FB 40C391EA
         E70C659E AAE7EF11 A3D46A5B 085EDD90 CC72CEA9 89210B00


    K = HMAC(K, V || 0x00 || provided_data) is
                                           0DF9110E 2F225898
         24A9476C 8E32088E 51A0DA36 633F8CD1 F7547DFF 696E4B29


    V = HMAC(K, V) is
                                           C0E3C8ED 5A8B579E
         3FEF9DF3 B7C2C212 980717CC 91AE1866 45FABB2C C784D5D7


rnd_val is
                           D8B67130 714194FF E5B2A35D BCD5E1A2
         9942AD5C 68F3DEB9 4ADD9E9E BAD86067 EDF04915 FB40C391
         EAE70C65 9EAAE7EF 11A3D46A 5B085EDD 90CC72CE A989210B


-------------------------------------------------------------
```

```
Second call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is  <empty>

  Seed_Material is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  Key is
                                               0DF9110E 2F225898
        24A9476C 8E32088E 51A0DA36 633F8CD1 F7547DFF 696E4B29


  V is
                                               C0E3C8ED 5A8B579E
        3FEF9DF3 B7C2C212 980717CC 91AE1866 45FABB2C C784D5D7


---------------------------

  Update

    provided_data
                                                C0C1C2 C3C4C5C6
```

```
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  ------------

  V || 0x00 || provided_data is
                       C0E3C8ED 5A8B579E 3FEF9DF3 B7C2C212
    980717CC 91AE1866 45FABB2C C784D5D7 00C0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  K = HMAC(K, V || 0x00 || provided_data) is
                                          C1A605C2 002F91FD
    0D0CAAD2 8F6DC96D 0D0C0362 404C9B6F 41EB52F4 5A61204C


  V = HMAC(K, V) is
                                          A9EFDB92 95BD1AE4
    A9C00AFF 6D03ED60 697D8F5A 067F1B2F 1826A94D 42060E21


  ------------

  V || 0x01 || provided_data is
                       A9EFDB92 95BD1AE4 A9C00AFF 6D03ED60
    697D8F5A 067F1B2F 1826A94D 42060E21 01C0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  K = HMAC(K, V || 0x01 || provided_data) is
                                          3D7763E5 303DB54B
    E20544A8 1E9F00CA DCFC1CB2 8DECB9CF C699F61D BAF88021


  V = HMAC(K, V) is
                                          FEBC0279 B7710DEC
    5C067EBE FA068E4B 5967491B 7EEF9475 83506D04 97CE67BA


Update (Key, V):

  Key is
                                          3D7763E5 303DB54B
```

```
        E20544A8 1E9F00CA DCFC1CB2 8DECB9CF C699F61D BAF88021


    V is
                                                FEBC0279 B7710DEC
        5C067EBE FA068E4B 5967491B 7EEF9475 83506D04 97CE67BA


****************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                8BBA71C2 583F2530
        C259C907 84A59AC4 4D1C8056 917CCF38 8788102D 73824C6C


    temp is
                                                8BBA71C2 583F2530
        C259C907 84A59AC4 4D1C8056 917CCF38 8788102D 73824C6C


  ------------

    V = HMAC(K, V) is
                                                11D5D63B E1F01017
        D884CD69 D9334B9E BC01E7BD 8FDF2A8E 52572293 DC21C0E1


    temp is
                           8BBA71C2 583F2530 C259C907 84A59AC4
        4D1C8056 917CCF38 8788102D 73824C6C 11D5D63B E1F01017
        D884CD69 D9334B9E BC01E7BD 8FDF2A8E 52572293 DC21C0E1


----------------------------

  returned_bits is
                           8BBA71C2 583F2530 C259C907 84A59AC4
        4D1C8056 917CCF38 8788102D 73824C6C 11D5D63B E1F01017
```

```
        D884CD69 D9334B9E BC01E7BD 8FDF2A8E 52572293 DC21C0E1


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                          11 D5D63BE1 F01017D8
        84CD69D9 334B9EBC 01E7BD8F DF2A8E52 572293DC 21C0E100


    K = HMAC(K, V || 0x00 || provided_data) is
                                          2D21AC94 992FD82B
        0980D3D5 9551B9D0 7C8D54B2 52B61628 9344F8AC 869ED35B


    V = HMAC(K, V) is
                                          610C34CD BF6F7533
        547F2332 EAC57EE3 1E724FB2 9255566B 59783316 6CD0399F


rnd_val is
                         8BBA71C2 583F2530 C259C907 84A59AC4
        4D1C8056 917CCF38 8788102D 73824C6C 11D5D63B E1F01017
        D884CD69 D9334B9E BC01E7BD 8FDF2A8E 52572293 DC21C0E1


##############################################################

HMAC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                            000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    EntropyInput1 (for Reseed1) =
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                             20212223 24252627


    PersonalizationString =
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    nonce is
                                                20212223 24252627


    personal_str is
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    ------------
```

```
  V || 0x00 || provided_data is
                                                 010101 01010101
      01010101 01010101 01010101 01010101 01010101 01010101
      01000001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
      16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
      2E2F3031 32333435 36202122 23242526 27404142 43444546
      4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
      5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  K = HMAC(K, V || 0x00 || provided_data) is
                                                E48294AE A5171B5D
      6A091450 868B39C4 B14D4E1A 9B29F128 416E1E14 81D10F69


  V = HMAC(K, V) is
                                                40987A58 C3E1346C
      0023F00F 417FA7BD 09C72FED A9738670 993392DF 490E94E2


  ------------

  V || 0x01 || provided_data is
                                                  40987A 58C3E134
      6C0023F0 0F417FA7 BD09C72F EDA97386 70993392 DF490E94
      E2010001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
      16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
      2E2F3031 32333435 36202122 23242526 27404142 43444546
      4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
      5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  K = HMAC(K, V || 0x01 || provided_data) is
                                                65673C34 8E51CFAC
      C410BD20 0249A59A 9D6BAE77 6904271B B1F718DA 1D182042


  V = HMAC(K, V) is
                                                E0F91AC9 9630EEE6
      7CF830CF D5044FEB F55C0C11 5007997A DA11296F C4164A9A


Update (Key, V):

  Key is
                                                65673C34 8E51CFAC
```

C410BD20 0249A59A 9D6BAE77 6904271B B1F718DA 1D182042

V is
E0F91AC9 9630EEE6
7CF830CF D5044FEB F55C0C11 5007997A DA11296F C4164A9A

First call to Generate

****

HMAC_DRBG_Generate

requested_number_of_bits = 512

additional_input is
606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596

Generate FAILED: Reseed is required
****

HMAC_DRBG_Reseed_algorithm

entropy_input is
808182 83848586
8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6

additional_input is
606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596

Seed_Material is
8081 82838485 86878889 8A8B8C8D
8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E

```
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Key is
                                             65673C34 8E51CFAC
        C410BD20 0249A59A 9D6BAE77 6904271B B1F718DA 1D182042


  V is
                                             E0F91AC9 9630EEE6
        7CF830CF D5044FEB F55C0C11 5007997A DA11296F C4164A9A


---------------------------

  Update

    provided_data
                              8081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
          E0F91A C99630EE E67CF830 CFD5044F EBF55C0C 11500799
        7ADA1129 6FC4164A 9A008081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                                             3F5556FC 1A11F18F
        5A33BA25 176B9620 EAD725FA C9BDB742 C14FE54A 98009E8A


    V = HMAC(K, V) is
                                             8B023A87 012038CA
        F38F39C5 F120B858 5668FE6C D263A944 EBEA32F9 020D365C
```

```
    ------------

    V || 0x01 || provided_data is
          8B023A 87012038 CAF38F39 C5F120B8 585668FE 6CD263A9
        44EBEA32 F9020D36 5C018081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
                                            B381388C 1D7CFD56
        5930993B D9269066 5088D9B8 39969B87 F16DB6DF 4E4300D7


    V = HMAC(K, V) is
                                            FA042564 00E342E6
        55F43326 94E3B24C 04FB85BF 878021E4 52E73B8F 46D4BDC6


  Update (Key, V):

    Key is
                                            B381388C 1D7CFD56
        5930993B D9269066 5088D9B8 39969B87 F16DB6DF 4E4300D7


    V is
                                            FA042564 00E342E6
        55F43326 94E3B24C 04FB85BF 878021E4 52E73B8F 46D4BDC6


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                            44D78BBC 3EB67C59
        C22F6C31 003D212A 7837CCD8 4C438B55 150FD013 A8A78FE8
```

```
    temp is
                                                44D78BBC 3EB67C59
        C22F6C31 003D212A 7837CCD8 4C438B55 150FD013 A8A78FE8


  ------------

    V = HMAC(K, V) is
                                                EDEA81C6 72E4B8DD
        C8183886 E69C2E17 7DF574C1 F190DF27 1850F8CE 55EF20B8


    temp is
                           44D78BBC 3EB67C59 C22F6C31 003D212A
        7837CCD8 4C438B55 150FD013 A8A78FE8 EDEA81C6 72E4B8DD
        C8183886 E69C2E17 7DF574C1 F190DF27 1850F8CE 55EF20B8


---------------------------

  returned_bits is
                           44D78BBC 3EB67C59 C22F6C31 003D212A
        7837CCD8 4C438B55 150FD013 A8A78FE8 EDEA81C6 72E4B8DD
        C8183886 E69C2E17 7DF574C1 F190DF27 1850F8CE 55EF20B8


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                             ED EA81C672 E4B8DDC8
        183886E6 9C2E177D F574C1F1 90DF2718 50F8CE55 EF20B800


    K = HMAC(K, V || 0x00 || provided_data) is
                                                D41F6F33 65822170
        50B1F659 28FD6E94 CBC94568 FE3B6B53 389E1E3A 5B49E101
```

```
    V = HMAC(K, V) is
                                                A655C9E7 D133F1CD
        8B1161F2 7D54E75A 7E7C8042 BF74D47F 9FFD60E2 45EBA57E


rnd_val is
                           44D78BBC 3EB67C59 C22F6C31 003D212A
        7837CCD8 4C438B55 150FD013 A8A78FE8 EDEA81C6 72E4B8DD
        C8183886 E69C2E17 7DF574C1 F190DF27 1850F8CE 55EF20B8


------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Seed_Material is
```

```
                            C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Key is
                                            D41F6F33 65822170
        50B1F659 28FD6E94 CBC94568 FE3B6B53 389E1E3A 5B49E101


  V is
                                            A655C9E7 D133F1CD
        8B1161F2 7D54E75A 7E7C8042 BF74D47F 9FFD60E2 45EBA57E


---------------------------

  Update

    provided_data
                            C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
          A655C9 E7D133F1 CD8B1161 F27D54E7 5A7E7C80 42BF74D4
        7F9FFD60 E245EBA5 7E00C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                                            5C2A1146 F81ABA3A
        CFFBF538 A8BDFACC 7BF1FCBC E131B8C5 1138877A 7701B1CD


    V = HMAC(K, V) is
```

```
                                                2E7BF1B5 D13386DA
        220B6E1F BA67B999 D3CC7DDC F939FD50 4D1A1534 6ABC94D2


    ------------

    V || 0x01 || provided_data is
          2E7BF1 B5D13386 DA220B6E 1FBA67B9 99D3CC7D DCF939FD
        504D1A15 346ABC94 D201C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
                                                FBA80545 3E3C9A73
        64585CED BCD29230 FBC93D6F 129D21ED DDF6613B 3A8FF283


    V = HMAC(K, V) is
                                                83647A33 8C153CBA
        F0E49A54 A44FEA66 70CFD7C1 714D4AB3 5F11123D F27B69CF


  Update (Key, V):

    Key is
                                                FBA80545 3E3C9A73
        64585CED BCD29230 FBC93D6F 129D21ED DDF6613B 3A8FF283


    V is
                                                83647A33 8C153CBA
        F0E49A54 A44FEA66 70CFD7C1 714D4AB3 5F11123D F27B69CF


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------
```

```
    V = HMAC(K, V) is
                                                917780DC 0CE9989F
        EE6C0806 D6DA123A 18252947 58D4E1B5 82687231 780A2A9C


    temp is
                                                917780DC 0CE9989F
        EE6C0806 D6DA123A 18252947 58D4E1B5 82687231 780A2A9C


  ------------

    V = HMAC(K, V) is
                                                33F1D156 CCAD3277
        64B29A4C B2690177 AE96EF9E E92AD0C3 40BA0FD1 203C02C6


    temp is
                            917780DC 0CE9989F EE6C0806 D6DA123A
        18252947 58D4E1B5 82687231 780A2A9C 33F1D156 CCAD3277
        64B29A4C B2690177 AE96EF9E E92AD0C3 40BA0FD1 203C02C6


---------------------------

  returned_bits is
                            917780DC 0CE9989F EE6C0806 D6DA123A
        18252947 58D4E1B5 82687231 780A2A9C 33F1D156 CCAD3277
        64B29A4C B2690177 AE96EF9E E92AD0C3 40BA0FD1 203C02C6


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                          33 F1D156CC AD327764
        B29A4CB2 690177AE 96EF9EE9 2AD0C340 BA0FD120 3C02C600
```

```
    K = HMAC(K, V || 0x00 || provided_data) is
                                                AE59C70A 7C60ED49
        8378EA84 5BE97D8F F881E0EA 372E265F A6728429 3E1A46AC


    V = HMAC(K, V) is
                                                E2F04DE3 CE217961
        AE2B2D20 A7BA7C6C 820B5B14 926E5956 AE6DFA2E D1D63993


rnd_val is
                          917780DC 0CE9989F EE6C0806 D6DA123A
        18252947 58D4E1B5 82687231 780A2A9C 33F1D156 CCAD3277
        64B29A4C B2690177 AE96EF9E E92AD0C3 40BA0FD1 203C02C6
```

```
###############################################################

HMAC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                    20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm
```

```
    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                   20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                                                          000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
        63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


  Key is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


--------------------------

  Update

    provided_data
                                                          000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
```

```
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


------------

V || 0x00 || provided_data is
                                                    01010101
    01010101 01010101 01010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 01010101 00000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


K = HMAC(K, V || 0x00 || provided_data) is
    E5675B81 A558502A 38EBFD09 A9753D3E F31388D1 EF8EFC89
    1808526C D64ABF8C 3502D83F 20CE07DB 68F0FA99 22789E4C


V = HMAC(K, V) is
    F70F7FF2 45023323 7528314F A8EBF4D2 50B95649 06F0EF58
    41402759 CD72F743 72924730 1F85C172 1CCB323D 4D8B887F


------------

V || 0x01 || provided_data is
                                                    F70F7FF2
    45023323 7528314F A8EBF4D2 50B95649 06F0EF58 41402759
    CD72F743 72924730 1F85C172 1CCB323D 4D8B887F 01000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


K = HMAC(K, V || 0x01 || provided_data) is
    DE2451BA AF677086 D7C6FBDB 53638AC0 0FE1E7E9 B1CF6A30
    4ABC2005 D1A8A726 77A4E48A B5B3D2D1 35BA251A 764C77C7


V = HMAC(K, V) is
    D6F45225 560DF998 B7006216 D4FFAE27 44D97518 D7585280
```

```
        09A9DCE6 1D50A2FF B4C53C9E D7B405C5 6692FDA8 5523EC69


  Update (Key, V):

    Key is
        DE2451BA AF677086 D7C6FBDB 53638AC0 0FE1E7E9 B1CF6A30
        4ABC2005 D1A8A726 77A4E48A B5B3D2D1 35BA251A 764C77C7


    V is
        D6F45225 560DF998 B7006216 D4FFAE27 44D97518 D7585280
        09A9DCE6 1D50A2FF B4C53C9E D7B405C5 6692FDA8 5523EC69


---------------------------------------------------------------

First call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        FF08EED5 0F04D543 FAE5C9C8 FB31D784 89FE82C9 F77F60ED
        A91A86E5 5EFADB6B 3431BF08 86BC1A63 C44FAD9B 9715C092


    temp is
        FF08EED5 0F04D543 FAE5C9C8 FB31D784 89FE82C9 F77F60ED
        A91A86E5 5EFADB6B 3431BF08 86BC1A63 C44FAD9B 9715C092


  ------------

    V = HMAC(K, V) is
        6C24AA45 76A94444 23BF6B55 8CEA09FD BADCE2A5 C05BD480
        F8DEF079 75826DAA 53EF71EC 7E28CB38 1D10A7B0 C09A1D15
```

```
    temp is
        FF08EED5 0F04D543 FAE5C9C8 FB31D784 89FE82C9 F77F60ED
        A91A86E5 5EFADB6B 3431BF08 86BC1A63 C44FAD9B 9715C092
        6C24AA45 76A94444 23BF6B55 8CEA09FD BADCE2A5 C05BD480
        F8DEF079 75826DAA 53EF71EC 7E28CB38 1D10A7B0 C09A1D15


---------------------------

  returned_bits is
        FF08EED5 0F04D543 FAE5C9C8 FB31D784 89FE82C9 F77F60ED
        A91A86E5 5EFADB6B 3431BF08 86BC1A63 C44FAD9B 9715C092
        6C24AA45 76A94444 23BF6B55 8CEA09FD BADCE2A5 C05BD480
        F8DEF079 75826DAA 53EF71EC 7E28CB38 1D10A7B0 C09A1D15


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                            6C
        24AA4576 A9444423 BF6B558C EA09FDBA DCE2A5C0 5BD480F8
        DEF07975 826DAA53 EF71EC7E 28CB381D 10A7B0C0 9A1D1500


    K = HMAC(K, V || 0x00 || provided_data) is
        18ABF78C 40CBE6E8 600D08EA F18D1BF7 0843B2B0 7A15B490
        3E94462E 7F56DBB5 C5138A34 28860A33 0FDCF44E CA1CCCF4


    V = HMAC(K, V) is
        DD77E6C8 006B2F77 53357544 3B15471A 32442ACF 231FD04B
        A91F6650 4735CE0F 51BEC2CE 3D9A9B6E 0719E730 63B93FAA


rnd_val is
        FF08EED5 0F04D543 FAE5C9C8 FB31D784 89FE82C9 F77F60ED
        A91A86E5 5EFADB6B 3431BF08 86BC1A63 C44FAD9B 9715C092
        6C24AA45 76A94444 23BF6B55 8CEA09FD BADCE2A5 C05BD480
        F8DEF079 75826DAA 53EF71EC 7E28CB38 1D10A7B0 C09A1D15
```

```
------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        1B3D9FAB 561E4C87 B78EABAC 0773E0CE 6AF93E9B B67B7719
        C6176752 7000351D D7D6910F 3AA375B7 70D38CF2 0270CBB1


    temp is
        1B3D9FAB 561E4C87 B78EABAC 0773E0CE 6AF93E9B B67B7719
        C6176752 7000351D D7D6910F 3AA375B7 70D38CF2 0270CBB1


  ------------

    V = HMAC(K, V) is
        147AE249 F9DADB7A 5B4B6380 12C14ECA DCA32FBD DA8ED4BF
        73586EE5 DC9D543F 210437D4 866F7A2E FD326447 CAF4F68C


    temp is
        1B3D9FAB 561E4C87 B78EABAC 0773E0CE 6AF93E9B B67B7719
        C6176752 7000351D D7D6910F 3AA375B7 70D38CF2 0270CBB1
        147AE249 F9DADB7A 5B4B6380 12C14ECA DCA32FBD DA8ED4BF
        73586EE5 DC9D543F 210437D4 866F7A2E FD326447 CAF4F68C


---------------------------

  returned_bits is
        1B3D9FAB 561E4C87 B78EABAC 0773E0CE 6AF93E9B B67B7719
        C6176752 7000351D D7D6910F 3AA375B7 70D38CF2 0270CBB1
        147AE249 F9DADB7A 5B4B6380 12C14ECA DCA32FBD DA8ED4BF
```

```
        73586EE5 DC9D543F 210437D4 866F7A2E FD326447 CAF4F68C


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                              14
        7AE249F9 DADB7A5B 4B638012 C14ECADC A32FBDDA 8ED4BF73
        586EE5DC 9D543F21 0437D486 6F7A2EFD 326447CA F4F68C00


    K = HMAC(K, V || 0x00 || provided_data) is
        E53CFF8F DA284692 96F3D2D6 88164204 CC767F00 2107AEB6
        9EB94ACB 0AC7C5C5 AD431FDF D7367E09 2C0E78B5 E59964AA


    V = HMAC(K, V) is
        D24F1437 9D37B5AF 5EA4FF2D B78051D6 609007A7 86E2579C
        690997DF 3E82B760 437A98E4 59F10497 9C6A6209 D56F72FD


rnd_val is
        1B3D9FAB 561E4C87 B78EABAC 0773E0CE 6AF93E9B B67B7719
        C6176752 7000351D D7D6910F 3AA375B7 70D38CF2 0270CBB1
        147AE249 F9DADB7A 5B4B6380 12C14ECA DCA32FBD DA8ED4BF
        73586EE5 DC9D543F 210437D4 866F7A2E FD326447 CAF4F68C


##############################################################

HMAC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
```

```
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                              808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                              C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                    20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput1 =
                              606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    AdditionalInput2 =
                              A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


##############################################################
```

```
**************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                              000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                    20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                                                          000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
        63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


  Key is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                                                          000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
```

```
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


------------

V || 0x00 || provided_data is
                                                    01010101
    01010101 01010101 01010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 01010101 00000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


K = HMAC(K, V || 0x00 || provided_data) is
    E5675B81 A558502A 38EBFD09 A9753D3E F31388D1 EF8EFC89
    1808526C D64ABF8C 3502D83F 20CE07DB 68F0FA99 22789E4C


V = HMAC(K, V) is
    F70F7FF2 45023323 7528314F A8EBF4D2 50B95649 06F0EF58
    41402759 CD72F743 72924730 1F85C172 1CCB323D 4D8B887F


------------

V || 0x01 || provided_data is
                                                    F70F7FF2
    45023323 7528314F A8EBF4D2 50B95649 06F0EF58 41402759
    CD72F743 72924730 1F85C172 1CCB323D 4D8B887F 01000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


K = HMAC(K, V || 0x01 || provided_data) is
    DE2451BA AF677086 D7C6FBDB 53638AC0 0FE1E7E9 B1CF6A30
    4ABC2005 D1A8A726 77A4E48A B5B3D2D1 35BA251A 764C77C7
```

```
    V = HMAC(K, V) is
        D6F45225 560DF998 B7006216 D4FFAE27 44D97518 D7585280
        09A9DCE6 1D50A2FF B4C53C9E D7B405C5 6692FDA8 5523EC69


  Update (Key, V):

    Key is
        DE2451BA AF677086 D7C6FBDB 53638AC0 0FE1E7E9 B1CF6A30
        4ABC2005 D1A8A726 77A4E48A B5B3D2D1 35BA251A 764C77C7


    V is
        D6F45225 560DF998 B7006216 D4FFAE27 44D97518 D7585280
        09A9DCE6 1D50A2FF B4C53C9E D7B405C5 6692FDA8 5523EC69


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is
                           606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                           606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

```
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


------------

V || 0x00 || provided_data is
                      D6F45225 560DF998 B7006216 D4FFAE27
    44D97518 D7585280 09A9DCE6 1D50A2FF B4C53C9E D7B405C5
    6692FDA8 5523EC69 00606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x00 || provided_data) is
    5BA16AA7 BD2432F2 F1553EFA 42AFFEB9 6E429977 94C4F924
    F924BD53 C2571A12 2164A46A 9D760495 F2B4E83D 484C047A


V = HMAC(K, V) is
    71DA2378 FC0B0FB7 CBEB0FC0 252EE2E2 443DF2B2 CF9EE746
    94886FC9 45D7996E 85CFFEDC C9DBCF44 3AEE92FF BEC95804


------------

V || 0x01 || provided_data is
                      71DA2378 FC0B0FB7 CBEB0FC0 252EE2E2
    443DF2B2 CF9EE746 94886FC9 45D7996E 85CFFEDC C9DBCF44
    3AEE92FF BEC95804 01606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x01 || provided_data) is
    3089EB25 D72DB470 D0BC6DEA BA31774E 0E4C8C50 E95D8B34
    6008395E BC21568A E7A2E89F A6507D97 591887EB 1D94D037


V = HMAC(K, V) is
    A22922DE 91403C5A 2A65EF5E 53586775 96A3B2C7 CA75F99F
    C90789BD 0B7A4444 A361FE0B B058B244 5B79E361 BF5E70D9
```

```
  ------------

    V = HMAC(K, V) is
        52DCD4A4 07EE8506 D9CFF5B0 1F938959 73D45E58 52AFA29A
        8F11ADFC CDF21274 57C3BAB6 D6A0EC28 7DAB83C6 1011D311


    temp is
        52DCD4A4 07EE8506 D9CFF5B0 1F938959 73D45E58 52AFA29A
        8F11ADFC CDF21274 57C3BAB6 D6A0EC28 7DAB83C6 1011D311


  ------------

    V = HMAC(K, V) is
        D3CC40D6 FE744874 4A13E811 ABE42206 9118240B 09B4E330
        FB7EB1E1 C1871B73 92C5B7EF A753EDA2 260D41ED A4B0A8EE


    temp is
        52DCD4A4 07EE8506 D9CFF5B0 1F938959 73D45E58 52AFA29A
        8F11ADFC CDF21274 57C3BAB6 D6A0EC28 7DAB83C6 1011D311
        D3CC40D6 FE744874 4A13E811 ABE42206 9118240B 09B4E330
        FB7EB1E1 C1871B73 92C5B7EF A753EDA2 260D41ED A4B0A8EE


---------------------------

  returned_bits is
        52DCD4A4 07EE8506 D9CFF5B0 1F938959 73D45E58 52AFA29A
        8F11ADFC CDF21274 57C3BAB6 D6A0EC28 7DAB83C6 1011D311
        D3CC40D6 FE744874 4A13E811 ABE42206 9118240B 09B4E330
        FB7EB1E1 C1871B73 92C5B7EF A753EDA2 260D41ED A4B0A8EE


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                           606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE

V || 0x00 || provided_data is
D3CC40D6 FE744874 4A13E811 ABE42206
9118240B 09B4E330 FB7EB1E1 C1871B73 92C5B7EF A753EDA2
260D41ED A4B0A8EE 00606162 63646566 6768696A 6B6C6D6E
6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE

K = HMAC(K, V || 0x00 || provided_data) is
771D7ECC 7123E344 3ADB89D1 B603E562 388ED87D 0AEB880C
E39C5C7A 2A89E4D8 204CDA7D 9F004C3B 6667B4D4 E8618AB8

V = HMAC(K, V) is
3D063B7D AAD0ADB7 0C47A2BF 1B230784 DA404A4C 12B938D7
62B69E88 79B63A71 53501820 15D3228D 2E06722D 79BD737E

V || 0x01 || provided_data is
3D063B7D AAD0ADB7 0C47A2BF 1B230784
DA404A4C 12B938D7 62B69E88 79B63A71 53501820 15D3228D
2E06722D 79BD737E 01606162 63646566 6768696A 6B6C6D6E
6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE

K = HMAC(K, V || 0x01 || provided_data) is
FDB20FD7 B77F2156 4502583E AC235F3B 21C20A19 4560D1BD
FDC2C11F FB5E080E B489EF00 21B03C0A 40408DA1 111FB993

V = HMAC(K, V) is
27CE0060 D10422FB 7B643CE0 629E9DB5 6A1DE24B C240E025
417CDA29 8C34D886 FA41695C 9FD4364B A8E8044A 6CD95873

```
rnd_val is
        52DCD4A4 07EE8506 D9CFF5B0 1F938959 73D45E58 52AFA29A
        8F11ADFC CDF21274 57C3BAB6 D6A0EC28 7DAB83C6 1011D311
        D3CC40D6 FE744874 4A13E811 ABE42206 9118240B 09B4E330
        FB7EB1E1 C1871B73 92C5B7EF A753EDA2 260D41ED A4B0A8EE


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    ------------

    V || 0x00 || provided_data is
                          27CE0060 D10422FB 7B643CE0 629E9DB5
        6A1DE24B C240E025 417CDA29 8C34D886 FA41695C 9FD4364B
        A8E8044A 6CD95873 00A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
```

```
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  K = HMAC(K, V || 0x00 || provided_data) is
      517B62B9 F5FFA061 2AEBEAAA 197F0182 81A2A93A E972E47A
      874D25CC D2968468 9513584D 05A59A34 1A063F05 F49F628A


  V = HMAC(K, V) is
      8E003226 D59AC8C3 057114CC 583643DC 5B30CB9B AB9CE09E
      CB0FCBA5 E9D3767E 40B57B67 C7B9B627 371D7EF0 EBE01D9E


  ------------

  V || 0x01 || provided_data is
                       8E003226 D59AC8C3 057114CC 583643DC
      5B30CB9B AB9CE09E CB0FCBA5 E9D3767E 40B57B67 C7B9B627
      371D7EF0 EBE01D9E 01A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  K = HMAC(K, V || 0x01 || provided_data) is
      B403259D 1B927583 94D8AF63 84D8548E C962457B 14005AB0
      B3C49530 77365A85 895CE8A9 247B3EA1 32308830 FEBBE984


  V = HMAC(K, V) is
      89BC4ADF F69AC101 B3B83AA8 4BBF0F0E 3880BFA4 97C19D27
      39C1D876 47225AF9 DD545E9F 9DED4011 E2D2F74E 322D1D34


------------

  V = HMAC(K, V) is
      A8E2404D 14F6AE1F A9B66686 3D4C0265 2B806170 3F958798
      870032C9 D6D3CA10 302DC1C5 FE0F5B21 1F760EFB 4177684B


  temp is
      A8E2404D 14F6AE1F A9B66686 3D4C0265 2B806170 3F958798
```

```
        870032C9 D6D3CA10 302DC1C5 FE0F5B21 1F760EFB 4177684B


  ------------

    V = HMAC(K, V) is
        A5056D84 B35B9FCC E4C44818 080346AD CC9AC610 E4719575
        B0D1713D DF30C671 99EA0A17 B1592E9B 75390462 D3059C35


    temp is
        A8E2404D 14F6AE1F A9B66686 3D4C0265 2B806170 3F958798
        870032C9 D6D3CA10 302DC1C5 FE0F5B21 1F760EFB 4177684B
        A5056D84 B35B9FCC E4C44818 080346AD CC9AC610 E4719575
        B0D1713D DF30C671 99EA0A17 B1592E9B 75390462 D3059C35


---------------------------

  returned_bits is
        A8E2404D 14F6AE1F A9B66686 3D4C0265 2B806170 3F958798
        870032C9 D6D3CA10 302DC1C5 FE0F5B21 1F760EFB 4177684B
        A5056D84 B35B9FCC E4C44818 080346AD CC9AC610 E4719575
        B0D1713D DF30C671 99EA0A17 B1592E9B 75390462 D3059C35


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    ------------

    V || 0x00 || provided_data is
                          A5056D84 B35B9FCC E4C44818 080346AD
        CC9AC610 E4719575 B0D1713D DF30C671 99EA0A17 B1592E9B
        75390462 D3059C35 00A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
```

```
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    K = HMAC(K, V || 0x00 || provided_data) is
        C1BE3D41 76D35248 9193251F 10D37B56 65045FA1 013AEF3F
        5A37A984 8FD2387A 59B33F9B 575F73A5 192FDCC7 3B0FA53E


    V = HMAC(K, V) is
        C5DE0CEC 4C36EDB0 228BCCC9 9AA5EBC9 9286C1A9 3735E767
        10AF8539 A99F3452 FD9DB65A 2F4A5CA1 F517B0D5 31824731


    ------------

    V || 0x01 || provided_data is
                          C5DE0CEC 4C36EDB0 228BCCC9 9AA5EBC9
        9286C1A9 3735E767 10AF8539 A99F3452 FD9DB65A 2F4A5CA1
        F517B0D5 31824731 01A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    K = HMAC(K, V || 0x01 || provided_data) is
        BB28D41B A296C891 577EBB93 4C0E5275 24BC193A 4D7D710A
        9E265304 82B810FF C829B71C 13A933D8 A4EE193D 9DDDC831


    V = HMAC(K, V) is
        5B6628DF 4BBE2767 1ECED5EF 03ECEDA7 FB399DA3 E756658F
        8F86A6F0 D115F17E A973BEEF B2BE905B 9115AACD EE5AB92A


rnd_val is
        A8E2404D 14F6AE1F A9B66686 3D4C0265 2B806170 3F958798
        870032C9 D6D3CA10 302DC1C5 FE0F5B21 1F760EFB 4177684B
        A5056D84 B35B9FCC E4C44818 080346AD CC9AC610 E4719575
        B0D1713D DF30C671 99EA0A17 B1592E9B 75390462 D3059C35


################################################################
```

```
HMAC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                    20212223 24252627 28292A2B


    PersonalizationString =
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    AdditionalInput = <empty>

##################################################################
```

```
**************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                  20212223 24252627 28292A2B


    personal_str is
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                      0001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  Key is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
```

```
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                    0001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    ------------

    V || 0x00 || provided_data is
                  010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01000001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    K = HMAC(K, V || 0x00 || provided_data) is
        759FC2E2 D33686FF B43AB4F9 27A9E74D 7C30CE89 05C5AEDF
        7A84FF76 479BD8B6 D930A267 6D76D9BC B2F420A3 4B76654A


    V = HMAC(K, V) is
        D873522C B0FC9099 33B67222 16975EA8 B7EA9349 6647EB8B
        BC9A0873 5DE801C3 6D01ABE8 52B764E9 9514935A 9567A39D
```

```
    ------------

    V || 0x01 || provided_data is
                   D87352 2CB0FC90 9933B672 2216975E A8B7EA93
        496647EB 8BBC9A08 735DE801 C36D01AB E852B764 E9951493
        5A9567A3 9D010001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    K = HMAC(K, V || 0x01 || provided_data) is
        085987EF 2F1BD2B4 01CF188A EF3E3428 9AB194F5 803FB7E5
        2A0072E2 A4B86949 38AD044F BEDCEAAD EB9618C7 D7393448


    V = HMAC(K, V) is
        8E065B64 B430910B 4950528A F23A9FA2 866F8DAA 9106B72E
        38BA0B93 D033B851 04485F29 D1AD7EB6 FF1643D6 9129654D


  Update (Key, V):

    Key is
        085987EF 2F1BD2B4 01CF188A EF3E3428 9AB194F5 803FB7E5
        2A0072E2 A4B86949 38AD044F BEDCEAAD EB9618C7 D7393448


    V is
        8E065B64 B430910B 4950528A F23A9FA2 866F8DAA 9106B72E
        38BA0B93 D033B851 04485F29 D1AD7EB6 FF1643D6 9129654D


---------------------------------------------------------------

First call to Generate

***************************************************************
```

```
HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        03AB8BCE 4D1DBBB6 36C5C5B7 E1C58499 FEB1C619 CDD11D35
        CD6CF6BB 8F20EF27 B6F5F905 4FF900DB 9EBF7BF3 0ED4DCBB


    temp is
        03AB8BCE 4D1DBBB6 36C5C5B7 E1C58499 FEB1C619 CDD11D35
        CD6CF6BB 8F20EF27 B6F5F905 4FF900DB 9EBF7BF3 0ED4DCBB


  ------------

    V = HMAC(K, V) is
        BC8D5B51 C965EA22 6FFEE2CA 5AB2EFD0 0754DC32 F357BF7A
        E42275E0 F7704DC4 4E50A522 0AD05AB6 98A22640 AC634829


    temp is
        03AB8BCE 4D1DBBB6 36C5C5B7 E1C58499 FEB1C619 CDD11D35
        CD6CF6BB 8F20EF27 B6F5F905 4FF900DB 9EBF7BF3 0ED4DCBB
        BC8D5B51 C965EA22 6FFEE2CA 5AB2EFD0 0754DC32 F357BF7A
        E42275E0 F7704DC4 4E50A522 0AD05AB6 98A22640 AC634829


---------------------------

  returned_bits is
        03AB8BCE 4D1DBBB6 36C5C5B7 E1C58499 FEB1C619 CDD11D35
        CD6CF6BB 8F20EF27 B6F5F905 4FF900DB 9EBF7BF3 0ED4DCBB
        BC8D5B51 C965EA22 6FFEE2CA 5AB2EFD0 0754DC32 F357BF7A
        E42275E0 F7704DC4 4E50A522 0AD05AB6 98A22640 AC634829


  call Update(additional_input, K, V)
---------------------------

  Update
```

```
    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                                BC
        8D5B51C9 65EA226F FEE2CA5A B2EFD007 54DC32F3 57BF7AE4
        2275E0F7 704DC44E 50A5220A D05AB698 A22640AC 63482900


    K = HMAC(K, V || 0x00 || provided_data) is
        6FF4623B 22742731 AD3855C1 446809EA 9EC2015B 75140D0C
        C47CFEAD 2F520948 78BFB048 F4FC4C8A 47E52D96 64ADF033


    V = HMAC(K, V) is
        0D61885B 765A2E62 04BC92F5 BFBF4FA5 4ABB7668 245399A0
        B87B4771 0E75CF2A D8A089EF 7827EF56 19CEF3AB 668708C1


rnd_val is
        03AB8BCE 4D1DBBB6 36C5C5B7 E1C58499 FEB1C619 CDD11D35
        CD6CF6BB 8F20EF27 B6F5F905 4FF900DB 9EBF7BF3 0ED4DCBB
        BC8D5B51 C965EA22 6FFEE2CA 5AB2EFD0 0754DC32 F357BF7A
        E42275E0 F7704DC4 4E50A522 0AD05AB6 98A22640 AC634829


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        B907E771 44FD55A5 4E9BA1A6 A0EED0AA C780020C 41A15DD8
        9A6C1638 30BA1D09 4E6A1710 0FF71EE3 0A96E1EE 04D2A966
```

```
    temp is
        B907E771 44FD55A5 4E9BA1A6 A0EED0AA C780020C 41A15DD8
        9A6C1638 30BA1D09 4E6A1710 0FF71EE3 0A96E1EE 04D2A966


  ------------

    V = HMAC(K, V) is
        03832A4E 404F1966 C2B5F4CB 61B9927E 8D12AC1E 1A24CF23
        88C14E8E C96C3518 1EAEE32A AA46330D EAAFE5E7 CE783C74


    temp is
        B907E771 44FD55A5 4E9BA1A6 A0EED0AA C780020C 41A15DD8
        9A6C1638 30BA1D09 4E6A1710 0FF71EE3 0A96E1EE 04D2A966
        03832A4E 404F1966 C2B5F4CB 61B9927E 8D12AC1E 1A24CF23
        88C14E8E C96C3518 1EAEE32A AA46330D EAAFE5E7 CE783C74


---------------------------

  returned_bits is
        B907E771 44FD55A5 4E9BA1A6 A0EED0AA C780020C 41A15DD8
        9A6C1638 30BA1D09 4E6A1710 0FF71EE3 0A96E1EE 04D2A966
        03832A4E 404F1966 C2B5F4CB 61B9927E 8D12AC1E 1A24CF23
        88C14E8E C96C3518 1EAEE32A AA46330D EAAFE5E7 CE783C74


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                            03
        832A4E40 4F1966C2 B5F4CB61 B9927E8D 12AC1E1A 24CF2388
        C14E8EC9 6C35181E AEE32AAA 46330DEA AFE5E7CE 783C7400


    K = HMAC(K, V || 0x00 || provided_data) is
        EC249919 FFD99A78 321BBC13 DD7C3718 DC349F49 A255AC62
```

```
        D691306F B5BAFBDD 035BEADD 49D42B0C 7D4EA325 A0649B04


    V = HMAC(K, V) is
        5CE2AAC0 55EA1A0D 199DAF5C F250EB3E E8711ED5 5D2589E3
        AED9FF62 9F47199D 7EB1669E 7CE6CD51 90C528D5 63D72107


rnd_val is
        B907E771 44FD55A5 4E9BA1A6 A0EED0AA C780020C 41A15DD8
        9A6C1638 30BA1D09 4E6A1710 0FF71EE3 0A96E1EE 04D2A966
        03832A4E 404F1966 C2B5F4CB 61B9927E 8D12AC1E 1A24CF23
        88C14E8E C96C3518 1EAEE32A AA46330D EAAFE5E7 CE783C74


################################################################

HMAC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E
```

```
    Nonce =
                                  20212223 24252627 28292A2B


    PersonalizationString =
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    AdditionalInput1 =
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    AdditionalInput2 =
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


##################################################################

******************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                  20212223 24252627 28292A2B
```

```
    personal_str is
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                      0001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  Key is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                      0001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
```

```
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


------------

V || 0x00 || provided_data is
                010101 01010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 01010101 01010101
    01010101 01000001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


K = HMAC(K, V || 0x00 || provided_data) is
    759FC2E2 D33686FF B43AB4F9 27A9E74D 7C30CE89 05C5AEDF
    7A84FF76 479BD8B6 D930A267 6D76D9BC B2F420A3 4B76654A


V = HMAC(K, V) is
    D873522C B0FC9099 33B67222 16975EA8 B7EA9349 6647EB8B
    BC9A0873 5DE801C3 6D01ABE8 52B764E9 9514935A 9567A39D


------------

V || 0x01 || provided_data is
                D87352 2CB0FC90 9933B672 2216975E A8B7EA93
    496647EB 8BBC9A08 735DE801 C36D01AB E852B764 E9951493
    5A9567A3 9D010001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
```

```
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    K = HMAC(K, V || 0x01 || provided_data) is
        085987EF 2F1BD2B4 01CF188A EF3E3428 9AB194F5 803FB7E5
        2A0072E2 A4B86949 38AD044F BEDCEAAD EB9618C7 D7393448


    V = HMAC(K, V) is
        8E065B64 B430910B 4950528A F23A9FA2 866F8DAA 9106B72E
        38BA0B93 D033B851 04485F29 D1AD7EB6 FF1643D6 9129654D


  Update (Key, V):

    Key is
        085987EF 2F1BD2B4 01CF188A EF3E3428 9AB194F5 803FB7E5
        2A0072E2 A4B86949 38AD044F BEDCEAAD EB9618C7 D7393448


    V is
        8E065B64 B430910B 4950528A F23A9FA2 866F8DAA 9106B72E
        38BA0B93 D033B851 04485F29 D1AD7EB6 FF1643D6 9129654D


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------
```

```
Update

  provided_data
                          606162 63646566 6768696A 6B6C6D6E
      6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
      8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
      9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
      B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


  ------------

  V || 0x00 || provided_data is
                        8E065B64 B430910B 4950528A F23A9FA2
      866F8DAA 9106B72E 38BA0B93 D033B851 04485F29 D1AD7EB6
      FF1643D6 9129654D 00606162 63646566 6768696A 6B6C6D6E
      6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
      8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
      9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
      B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


  K = HMAC(K, V || 0x00 || provided_data) is
      40F45F9B DB63CE2D C49A99E2 22EB624D 1392BF1E 31F6BE87
      E4FBA82F 7BB4F4B6 1A26C174 B21EBBB7 843E7378 31F2D481


  V = HMAC(K, V) is
      BB1F9B0F 08693EE1 512D9E7E 94CED7F8 4CCA5D1F 07B74BCB
      4D988A48 4E6CABDD 0BDBCAA7 0073F85D D3B981FE 6F0588DE


  ------------

  V || 0x01 || provided_data is
                        BB1F9B0F 08693EE1 512D9E7E 94CED7F8
      4CCA5D1F 07B74BCB 4D988A48 4E6CABDD 0BDBCAA7 0073F85D
      D3B981FE 6F0588DE 01606162 63646566 6768696A 6B6C6D6E
      6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
      8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
      9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
      B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


  K = HMAC(K, V || 0x01 || provided_data) is
```

```
        F43A39BD 8EBD1620 2FD2A304 EE4D3F5A C29A8855 98BD4370
        E3EC8A77 8F45378E DFF8936C D073D36A 6AC105FF A2BE704C


    V = HMAC(K, V) is
        F2B03FB9 BA930DE3 71C08DD4 D1D26541 2A7AC84A B2314D89
        2C30AFC9 BA96423A CD267E78 F84671DE 43B61E79 6C6687D1


  ------------

    V = HMAC(K, V) is
        3918F6DF 5E50B922 CDD7D0FB 87967822 33141EEE 8A14AB69
        B2B3970A F1D30D9F 344225A1 5384869B 208ADB4B 5674C6DA


    temp is
        3918F6DF 5E50B922 CDD7D0FB 87967822 33141EEE 8A14AB69
        B2B3970A F1D30D9F 344225A1 5384869B 208ADB4B 5674C6DA


  ------------

    V = HMAC(K, V) is
        0C9ED74F 56BC8FB4 8145FB36 90FDA956 1AD6038A 5B1E0BA2
        AC09FCC5 D35E5898 3570F37C CE516D76 407A2342 F802CCB9


    temp is
        3918F6DF 5E50B922 CDD7D0FB 87967822 33141EEE 8A14AB69
        B2B3970A F1D30D9F 344225A1 5384869B 208ADB4B 5674C6DA
        0C9ED74F 56BC8FB4 8145FB36 90FDA956 1AD6038A 5B1E0BA2
        AC09FCC5 D35E5898 3570F37C CE516D76 407A2342 F802CCB9


---------------------------

  returned_bits is
        3918F6DF 5E50B922 CDD7D0FB 87967822 33141EEE 8A14AB69
        B2B3970A F1D30D9F 344225A1 5384869B 208ADB4B 5674C6DA
        0C9ED74F 56BC8FB4 8145FB36 90FDA956 1AD6038A 5B1E0BA2
        AC09FCC5 D35E5898 3570F37C CE516D76 407A2342 F802CCB9


  call Update(additional_input, K, V)
---------------------------
```

Update

provided_data
                        606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE

V || 0x00 || provided_data is
                    0C9ED74F 56BC8FB4 8145FB36 90FDA956
    1AD6038A 5B1E0BA2 AC09FCC5 D35E5898 3570F37C CE516D76
    407A2342 F802CCB9 00606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE

K = HMAC(K, V || 0x00 || provided_data) is
    B28EF895 0D1F0F9E 7528FE77 60ADBCFD 3EE1100C 1DE8173B
    D09B070B 44526378 83FC310B 32FA6C16 700AA4FE 61A0A397

V = HMAC(K, V) is
    0A4B15DE 6B992614 D3502202 23171C33 DD4553F1 C068F00D
    59D3FCB8 73635241 79C956AA 281FFD6B 350C8ECB 35EB71A4

V || 0x01 || provided_data is
                    0A4B15DE 6B992614 D3502202 23171C33
    DD4553F1 C068F00D 59D3FCB8 73635241 79C956AA 281FFD6B
    350C8ECB 35EB71A4 01606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE

K = HMAC(K, V || 0x01 || provided_data) is

```
        1D99B92D E9846C92 22D0EE91 E7423C62 C165B662 B6B29D59
        8D0AAA82 D354FC3F C3AC2D65 E92D43A5 012A494D D8995AEB


    V = HMAC(K, V) is
        A86E8815 2A533A42 829B9F7E 2589A79B B4FBACF9 51349F14
        FF9D2538 0669EB08 683F1B0F BE45F5FF D3DB2A6D 5412522B


rnd_val is
        3918F6DF 5E50B922 CDD7D0FB 87967822 33141EEE 8A14AB69
        B2B3970A F1D30D9F 344225A1 5384869B 208ADB4B 5674C6DA
        0C9ED74F 56BC8FB4 8145FB36 90FDA956 1AD6038A 5B1E0BA2
        AC09FCC5 D35E5898 3570F37C CE516D76 407A2342 F802CCB9


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E
```

```
  ------------

  V || 0x00 || provided_data is
                        A86E8815 2A533A42 829B9F7E 2589A79B
      B4FBACF9 51349F14 FF9D2538 0669EB08 683F1B0F BE45F5FF
      D3DB2A6D 5412522B 00A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  K = HMAC(K, V || 0x00 || provided_data) is
      D8618675 35A0AC79 ECA3C968 6BDE77B8 BF7D52A0 EE50D8D3
      B089D770 8B60F0C3 72234ACA 2B791B75 5B31E7AC E515336B


  V = HMAC(K, V) is
      3072E24D 08F157E1 F0446641 BDCEAB60 1BBE5209 059DE17E
      98927025 BBCF3B82 BB82B0BF 7440DBC6 7C891877 9D86858D


  ------------

  V || 0x01 || provided_data is
                        3072E24D 08F157E1 F0446641 BDCEAB60
      1BBE5209 059DE17E 98927025 BBCF3B82 BB82B0BF 7440DBC6
      7C891877 9D86858D 01A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  K = HMAC(K, V || 0x01 || provided_data) is
      E070149D 96AD5AE2 CAED9BC9 3A875FD8 B6291122 58E92889
      CDC186B7 A843F3F6 848C8502 CC688B04 3556C54D 3CD5A28A


  V = HMAC(K, V) is
      9FA62895 A425AD21 F19FFC95 6341DEAB 7B940EBE E5A2E475
      0BC6EBAD E3F1793A 41422A7E 078B98D8 C740D638 E0C6526A


------------
```

```
    V = HMAC(K, V) is
        BFFE3657 BE463125 BC247C54 B3A5B608 A7198008 78F5058A
        34ECAC69 2837F275 F0449FB1 5B04C2F1 2F12A189 87FF1E5B


    temp is
        BFFE3657 BE463125 BC247C54 B3A5B608 A7198008 78F5058A
        34ECAC69 2837F275 F0449FB1 5B04C2F1 2F12A189 87FF1E5B


  ------------

    V = HMAC(K, V) is
        10370288 FF0074CA 6D99DD0B 5912AE3A B2875B18 201626E6
        1D2E3A0C FF95F45E 49B02FB8 CFBDE860 0B222872 82E01DF3


    temp is
        BFFE3657 BE463125 BC247C54 B3A5B608 A7198008 78F5058A
        34ECAC69 2837F275 F0449FB1 5B04C2F1 2F12A189 87FF1E5B
        10370288 FF0074CA 6D99DD0B 5912AE3A B2875B18 201626E6
        1D2E3A0C FF95F45E 49B02FB8 CFBDE860 0B222872 82E01DF3


---------------------------

  returned_bits is
        BFFE3657 BE463125 BC247C54 B3A5B608 A7198008 78F5058A
        34ECAC69 2837F275 F0449FB1 5B04C2F1 2F12A189 87FF1E5B
        10370288 FF0074CA 6D99DD0B 5912AE3A B2875B18 201626E6
        1D2E3A0C FF95F45E 49B02FB8 CFBDE860 0B222872 82E01DF3


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E
```

```
    ------------

    V || 0x00 || provided_data is
                          10370288 FF0074CA 6D99DD0B 5912AE3A
        B2875B18 201626E6 1D2E3A0C FF95F45E 49B02FB8 CFBDE860
        0B222872 82E01DF3 00A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    K = HMAC(K, V || 0x00 || provided_data) is
        0E744D90 FE08D1BD 53AC0DEE E23659C5 A07BCC3E FE9FA961
        63352A8C 17ED67D3 90FE4950 C7DA111B 2555A82A D3BFCE5D


    V = HMAC(K, V) is
        12677BF7 2691959E 9C09F5F2 AA618376 97E0E4C1 51873C3A
        BAFF4230 FCE4F512 19B29624 9348EFC8 A1130840 4625EA69


    ------------

    V || 0x01 || provided_data is
                          12677BF7 2691959E 9C09F5F2 AA618376
        97E0E4C1 51873C3A BAFF4230 FCE4F512 19B29624 9348EFC8
        A1130840 4625EA69 01A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    K = HMAC(K, V || 0x01 || provided_data) is
        0B77DD3B ED4BFFE4 F6494C1B 7522F2AB 93EE1338 ED89CFC1
        6CF81218 4E133482 A04F7007 BF4A4D85 FA138745 1B6D8BE3


    V = HMAC(K, V) is
        020E9776 277D8B88 4E16E40D 7B7AF404 4952A9B9 5DA33382
        2ADB6417 D726E901 46142F6E B388A3A3 7A669D27 9432DACD


rnd_val is
```

BFFE3657 BE463125 BC247C54 B3A5B608 A7198008 78F5058A
34ECAC69 2837F275 F0449FB1 5B04C2F1 2F12A189 87FF1E5B
10370288 FF0074CA 6D99DD0B 5912AE3A B2875B18 201626E6
1D2E3A0C FF95F45E 49B02FB8 CFBDE860 0B222872 82E01DF3

##

HMAC_DRBG

Requested Security Strength = 192

Requested Hash Algorithm = SHA-384

prediction_resistance_flag = "ENABLED"
EntropyInput =
000102 03040506 0708090A 0B0C0D0E
0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E

EntropyInput1 (for Reseed1) =
808182 83848586 8788898A 8B8C8D8E
8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE

EntropyInput2 (for Reseed2) =
C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E

Nonce =
20212223 24252627 28292A2B

PersonalizationString = <empty>

AdditionalInput = <empty>

```
################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                              000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                    20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                                                          000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
        63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


  Key is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update
```

```
provided_data
                                                          000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


------------

V || 0x00 || provided_data is
                                                        01010101
    01010101 01010101 01010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 01010101 00000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


K = HMAC(K, V || 0x00 || provided_data) is
    E5675B81 A558502A 38EBFD09 A9753D3E F31388D1 EF8EFC89
    1808526C D64ABF8C 3502D83F 20CE07DB 68F0FA99 22789E4C


V = HMAC(K, V) is
    F70F7FF2 45023323 7528314F A8EBF4D2 50B95649 06F0EF58
    41402759 CD72F743 72924730 1F85C172 1CCB323D 4D8B887F


------------

V || 0x01 || provided_data is
                                                        F70F7FF2
    45023323 7528314F A8EBF4D2 50B95649 06F0EF58 41402759
    CD72F743 72924730 1F85C172 1CCB323D 4D8B887F 01000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


K = HMAC(K, V || 0x01 || provided_data) is
```

```
        DE2451BA AF677086 D7C6FBDB 53638AC0 0FE1E7E9 B1CF6A30
        4ABC2005 D1A8A726 77A4E48A B5B3D2D1 35BA251A 764C77C7


    V = HMAC(K, V) is
        D6F45225 560DF998 B7006216 D4FFAE27 44D97518 D7585280
        09A9DCE6 1D50A2FF B4C53C9E D7B405C5 6692FDA8 5523EC69


  Update (Key, V):

    Key is
        DE2451BA AF677086 D7C6FBDB 53638AC0 0FE1E7E9 B1CF6A30
        4ABC2005 D1A8A726 77A4E48A B5B3D2D1 35BA251A 764C77C7


    V is
        D6F45225 560DF998 B7006216 D4FFAE27 44D97518 D7585280
        09A9DCE6 1D50A2FF B4C53C9E D7B405C5 6692FDA8 5523EC69


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE
```

```
    additional_input is  <empty>

  Seed_Material is
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  Key is
        DE2451BA AF677086 D7C6FBDB 53638AC0 0FE1E7E9 B1CF6A30
        4ABC2005 D1A8A726 77A4E48A B5B3D2D1 35BA251A 764C77C7


  V is
        D6F45225 560DF998 B7006216 D4FFAE27 44D97518 D7585280
        09A9DCE6 1D50A2FF B4C53C9E D7B405C5 6692FDA8 5523EC69


---------------------------

  Update

    provided_data
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    ------------

    V || 0x00 || provided_data is
                           D6F45225 560DF998 B7006216 D4FFAE27
        44D97518 D7585280 09A9DCE6 1D50A2FF B4C53C9E D7B405C5
        6692FDA8 5523EC69 00808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    K = HMAC(K, V || 0x00 || provided_data) is
        4BEF4E9F 3D8105E6 700CBA90 8ABA29CB 42D3F72D 9EEF2FE3
```

```
        DE136559 1A50E527 21318D64 8944859C A97B12C7 672BD3E3


    V = HMAC(K, V) is
        7FFBC5F8 8ABDF011 517370E2 D6081072 C680E523 14F66156
        42F38C60 CF73C071 13F90D9F A85FC132 B24753DC 119FBF74


    ------------

    V || 0x01 || provided_data is
                          7FFBC5F8 8ABDF011 517370E2 D6081072
        C680E523 14F66156 42F38C60 CF73C071 13F90D9F A85FC132
        B24753DC 119FBF74 01808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    K = HMAC(K, V || 0x01 || provided_data) is
        F51761FD 6C4C10BC 6843A51A FE40EFE9 2AC78D7C 2CE62FFA
        562E530C 40F165CB 58EA3DF8 447FB5CA 75A4A0C9 7004431E


    V = HMAC(K, V) is
        5279E3F8 A1887F7C 0CE2A9FC 1CCE90B1 E3B8021A 8FFACEE2
        66F1D4CB F8589D67 05D0FE7B 6B7EAFC6 70B73EC3 60A5BD35


  Update (Key, V):

    Key is
        F51761FD 6C4C10BC 6843A51A FE40EFE9 2AC78D7C 2CE62FFA
        562E530C 40F165CB 58EA3DF8 447FB5CA 75A4A0C9 7004431E


    V is
        5279E3F8 A1887F7C 0CE2A9FC 1CCE90B1 E3B8021A 8FFACEE2
        66F1D4CB F8589D67 05D0FE7B 6B7EAFC6 70B73EC3 60A5BD35


**************************************************************

HMAC_DRBG_Generate
```

```
  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        0DC4AC80 D862FBB4 83980077 5BF1E7D3 7AE1E195 A9A30C44
        3A4229B2 8D277E2A BE8E7E41 AC5A870E F3824657 4203FD0D


    temp is
        0DC4AC80 D862FBB4 83980077 5BF1E7D3 7AE1E195 A9A30C44
        3A4229B2 8D277E2A BE8E7E41 AC5A870E F3824657 4203FD0D


  ------------

    V = HMAC(K, V) is
        0C68069F 3DE0F533 57F8B80A FE695876 C731D774 E80CCDA5
        8927FE45 F6168BE8 BC56F876 8ED2065D 0C5829D7 8694EDCF


    temp is
        0DC4AC80 D862FBB4 83980077 5BF1E7D3 7AE1E195 A9A30C44
        3A4229B2 8D277E2A BE8E7E41 AC5A870E F3824657 4203FD0D
        0C68069F 3DE0F533 57F8B80A FE695876 C731D774 E80CCDA5
        8927FE45 F6168BE8 BC56F876 8ED2065D 0C5829D7 8694EDCF


---------------------------

  returned_bits is
        0DC4AC80 D862FBB4 83980077 5BF1E7D3 7AE1E195 A9A30C44
        3A4229B2 8D277E2A BE8E7E41 AC5A870E F3824657 4203FD0D
        0C68069F 3DE0F533 57F8B80A FE695876 C731D774 E80CCDA5
        8927FE45 F6168BE8 BC56F876 8ED2065D 0C5829D7 8694EDCF


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>
```

```
    ------------

    V || 0x00 || provided_data is
                                                              0C
        68069F3D E0F53357 F8B80AFE 695876C7 31D774E8 0CCDA589
        27FE45F6 168BE8BC 56F8768E D2065D0C 5829D786 94EDCF00


    K = HMAC(K, V || 0x00 || provided_data) is
        24CBF22F 1D9D609B 057D661F FA38E1FE 4C3A248F 6703EF33
        7AC3342E 16764CC0 9FA53F01 F7A89CED 3543C990 0A4A84AB


    V = HMAC(K, V) is
        CC054BC6 66BF8793 429D4B82 E23059CC BAD4ABB4 F9368AF2
        0D54F4C5 63C1BE92 5DADF8E3 B039D3C8 A1FE432A DC573A31


rnd_val is
        0DC4AC80 D862FBB4 83980077 5BF1E7D3 7AE1E195 A9A30C44
        3A4229B2 8D277E2A BE8E7E41 AC5A870E F3824657 4203FD0D
        0C68069F 3DE0F533 57F8B80A FE695876 C731D774 E80CCDA5
        8927FE45 F6168BE8 BC56F876 8ED2065D 0C5829D7 8694EDCF


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

Generate FAILED: Reseed is required
***************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                             C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
```

```
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    additional_input is  <empty>

  Seed_Material is
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  Key is
        24CBF22F 1D9D609B 057D661F FA38E1FE 4C3A248F 6703EF33
        7AC3342E 16764CC0 9FA53F01 F7A89CED 3543C990 0A4A84AB


  V is
        CC054BC6 66BF8793 429D4B82 E23059CC BAD4ABB4 F9368AF2
        0D54F4C5 63C1BE92 5DADF8E3 B039D3C8 A1FE432A DC573A31


---------------------------

  Update

    provided_data
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    ------------

    V || 0x00 || provided_data is
                          CC054BC6 66BF8793 429D4B82 E23059CC
        BAD4ABB4 F9368AF2 0D54F4C5 63C1BE92 5DADF8E3 B039D3C8
        A1FE432A DC573A31 00C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E
```

```
  K = HMAC(K, V || 0x00 || provided_data) is
      53C01F08 5511CBB7 900AC343 096A1F10 988EA942 C044BBA8
      6847CEFF 981966B6 6E254A9B 8219CDDF E4FE3B41 226FD5CF


  V = HMAC(K, V) is
      A7006AEE 57CEEEF0 B6D4D886 C9B31281 18544E30 397D36E5
      CC9971B2 66C425AF D106A34E 220282EA 831153CE 6654A4F2


  ------------

  V || 0x01 || provided_data is
                         A7006AEE 57CEEEF0 B6D4D886 C9B31281
      18544E30 397D36E5 CC9971B2 66C425AF D106A34E 220282EA
      831153CE 6654A4F2 01C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
      CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
      E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
      FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
      1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  K = HMAC(K, V || 0x01 || provided_data) is
      B05A00CE 2CFD708F 3ACB9092 0F152F8A D9CE740A 76C8A56E
      2C8220C0 B1C02396 4A0CA788 B4CFE25A 70938AA8 D5FF6525


  V = HMAC(K, V) is
      C9B3C782 6FFA7EFD E6E30723 E87F5A4C EC563A14 91789FE1
      1A7083A2 711E5366 866502D2 A74C64D0 71CCEFC0 5CEB3CBA


Update (Key, V):

  Key is
      B05A00CE 2CFD708F 3ACB9092 0F152F8A D9CE740A 76C8A56E
      2C8220C0 B1C02396 4A0CA788 B4CFE25A 70938AA8 D5FF6525


  V is
      C9B3C782 6FFA7EFD E6E30723 E87F5A4C EC563A14 91789FE1
      1A7083A2 711E5366 866502D2 A74C64D0 71CCEFC0 5CEB3CBA
```

```
***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        018413E2 105E8803 FA13F8E8 65D538B4 747B3297 2577F180
        70A3F1B6 49986781 027DC908 210BAD0F 0E1DA470 A0450EFD


    temp is
        018413E2 105E8803 FA13F8E8 65D538B4 747B3297 2577F180
        70A3F1B6 49986781 027DC908 210BAD0F 0E1DA470 A0450EFD


  ------------

    V = HMAC(K, V) is
        0EC93DC0 06D24E95 BC6BA656 7AB36074 A29F2C93 B836FAF9
        62F80560 E44D759F F920BCFA 83EF4595 16F7196D 0885C522


    temp is
        018413E2 105E8803 FA13F8E8 65D538B4 747B3297 2577F180
        70A3F1B6 49986781 027DC908 210BAD0F 0E1DA470 A0450EFD
        0EC93DC0 06D24E95 BC6BA656 7AB36074 A29F2C93 B836FAF9
        62F80560 E44D759F F920BCFA 83EF4595 16F7196D 0885C522


---------------------------

  returned_bits is
        018413E2 105E8803 FA13F8E8 65D538B4 747B3297 2577F180
        70A3F1B6 49986781 027DC908 210BAD0F 0E1DA470 A0450EFD
        0EC93DC0 06D24E95 BC6BA656 7AB36074 A29F2C93 B836FAF9
        62F80560 E44D759F F920BCFA 83EF4595 16F7196D 0885C522


  call Update(additional_input, K, V)
---------------------------
```

```
  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                                  0E
        C93DC006 D24E95BC 6BA6567A B36074A2 9F2C93B8 36FAF962
        F80560E4 4D759FF9 20BCFA83 EF459516 F7196D08 85C52200


    K = HMAC(K, V || 0x00 || provided_data) is
        9AA45364 6096D875 09CE753A CBA6D6B9 00C28240 41340F09
        92F198E8 96F4A311 3AFE97D7 BF59F066 9BBF7C98 80D24887


    V = HMAC(K, V) is
        735DA3B1 0D10469D 49B2D2DE B56CB890 275222E1 59BD3570
        DEE47333 7721C8AA BFC94350 775D25FB 5DFB3581 A048241F


rnd_val is
        018413E2 105E8803 FA13F8E8 65D538B4 747B3297 2577F180
        70A3F1B6 49986781 027DC908 210BAD0F 0E1DA470 A0450EFD
        0EC93DC0 06D24E95 BC6BA656 7AB36074 A29F2C93 B836FAF9
        62F80560 E44D759F F920BCFA 83EF4595 16F7196D 0885C522


################################################################

HMAC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E
```

```
    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                   20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput1 =
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    AdditionalInput2 =
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


##################################################################

******************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
```

```
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                    20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                                                          000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
        63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


  Key is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                                                          000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
        63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B
```

```
------------

V || 0x00 || provided_data is
                                                    01010101
    01010101 01010101 01010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 01010101 00000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


K = HMAC(K, V || 0x00 || provided_data) is
    E5675B81 A558502A 38EBFD09 A9753D3E F31388D1 EF8EFC89
    1808526C D64ABF8C 3502D83F 20CE07DB 68F0FA99 22789E4C


V = HMAC(K, V) is
    F70F7FF2 45023323 7528314F A8EBF4D2 50B95649 06F0EF58
    41402759 CD72F743 72924730 1F85C172 1CCB323D 4D8B887F


------------

V || 0x01 || provided_data is
                                                    F70F7FF2
    45023323 7528314F A8EBF4D2 50B95649 06F0EF58 41402759
    CD72F743 72924730 1F85C172 1CCB323D 4D8B887F 01000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


K = HMAC(K, V || 0x01 || provided_data) is
    DE2451BA AF677086 D7C6FBDB 53638AC0 0FE1E7E9 B1CF6A30
    4ABC2005 D1A8A726 77A4E48A B5B3D2D1 35BA251A 764C77C7


V = HMAC(K, V) is
    D6F45225 560DF998 B7006216 D4FFAE27 44D97518 D7585280
    09A9DCE6 1D50A2FF B4C53C9E D7B405C5 6692FDA8 5523EC69
```

```
  Update (Key, V):

    Key is
        DE2451BA AF677086 D7C6FBDB 53638AC0 0FE1E7E9 B1CF6A30
        4ABC2005 D1A8A726 77A4E48A B5B3D2D1 35BA251A 764C77C7


    V is
        D6F45225 560DF998 B7006216 D4FFAE27 44D97518 D7585280
        09A9DCE6 1D50A2FF B4C53C9E D7B405C5 6692FDA8 5523EC69


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is
                           606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                           808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    additional_input is
                           606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
```

```
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


  Seed_Material is
                                                 8081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
        9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
        B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


  Key is
        DE2451BA AF677086 D7C6FBDB 53638AC0 0FE1E7E9 B1CF6A30
        4ABC2005 D1A8A726 77A4E48A B5B3D2D1 35BA251A 764C77C7


  V is
        D6F45225 560DF998 B7006216 D4FFAE27 44D97518 D7585280
        09A9DCE6 1D50A2FF B4C53C9E D7B405C5 6692FDA8 5523EC69


---------------------------

  Update

    provided_data
                                                 8081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
        9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
        B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    ------------
```

```
V || 0x00 || provided_data is
                                                  D6F452 25560DF9
    98B70062 16D4FFAE 2744D975 18D75852 8009A9DC E61D50A2
    FFB4C53C 9ED7B405 C56692FD A85523EC 69008081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x00 || provided_data) is
    9FADF2CA B5F52BCD 4ED1DDC8 3A7A3333 F94771A6 C45949C2
    4F4D09DD 0156984F 7AE3882D 6B938BCD 30A657B3 74B8FB9F


V = HMAC(K, V) is
    0B4AEB0C 12A47693 2ED81E9F B8981807 CF0B35B7 94F53FAA
    1CEB37A0 DA9EB792 87C3BA50 F9F23E28 8A5B4F20 F3ED87A3


------------

V || 0x01 || provided_data is
                                                  0B4AEB 0C12A476
    932ED81E 9FB89818 07CF0B35 B794F53F AA1CEB37 A0DA9EB7
    9287C3BA 50F9F23E 288A5B4F 20F3ED87 A3018081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x01 || provided_data) is
    17C9901C CA056D1D 21D8D70B 9893574B 451CFF6F 385AB5CC
    7B931108 1F0A9F3A 2D4BF499 CC551F63 7D693B66 9433E536
```

```
    V = HMAC(K, V) is
        6B29D52D E3BB63A9 8642E78B 2BE7703D 2A35750F FB9EAA1C
        3D3EFBF1 BB6C0AB1 8564DB62 D3B60133 397B0EDB B2C06D53


  Update (Key, V):

    Key is
        17C9901C CA056D1D 21D8D70B 9893574B 451CFF6F 385AB5CC
        7B931108 1F0A9F3A 2D4BF499 CC551F63 7D693B66 9433E536


    V is
        6B29D52D E3BB63A9 8642E78B 2BE7703D 2A35750F FB9EAA1C
        3D3EFBF1 BB6C0AB1 8564DB62 D3B60133 397B0EDB B2C06D53


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        61AA7FC4 4CD9D28E 5A19092C 5ADBA05D F7A4EADC FBBB920F
        2A2EF8DC 1692F203 EC3EAC8D 38FD917D 13CA80AC A874003E


    temp is
        61AA7FC4 4CD9D28E 5A19092C 5ADBA05D F7A4EADC FBBB920F
        2A2EF8DC 1692F203 EC3EAC8D 38FD917D 13CA80AC A874003E


  ------------

    V = HMAC(K, V) is
        CD556DD9 954C5802 4AA6B155 1049E612 D548C6EA CACC5C26
        0CACCD88 47CFE880 8B5B57D2 F3405ECD 1DD84756 585E8FBE
```

```
    temp is
        61AA7FC4 4CD9D28E 5A19092C 5ADBA05D F7A4EADC FBBB920F
        2A2EF8DC 1692F203 EC3EAC8D 38FD917D 13CA80AC A874003E
        CD556DD9 954C5802 4AA6B155 1049E612 D548C6EA CACC5C26
        0CACCD88 47CFE880 8B5B57D2 F3405ECD 1DD84756 585E8FBE


---------------------------

  returned_bits is
        61AA7FC4 4CD9D28E 5A19092C 5ADBA05D F7A4EADC FBBB920F
        2A2EF8DC 1692F203 EC3EAC8D 38FD917D 13CA80AC A874003E
        CD556DD9 954C5802 4AA6B155 1049E612 D548C6EA CACC5C26
        0CACCD88 47CFE880 8B5B57D2 F3405ECD 1DD84756 585E8FBE


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                            CD
        556DD995 4C58024A A6B15510 49E612D5 48C6EACA CC5C260C
        ACCD8847 CFE8808B 5B57D2F3 405ECD1D D8475658 5E8FBE00


    K = HMAC(K, V || 0x00 || provided_data) is
        5B78D72D D7D4EFB3 F45AC31B 89802B49 0FF3CFB4 D324A419
        EC6D0385 DF1E750C 08D0B874 B3A3814E 521B229B B6C67497


    V = HMAC(K, V) is
        758EFB2B 4B1FCD20 CBA02F0A E71F3A3E EDD9B1D1 CC7CA8AE
        5838BD43 DB6C42AE DE8CE9BD 4B3827F1 1B1806BA A22275E9


rnd_val is
        61AA7FC4 4CD9D28E 5A19092C 5ADBA05D F7A4EADC FBBB920F
        2A2EF8DC 1692F203 EC3EAC8D 38FD917D 13CA80AC A874003E
        CD556DD9 954C5802 4AA6B155 1049E612 D548C6EA CACC5C26
        0CACCD88 47CFE880 8B5B57D2 F3405ECD 1DD84756 585E8FBE
```

```
---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Generate FAILED: Reseed is required
***************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    additional_input is
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  Seed_Material is
                                                  C0C1 C2C3C4C5
        C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
        DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
```

```
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  Key is
        5B78D72D D7D4EFB3 F45AC31B 89802B49 0FF3CFB4 D324A419
        EC6D0385 DF1E750C 08D0B874 B3A3814E 521B229B B6C67497


  V is
        758EFB2B 4B1FCD20 CBA02F0A E71F3A3E EDD9B1D1 CC7CA8AE
        5838BD43 DB6C42AE DE8CE9BD 4B3827F1 1B1806BA A22275E9


---------------------------

  Update

    provided_data
                                                C0C1 C2C3C4C5
        C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
        DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    ------------

    V || 0x00 || provided_data is
                                              758EFB 2B4B1FCD
        20CBA02F 0AE71F3A 3EEDD9B1 D1CC7CA8 AE5838BD 43DB6C42
        AEDE8CE9 BD4B3827 F11B1806 BAA22275 E900C0C1 C2C3C4C5
        C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
        DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
```

```
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  K = HMAC(K, V || 0x00 || provided_data) is
      0AF353E9 02F91380 C592800E A2C074F0 C27BDC69 519AA7B5
      1114AE83 51925AD7 7AC74BBE 516FD004 D590A0D6 66FFC44F


  V = HMAC(K, V) is
      3A34E67C 3AF1808B 134C4EBA 578CFC96 B21F4942 7EA7474A
      9E42E096 E981B82B 8C86E9E6 0FC184F1 8FD68D74 2561E441


  ------------

  V || 0x01 || provided_data is
                                                3A34E6 7C3AF180
      8B134C4E BA578CFC 96B21F49 427EA747 4A9E42E0 96E981B8
      2B8C86E9 E60FC184 F18FD68D 742561E4 4101C0C1 C2C3C4C5
      C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
      DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
      F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
      0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
      26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  K = HMAC(K, V || 0x01 || provided_data) is
      DDE62D1D 19862D57 3E96719E 2E783954 C8D7CC72 DA242C94
      E1FC41C2 FCA96B44 29F41F62 5B19769B 7454FC6E C0133D85


  V = HMAC(K, V) is
      7F4C4B95 7AF571A9 C7178615 C105D370 10F02FFB BF35A3B3
      E553BC9A 22A790CF B55AD5B6 B6A9F995 89CB230F 70C43A5D


Update (Key, V):

  Key is
```

DDE62D1D 19862D57 3E96719E 2E783954 C8D7CC72 DA242C94
E1FC41C2 FCA96B44 29F41F62 5B19769B 7454FC6E C0133D85

V is
7F4C4B95 7AF571A9 C7178615 C105D370 10F02FFB BF35A3B3
E553BC9A 22A790CF B55AD5B6 B6A9F995 89CB230F 70C43A5D

****

HMAC_DRBG_Generate

requested_number_of_bits = 768

additional_input is <empty>

V = HMAC(K, V) is
8659E679 E61EF663 2374C514 07F7DDA2 7DC0CE8D 8A444EB8
CA912CE1 3BB20D88 9E880E65 71913D67 2498DE90 2B71CEDA

temp is
8659E679 E61EF663 2374C514 07F7DDA2 7DC0CE8D 8A444EB8
CA912CE1 3BB20D88 9E880E65 71913D67 2498DE90 2B71CEDA

V = HMAC(K, V) is
5D644344 C63CD4D9 43CB6872 30867D60 F4712AEC 962EB77C
CDB141F6 678C622A 65A0B2B3 E3DBD812 891EA5FC F09D2F19

temp is
8659E679 E61EF663 2374C514 07F7DDA2 7DC0CE8D 8A444EB8
CA912CE1 3BB20D88 9E880E65 71913D67 2498DE90 2B71CEDA
5D644344 C63CD4D9 43CB6872 30867D60 F4712AEC 962EB77C
CDB141F6 678C622A 65A0B2B3 E3DBD812 891EA5FC F09D2F19

---

returned_bits is

```
        8659E679 E61EF663 2374C514 07F7DDA2 7DC0CE8D 8A444EB8
        CA912CE1 3BB20D88 9E880E65 71913D67 2498DE90 2B71CEDA
        5D644344 C63CD4D9 43CB6872 30867D60 F4712AEC 962EB77C
        CDB141F6 678C622A 65A0B2B3 E3DBD812 891EA5FC F09D2F19


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                            5D
        644344C6 3CD4D943 CB687230 867D60F4 712AEC96 2EB77CCD
        B141F667 8C622A65 A0B2B3E3 DBD81289 1EA5FCF0 9D2F1900


    K = HMAC(K, V || 0x00 || provided_data) is
        8650C034 55987FF7 37FDB25C B0B5587A 88BE8DFB 57B3C993
        396F7E3F 194FCC9F 6E609234 15784F56 E77D9046 6225D4B2


    V = HMAC(K, V) is
        B3D93B3A 3FAFCB35 81C2E98F 1B06B4DE 9C31142F 0F047C08
        EEE7F281 A9A6129F 0EB9F380 A9E3DF62 E2DD2CCB 735DC4E2


rnd_val is
        8659E679 E61EF663 2374C514 07F7DDA2 7DC0CE8D 8A444EB8
        CA912CE1 3BB20D88 9E880E65 71913D67 2498DE90 2B71CEDA
        5D644344 C63CD4D9 43CB6872 30867D60 F4712AEC 962EB77C
        CDB141F6 678C622A 65A0B2B3 E3DBD812 891EA5FC F09D2F19


##############################################################

HMAC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384
```

```
    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                  20212223 24252627 28292A2B


    PersonalizationString =
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    AdditionalInput = <empty>

##################################################################

******************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
```

```
                          000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                  20212223 24252627 28292A2B


    personal_str is
                          404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                     0001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  Key is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------
```

Update

provided_data
0001 02030405 06070809 0A0B0C0D 0E0F1011
12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE

V || 0x00 || provided_data is
010101 01010101 01010101 01010101 01010101
01010101 01010101 01010101 01010101 01010101 01010101
01010101 01000001 02030405 06070809 0A0B0C0D 0E0F1011
12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE

K = HMAC(K, V || 0x00 || provided_data) is
759FC2E2 D33686FF B43AB4F9 27A9E74D 7C30CE89 05C5AEDF
7A84FF76 479BD8B6 D930A267 6D76D9BC B2F420A3 4B76654A

V = HMAC(K, V) is
D873522C B0FC9099 33B67222 16975EA8 B7EA9349 6647EB8B
BC9A0873 5DE801C3 6D01ABE8 52B764E9 9514935A 9567A39D

V || 0x01 || provided_data is
D87352 2CB0FC90 9933B672 2216975E A8B7EA93

```
        496647EB 8BBC9A08 735DE801 C36D01AB E852B764 E9951493
        5A9567A3 9D010001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    K = HMAC(K, V || 0x01 || provided_data) is
        085987EF 2F1BD2B4 01CF188A EF3E3428 9AB194F5 803FB7E5
        2A0072E2 A4B86949 38AD044F BEDCEAAD EB9618C7 D7393448


    V = HMAC(K, V) is
        8E065B64 B430910B 4950528A F23A9FA2 866F8DAA 9106B72E
        38BA0B93 D033B851 04485F29 D1AD7EB6 FF1643D6 9129654D


  Update (Key, V):

    Key is
        085987EF 2F1BD2B4 01CF188A EF3E3428 9AB194F5 803FB7E5
        2A0072E2 A4B86949 38AD044F BEDCEAAD EB9618C7 D7393448


    V is
        8E065B64 B430910B 4950528A F23A9FA2 866F8DAA 9106B72E
        38BA0B93 D033B851 04485F29 D1AD7EB6 FF1643D6 9129654D


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>
```

```
Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                             808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    additional_input is  <empty>

  Seed_Material is
                             808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  Key is
        085987EF 2F1BD2B4 01CF188A EF3E3428 9AB194F5 803FB7E5
        2A0072E2 A4B86949 38AD044F BEDCEAAD EB9618C7 D7393448


  V is
        8E065B64 B430910B 4950528A F23A9FA2 866F8DAA 9106B72E
        38BA0B93 D033B851 04485F29 D1AD7EB6 FF1643D6 9129654D


---------------------------

  Update

    provided_data
                             808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE
```

```
  ------------

  V || 0x00 || provided_data is
                       8E065B64 B430910B 4950528A F23A9FA2
      866F8DAA 9106B72E 38BA0B93 D033B851 04485F29 D1AD7EB6
      FF1643D6 9129654D 00808182 83848586 8788898A 8B8C8D8E
      8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
      A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
      BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
      D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  K = HMAC(K, V || 0x00 || provided_data) is
      1C9FA6D8 1D8DFE6C F9BB52AA ABBFD392 0E64EBB5 D4ECA0CB
      43732C17 7E16D25F E60376EC 2B288F9A 83263608 FD02235D


  V = HMAC(K, V) is
      636BA84D AEECE502 2D2D64C9 DE0FA460 01291377 3B0A12D2
      D5E684A4 ED30DEFC 4B52F771 A1FAF136 D27B13D7 C3C89A27


  ------------

  V || 0x01 || provided_data is
                       636BA84D AEECE502 2D2D64C9 DE0FA460
      01291377 3B0A12D2 D5E684A4 ED30DEFC 4B52F771 A1FAF136
      D27B13D7 C3C89A27 01808182 83848586 8788898A 8B8C8D8E
      8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
      A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
      BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
      D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  K = HMAC(K, V || 0x01 || provided_data) is
      4D2276F7 3EA64903 043B719C A9070167 CDCCCC14 4C0112E4
      2C9A74A2 88E692B8 AAFA77E9 7E5BA72B 33F9212F B358347D


  V = HMAC(K, V) is
      A0F9444C 406CB1F5 474077CE B92954A5 01EEBB4F C46C8757
      58367BA6 48D99E24 75994FF3 AA4F9C3E FADD63B7 0B67EE71


Update (Key, V):
```

```
    Key is
        4D2276F7 3EA64903 043B719C A9070167 CDCCCC14 4C0112E4
        2C9A74A2 88E692B8 AAFA77E9 7E5BA72B 33F9212F B358347D


    V is
        A0F9444C 406CB1F5 474077CE B92954A5 01EEBB4F C46C8757
        58367BA6 48D99E24 75994FF3 AA4F9C3E FADD63B7 0B67EE71


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        804A3AD7 20F4FCE8 738D0632 514FEF16 430CB7D6 3A8DF1A5
        F02A3CE3 BD7ED6A6 68B69E63 E2BB93F0 96EE753D 6194A0F1


    temp is
        804A3AD7 20F4FCE8 738D0632 514FEF16 430CB7D6 3A8DF1A5
        F02A3CE3 BD7ED6A6 68B69E63 E2BB93F0 96EE753D 6194A0F1


  ------------

    V = HMAC(K, V) is
        A3271106 36530096 36337D22 167CC440 2D019AC2 16FA574F
        091CF6EA 283568D7 37A77BE3 8E8F0938 2C69E76B 142ABC3A


    temp is
        804A3AD7 20F4FCE8 738D0632 514FEF16 430CB7D6 3A8DF1A5
        F02A3CE3 BD7ED6A6 68B69E63 E2BB93F0 96EE753D 6194A0F1
        A3271106 36530096 36337D22 167CC440 2D019AC2 16FA574F
        091CF6EA 283568D7 37A77BE3 8E8F0938 2C69E76B 142ABC3A


---------------------------
```

```
  returned_bits is
        804A3AD7 20F4FCE8 738D0632 514FEF16 430CB7D6 3A8DF1A5
        F02A3CE3 BD7ED6A6 68B69E63 E2BB93F0 96EE753D 6194A0F1
        A3271106 36530096 36337D22 167CC440 2D019AC2 16FA574F
        091CF6EA 283568D7 37A77BE3 8E8F0938 2C69E76B 142ABC3A


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                              A3
        27110636 53009636 337D2216 7CC4402D 019AC216 FA574F09
        1CF6EA28 3568D737 A77BE38E 8F09382C 69E76B14 2ABC3A00


    K = HMAC(K, V || 0x00 || provided_data) is
        E2C0EF35 375E7405 0B95DC11 BEAA9A8B 336FFC44 478234D7
        0DDCD0CD 58C798E0 FBE0A03D 9D2110F7 024C6D88 E7497BB0


    V = HMAC(K, V) is
        062FD25F 4544B9F9 C1A6AC78 E0909B18 B447332D C1E4D48B
        EDF84413 1D0213C6 70480F0A 5308D2AE 001BA8EB ABFB8E3F


rnd_val is
        804A3AD7 20F4FCE8 738D0632 514FEF16 430CB7D6 3A8DF1A5
        F02A3CE3 BD7ED6A6 68B69E63 E2BB93F0 96EE753D 6194A0F1
        A3271106 36530096 36337D22 167CC440 2D019AC2 16FA574F
        091CF6EA 283568D7 37A77BE3 8E8F0938 2C69E76B 142ABC3A


------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate
```

```
  requested_number_of_bits = 768

    additional_input is  <empty>

Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    additional_input is  <empty>

  Seed_Material is
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  Key is
        E2C0EF35 375E7405 0B95DC11 BEAA9A8B 336FFC44 478234D7
        0DDCD0CD 58C798E0 FBE0A03D 9D2110F7 024C6D88 E7497BB0


  V is
        062FD25F 4544B9F9 C1A6AC78 E0909B18 B447332D C1E4D48B
        EDF84413 1D0213C6 70480F0A 5308D2AE 001BA8EB ABFB8E3F


---------------------------

  Update

    provided_data
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
```

FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E

V || 0x00 || provided_data is
062FD25F 4544B9F9 C1A6AC78 E0909B18
B447332D C1E4D48B EDF84413 1D0213C6 70480F0A 5308D2AE
001BA8EB ABFB8E3F 00C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E

K = HMAC(K, V || 0x00 || provided_data) is
BAFFB234 45445961 91E1AAA1 6E7B3E61 F9828D06 EA466F4C
2B53A319 5F55C0D7 BAF86AE7 CAAD72F5 66CB9048 E88E8700

V = HMAC(K, V) is
99E49A1C 9CBCFF92 46FBE4D8 2149EF06 75759443 CEF5A876
F856A566 B5ADA088 40B845B8 4A170D65 E4565CD6 224D46F7

V || 0x01 || provided_data is
99E49A1C 9CBCFF92 46FBE4D8 2149EF06
75759443 CEF5A876 F856A566 B5ADA088 40B845B8 4A170D65
E4565CD6 224D46F7 01C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E

K = HMAC(K, V || 0x01 || provided_data) is
938C379D EBC9F6E7 E31F9D37 20BDF8A9 F6DF97D9 1D56E1E4
A42D48CF 5CC0048B E7593F8F 621C3A11 3D6AEA12 3BE358A1

V = HMAC(K, V) is
A1E2B41D 1A621E6E B4444042 B18E0E93 4084F074 6694E764
904155E7 7C3E555D 80C5F9FB 7A550F71 8150E52F 3B0DEB34

```
  Update (Key, V):

    Key is
        938C379D EBC9F6E7 E31F9D37 20BDF8A9 F6DF97D9 1D56E1E4
        A42D48CF 5CC0048B E7593F8F 621C3A11 3D6AEA12 3BE358A1


    V is
        A1E2B41D 1A621E6E B4444042 B18E0E93 4084F074 6694E764
        904155E7 7C3E555D 80C5F9FB 7A550F71 8150E52F 3B0DEB34


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        73B8E55C 75320217 6A17B9B9 754A9FE6 F23B0186 1FCD4059
        6AEAA301 AF1AEF8A F0EAF22F BF34541E FFAB1431 666ACACC


    temp is
        73B8E55C 75320217 6A17B9B9 754A9FE6 F23B0186 1FCD4059
        6AEAA301 AF1AEF8A F0EAF22F BF34541E FFAB1431 666ACACC


  ------------

    V = HMAC(K, V) is
        759338C7 E2867281 9D53CFEF 10A3E19D AFBD5329 5F1980A9
        F491504A 27255067 84B7AC82 6D92C838 A8668171 CAAA86E7


    temp is
        73B8E55C 75320217 6A17B9B9 754A9FE6 F23B0186 1FCD4059
        6AEAA301 AF1AEF8A F0EAF22F BF34541E FFAB1431 666ACACC
        759338C7 E2867281 9D53CFEF 10A3E19D AFBD5329 5F1980A9
        F491504A 27255067 84B7AC82 6D92C838 A8668171 CAAA86E7
```

```
---------------------------

  returned_bits is
        73B8E55C 75320217 6A17B9B9 754A9FE6 F23B0186 1FCD4059
        6AEAA301 AF1AEF8A F0EAF22F BF34541E FFAB1431 666ACACC
        759338C7 E2867281 9D53CFEF 10A3E19D AFBD5329 5F1980A9
        F491504A 27255067 84B7AC82 6D92C838 A8668171 CAAA86E7


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                          75
        9338C7E2 8672819D 53CFEF10 A3E19DAF BD53295F 1980A9F4
        91504A27 25506784 B7AC826D 92C838A8 668171CA AA86E700


    K = HMAC(K, V || 0x00 || provided_data) is
        06F77A08 C07BABD4 ACC6761F 0726141B E48E3DA0 D140EB8A
        7B05E053 168F92A1 C66B625D A046E9D0 31E414E1 21AB0033


    V = HMAC(K, V) is
        FC7C27C8 34FBE90C 6539863F DF9B9478 3A98D67D E8CF1BD5
        4682E95F 80B48AC7 6935E0E2 B6E2876E 24DB08D4 72A65292


rnd_val is
        73B8E55C 75320217 6A17B9B9 754A9FE6 F23B0186 1FCD4059
        6AEAA301 AF1AEF8A F0EAF22F BF34541E FFAB1431 666ACACC
        759338C7 E2867281 9D53CFEF 10A3E19D AFBD5329 5F1980A9
        F491504A 27255067 84B7AC82 6D92C838 A8668171 CAAA86E7


################################################################

HMAC_DRBG
```

```
Requested Security Strength = 192

Requested Hash Algorithm = SHA-384

prediction_resistance_flag = "ENABLED"
EntropyInput =
                        000102 03040506 0708090A 0B0C0D0E
    0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
    2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
    3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
    5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


EntropyInput1 (for Reseed1) =
                        808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


EntropyInput2 (for Reseed2) =
                        C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Nonce =
                               20212223 24252627 28292A2B


PersonalizationString =
                        404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


AdditionalInput1 =
                        606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
```

```
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    AdditionalInput2 =
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                  20212223 24252627 28292A2B


    personal_str is
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                      0001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
```

```
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  Key is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


----------------------------

  Update

    provided_data
                     0001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    ------------

    V || 0x00 || provided_data is
                   010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01000001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
```

```
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
      9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  K = HMAC(K, V || 0x00 || provided_data) is
      759FC2E2 D33686FF B43AB4F9 27A9E74D 7C30CE89 05C5AEDF
      7A84FF76 479BD8B6 D930A267 6D76D9BC B2F420A3 4B76654A


  V = HMAC(K, V) is
      D873522C B0FC9099 33B67222 16975EA8 B7EA9349 6647EB8B
      BC9A0873 5DE801C3 6D01ABE8 52B764E9 9514935A 9567A39D


  ------------

  V || 0x01 || provided_data is
                 D87352 2CB0FC90 9933B672 2216975E A8B7EA93
      496647EB 8BBC9A08 735DE801 C36D01AB E852B764 E9951493
      5A9567A3 9D010001 02030405 06070809 0A0B0C0D 0E0F1011
      12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
      2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
      42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
      5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
      23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
      4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
      9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  K = HMAC(K, V || 0x01 || provided_data) is
      085987EF 2F1BD2B4 01CF188A EF3E3428 9AB194F5 803FB7E5
      2A0072E2 A4B86949 38AD044F BEDCEAAD EB9618C7 D7393448


  V = HMAC(K, V) is
      8E065B64 B430910B 4950528A F23A9FA2 866F8DAA 9106B72E
      38BA0B93 D033B851 04485F29 D1AD7EB6 FF1643D6 9129654D


Update (Key, V):

  Key is
      085987EF 2F1BD2B4 01CF188A EF3E3428 9AB194F5 803FB7E5
```

```
        2A0072E2 A4B86949 38AD044F BEDCEAAD EB9618C7 D7393448


    V is
        8E065B64 B430910B 4950528A F23A9FA2 866F8DAA 9106B72E
        38BA0B93 D033B851 04485F29 D1AD7EB6 FF1643D6 9129654D


---------------------------------------------------------------

First call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is
                           606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Generate FAILED: Reseed is required
***************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                           808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    additional_input is
                           606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

Seed_Material is

```
                                                  8081 82838485
      86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
      9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
      B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
      CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
      E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
      6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
      8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
      9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
      B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

Key is

```
      085987EF 2F1BD2B4 01CF188A EF3E3428 9AB194F5 803FB7E5
      2A0072E2 A4B86949 38AD044F BEDCEAAD EB9618C7 D7393448
```

V is

```
      8E065B64 B430910B 4950528A F23A9FA2 866F8DAA 9106B72E
      38BA0B93 D033B851 04485F29 D1AD7EB6 FF1643D6 9129654D
```

Update

provided_data

```
                                                  8081 82838485
      86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
      9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
      B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
      CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
      E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
      6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
      8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
      9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
      B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

V || 0x00 || provided_data is

```
                                                8E065B 64B43091
      0B495052 8AF23A9F A2866F8D AA9106B7 2E38BA0B 93D033B8
```

```
    5104485F 29D1AD7E B6FF1643 D6912965 4D008081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x00 || provided_data) is
    840E795F 167DF10E 956213C5 2BC483BC B6ECD132 849DF730
    C3E8D9CC 54F19C6B 3B09B80C 5C001A83 67F69B16 016B20DD


V = HMAC(K, V) is
    E02485E8 1B0E2312 7D733900 A6D9A67A C5255B9A B7EC719A
    8AD3B2B1 24806654 30DBC1EA 8BD5CF05 25895C0F 1C24C4B8


------------

V || 0x01 || provided_data is
                                            E02485 E81B0E23
    127D7339 00A6D9A6 7AC5255B 9AB7EC71 9A8AD3B2 B1248066
    5430DBC1 EA8BD5CF 0525895C 0F1C24C4 B8018081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x01 || provided_data) is
    82F6395B 724D720E 5C3A4AD0 FEDD38BF 78642799 23646108
    BC7F9542 E557E84D C5F034FC 6A33D4A7 288B2A28 CD3CB6B6


V = HMAC(K, V) is
    34CA293B AE154FA0 3531B6B0 A17F7D54 2BE4C52C 2AF71CB2
```

```
        9372160E 34403801 FF392CAB DE4B6332 F3C508A3 AB4B404C


  Update (Key, V):

    Key is
        82F6395B 724D720E 5C3A4AD0 FEDD38BF 78642799 23646108
        BC7F9542 E557E84D C5F034FC 6A33D4A7 288B2A28 CD3CB6B6


    V is
        34CA293B AE154FA0 3531B6B0 A17F7D54 2BE4C52C 2AF71CB2
        9372160E 34403801 FF392CAB DE4B6332 F3C508A3 AB4B404C


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        5EDACD29 898A1E8F B0E32CCD 77EF56C6 CBD0D9BD 7027CFF5
        3FEF9050 047682C6 9CE18B27 31CEDEF6 7E9066B9 4EDD2CAF


    temp is
        5EDACD29 898A1E8F B0E32CCD 77EF56C6 CBD0D9BD 7027CFF5
        3FEF9050 047682C6 9CE18B27 31CEDEF6 7E9066B9 4EDD2CAF


  ------------

    V = HMAC(K, V) is
        6683302E 3FB51FF8 6767A6FD B607BFD8 744DA141 E67E8326
        7850F789 7C927DE7 D4A27EEA 9A7A8131 C4C22D76 9CCA49E0


    temp is
        5EDACD29 898A1E8F B0E32CCD 77EF56C6 CBD0D9BD 7027CFF5
        3FEF9050 047682C6 9CE18B27 31CEDEF6 7E9066B9 4EDD2CAF
        6683302E 3FB51FF8 6767A6FD B607BFD8 744DA141 E67E8326
```

```
        7850F789 7C927DE7 D4A27EEA 9A7A8131 C4C22D76 9CCA49E0


---------------------------

  returned_bits is
        5EDACD29 898A1E8F B0E32CCD 77EF56C6 CBD0D9BD 7027CFF5
        3FEF9050 047682C6 9CE18B27 31CEDEF6 7E9066B9 4EDD2CAF
        6683302E 3FB51FF8 6767A6FD B607BFD8 744DA141 E67E8326
        7850F789 7C927DE7 D4A27EEA 9A7A8131 C4C22D76 9CCA49E0


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                           66
        83302E3F B51FF867 67A6FDB6 07BFD874 4DA141E6 7E832678
        50F7897C 927DE7D4 A27EEA9A 7A8131C4 C22D769C CA49E000


    K = HMAC(K, V || 0x00 || provided_data) is
        3893A359 D9196DC2 3573E2B6 CC3677FF 6D8175AF 71E93A4F
        C90DFE43 970E006A D6BCDC8A 7AC450D8 06E9E4A4 65D507F2


    V = HMAC(K, V) is
        A0D9C554 9FF79334 491E459B 6409ED7B A0641663 082F4BEB
        9FBC0B80 43FD87F5 29077B50 15CE5689 40E903A2 3BA509E6


rnd_val is
        5EDACD29 898A1E8F B0E32CCD 77EF56C6 CBD0D9BD 7027CFF5
        3FEF9050 047682C6 9CE18B27 31CEDEF6 7E9066B9 4EDD2CAF
        6683302E 3FB51FF8 6767A6FD B607BFD8 744DA141 E67E8326
        7850F789 7C927DE7 D4A27EEA 9A7A8131 C4C22D76 9CCA49E0


-------------------------------------------------------------
```

```
Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                           C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    additional_input is
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  Seed_Material is
                                                 C0C1 C2C3C4C5
        C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
        DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
```

DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E

Key is
3893A359 D9196DC2 3573E2B6 CC3677FF 6D8175AF 71E93A4F
C90DFE43 970E006A D6BCDC8A 7AC450D8 06E9E4A4 65D507F2

V is
A0D9C554 9FF79334 491E459B 6409ED7B A0641663 082F4BEB
9FBC0B80 43FD87F5 29077B50 15CE5689 40E903A2 3BA509E6

Update

provided_data
C0C1 C2C3C4C5
C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E

V || 0x00 || provided_data is
A0D9C5 549FF793
34491E45 9B6409ED 7BA06416 63082F4B EB9FBC0B 8043FD87
F529077B 5015CE56 8940E903 A23BA509 E600C0C1 C2C3C4C5
C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E

```
  K = HMAC(K, V || 0x00 || provided_data) is
      0C11B5B3 6E11FA9C 5A935C54 770D810A 207C2640 D61EF548
      90EE1E80 84705589 9F95E9D9 DB32E433 8A8F830D 03142E55


  V = HMAC(K, V) is
      94181C3E 1EBB1828 E2570709 FC31E329 134F34F6 1A03FCE3
      A194B127 E37A12DD 53D32F7E E7BB2679 12B3E260 BF77A2AD


  ------------

  V || 0x01 || provided_data is
                                                94181C 3E1EBB18
      28E25707 09FC31E3 29134F34 F61A03FC E3A194B1 27E37A12
      DD53D32F 7EE7BB26 7912B3E2 60BF77A2 AD01C0C1 C2C3C4C5
      C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
      DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
      F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
      0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
      26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  K = HMAC(K, V || 0x01 || provided_data) is
      374602CC 90D287DA 7C4A8F59 50108A83 AD5B6F0D 5A388ADB
      B0DC7AE2 59FA400B D2833624 BFB66E63 7C9BB152 B857CF75


  V = HMAC(K, V) is
      C9501771 CEF5FDA8 DE964F9F 2FF1E606 65736893 D2EF5E5E
      A75DBC11 02911BD8 BCCFAF0C AED2FA24 5FFE038C 0302F4A7


Update (Key, V):

  Key is
      374602CC 90D287DA 7C4A8F59 50108A83 AD5B6F0D 5A388ADB
      B0DC7AE2 59FA400B D2833624 BFB66E63 7C9BB152 B857CF75
```

```
    V is
        C9501771 CEF5FDA8 DE964F9F 2FF1E606 65736893 D2EF5E5E
        A75DBC11 02911BD8 BCCFAF0C AED2FA24 5FFE038C 0302F4A7


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        EFE5120A 69A85539 27016001 03492DFF 3D7F253E 83765107
        E2301DFA 51DCB14C 2F61DB1B 0030BF70 CCA6FB38 9BD34914


    temp is
        EFE5120A 69A85539 27016001 03492DFF 3D7F253E 83765107
        E2301DFA 51DCB14C 2F61DB1B 0030BF70 CCA6FB38 9BD34914


  ------------

    V = HMAC(K, V) is
        8929CC00 CCC8CA6F B9138FD4 5BB0A9BA 136D0E2B 9CE54D63
        4BC4D139 B238A097 1883C693 B9958354 A2CAFAFE 3654958D


    temp is
        EFE5120A 69A85539 27016001 03492DFF 3D7F253E 83765107
        E2301DFA 51DCB14C 2F61DB1B 0030BF70 CCA6FB38 9BD34914
        8929CC00 CCC8CA6F B9138FD4 5BB0A9BA 136D0E2B 9CE54D63
        4BC4D139 B238A097 1883C693 B9958354 A2CAFAFE 3654958D


---------------------------

  returned_bits is
        EFE5120A 69A85539 27016001 03492DFF 3D7F253E 83765107
        E2301DFA 51DCB14C 2F61DB1B 0030BF70 CCA6FB38 9BD34914
        8929CC00 CCC8CA6F B9138FD4 5BB0A9BA 136D0E2B 9CE54D63
        4BC4D139 B238A097 1883C693 B9958354 A2CAFAFE 3654958D
```

```
  call Update(additional_input, K, V)
--------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                                    89
        29CC00CC C8CA6FB9 138FD45B B0A9BA13 6D0E2B9C E54D634B
        C4D139B2 38A09718 83C693B9 958354A2 CAFAFE36 54958D00


    K = HMAC(K, V || 0x00 || provided_data) is
        8B7EDEA8 A8777A75 56CAD70E 21211E04 DEB8819F 6940BFDF
        373A03D2 8CDD8B22 990B6749 798F211B A8369112 AB0817CB


    V = HMAC(K, V) is
        3E747542 B9607748 97B0F107 523DEC6A E21FE528 86E471B1
        B8711BEB 10A653DB F3A00DF5 9F18AF74 7C6BBCC4 20208C6E


rnd_val is
        EFE5120A 69A85539 27016001 03492DFF 3D7F253E 83765107
        E2301DFA 51DCB14C 2F61DB1B 0030BF70 CCA6FB38 9BD34914
        8929CC00 CCC8CA6F B9138FD4 5BB0A9BA 136D0E2B 9CE54D63
        4BC4D139 B238A097 1883C693 B9958354 A2CAFAFE 3654958D
```

```
###############################################################

HMAC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                           20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm
```

```
    entropy_input is
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                           20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


  Key is
                           00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                           01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


------------

V || 0x00 || provided_data is
    01010101 01010101 01010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 00000102 03040506
    0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
    1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
    3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


K = HMAC(K, V || 0x00 || provided_data) is
                        45A111E3 AB3725B8 D02D1D8C A0AED099
    D32CF71C 2CA703C8 3708DDC3 AB0BDBEC 23719C1A 4C7273A8
    EB06EC14 B05853A0 793D492D C256DD1C 7DA4D148 BE8516CD


V = HMAC(K, V) is
                        B4F4EAD4 4D45EF54 6C9CE52C C9B0B50F
    37948762 32662A75 B91B6150 E5BB1802 C68698C7 1E5BBCEB
    2C39FB40 CE3EF53D 4F092229 4CA844A1 6E67E2B2 710250CA


------------

V || 0x01 || provided_data is
    B4F4EAD4 4D45EF54 6C9CE52C C9B0B50F 37948762 32662A75
    B91B6150 E5BB1802 C68698C7 1E5BBCEB 2C39FB40 CE3EF53D
    4F092229 4CA844A1 6E67E2B2 710250CA 01000102 03040506
    0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
    1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
    3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


K = HMAC(K, V || 0x01 || provided_data) is
                        A7E118A5 31DEF956 DCFF94BB 3D801F77
    5DC68F91 696A434C C25E270E 639044E1 A7240266 D3AA202D
```

```
        46C1054B 61024753 5007DF12 CFC8DA45 982A587F C81C47D5


    V = HMAC(K, V) is
                         110793EA A60DC9DB CD420810 4088A23D
        AECC1226 EAF1D03B BA9D83A6 95999165 71907346 B15A0439
        362B9C8E E330E52D EACC639B 98E8030A 95780CD7 C24B04D5


  Update (Key, V):

    Key is
                         A7E118A5 31DEF956 DCFF94BB 3D801F77
        5DC68F91 696A434C C25E270E 639044E1 A7240266 D3AA202D
        46C1054B 61024753 5007DF12 CFC8DA45 982A587F C81C47D5


    V is
                         110793EA A60DC9DB CD420810 4088A23D
        AECC1226 EAF1D03B BA9D83A6 95999165 71907346 B15A0439
        362B9C8E E330E52D EACC639B 98E8030A 95780CD7 C24B04D5


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                         A463395A A79F237A 22E5BD24 462BD303
        E1BE5103 BA37299B ED170E10 713EE9CD A62FABD5 171231E1
        F6D82629 BC521D41 178D002D 92918F39 7824E449 004E9AE1


    temp is
                         A463395A A79F237A 22E5BD24 462BD303
        E1BE5103 BA37299B ED170E10 713EE9CD A62FABD5 171231E1
```

```
        F6D82629 BC521D41 178D002D 92918F39 7824E449 004E9AE1


  ------------

    V = HMAC(K, V) is
                           851F7BFA 11CD616E F519A9E2 A05951D9
        108AB389 59CA7E9E 80B18ADF CC622389 495795CB FB7D39AF
        6C8571DD CE035CA6 890C7A1A F80861F0 629EF1B6 952BA206


    temp is
                                                 A463395A A79F237A
        22E5BD24 462BD303 E1BE5103 BA37299B ED170E10 713EE9CD
        A62FABD5 171231E1 F6D82629 BC521D41 178D002D 92918F39
        7824E449 004E9AE1 851F7BFA 11CD616E F519A9E2 A05951D9
        108AB389 59CA7E9E 80B18ADF CC622389 495795CB FB7D39AF
        6C8571DD CE035CA6 890C7A1A F80861F0 629EF1B6 952BA206


---------------------------

  returned_bits is
                                                 A463395A A79F237A
        22E5BD24 462BD303 E1BE5103 BA37299B ED170E10 713EE9CD
        A62FABD5 171231E1 F6D82629 BC521D41 178D002D 92918F39
        7824E449 004E9AE1 851F7BFA 11CD616E F519A9E2 A05951D9
        108AB389 59CA7E9E 80B18ADF CC622389 495795CB FB7D39AF
        6C8571DD CE035CA6 890C7A1A F80861F0 629EF1B6 952BA206


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                         85 1F7BFA11 CD616EF5 19A9E2A0 5951D910
        8AB38959 CA7E9E80 B18ADFCC 62238949 5795CBFB 7D39AF6C
        8571DDCE 035CA689 0C7A1AF8 0861F062 9EF1B695 2BA20600
```

```
    K = HMAC(K, V || 0x00 || provided_data) is
                          8B4FD7FC B0ECB6E6 28F90F71 57A26D11
        58B7269B 5FA2C7F5 54C49FFE 1E24F566 9F69B0F8 6D83FBE8
        DCA24E24 E6F652E2 EEE97482 8DC99CD1 05D12D5D 6D539188


    V = HMAC(K, V) is
                          27383F81 81766C53 A67EBA6D 822DF9F3
        6EF30976 0F1CAA2D 1D41F5B4 EA54D4C3 B9FFCC0C F8303EFA
        6803D7E9 F722F8D1 500E0E83 5AB8CC8F 7B3F3B99 C9472DB2


rnd_val is
                                              A463395A A79F237A
        22E5BD24 462BD303 E1BE5103 BA37299B ED170E10 713EE9CD
        A62FABD5 171231E1 F6D82629 BC521D41 178D002D 92918F39
        7824E449 004E9AE1 851F7BFA 11CD616E F519A9E2 A05951D9
        108AB389 59CA7E9E 80B18ADF CC622389 495795CB FB7D39AF
        6C8571DD CE035CA6 890C7A1A F80861F0 629EF1B6 952BA206


-------------------------------------------------------------

Second call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                          FB5BD98D 2CB25EC4 955CD152 04D68C49
        7281CA0C E2201DAC A5E412DD FDEBAF98 D724D216 62E45ABA
        9AE200D9 41C4CF76 039808F2 9A800034 6A6CC97D 44417737


    temp is
                          FB5BD98D 2CB25EC4 955CD152 04D68C49
        7281CA0C E2201DAC A5E412DD FDEBAF98 D724D216 62E45ABA
        9AE200D9 41C4CF76 039808F2 9A800034 6A6CC97D 44417737
```

```
  ------------

    V = HMAC(K, V) is
                           A89F9047 2AC6088B 45C666C5 61686F19
        1745228F 11ED556A 519DA9AA 1646D15B 901382D8 7726D17D
        C5139FDE E1E8BDB0 F328D4B1 05865BD1 D815641E 6B1DBA23


    temp is
                                              FB5BD98D 2CB25EC4
        955CD152 04D68C49 7281CA0C E2201DAC A5E412DD FDEBAF98
        D724D216 62E45ABA 9AE200D9 41C4CF76 039808F2 9A800034
        6A6CC97D 44417737 A89F9047 2AC6088B 45C666C5 61686F19
        1745228F 11ED556A 519DA9AA 1646D15B 901382D8 7726D17D
        C5139FDE E1E8BDB0 F328D4B1 05865BD1 D815641E 6B1DBA23


---------------------------

  returned_bits is
                                              FB5BD98D 2CB25EC4
        955CD152 04D68C49 7281CA0C E2201DAC A5E412DD FDEBAF98
        D724D216 62E45ABA 9AE200D9 41C4CF76 039808F2 9A800034
        6A6CC97D 44417737 A89F9047 2AC6088B 45C666C5 61686F19
        1745228F 11ED556A 519DA9AA 1646D15B 901382D8 7726D17D
        C5139FDE E1E8BDB0 F328D4B1 05865BD1 D815641E 6B1DBA23


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                         A8 9F90472A C6088B45 C666C561 686F1917
        45228F11 ED556A51 9DA9AA16 46D15B90 1382D877 26D17DC5
        139FDEE1 E8BDB0F3 28D4B105 865BD1D8 15641E6B 1DBA2300


    K = HMAC(K, V || 0x00 || provided_data) is
                           1A8D4FBF B9FCE595 14C1CDB3 A025DE7E
```

```
        FEAA60ED EF3E73A1 B4518CC6 003A67C3 C9E4837E FE0E84B2
        C98C0E87 6D2F6D2A AF583347 01261298 CA98D068 FEF520B8


    V = HMAC(K, V) is
                           8A43F190 1A6ACFFF F8D60A0C 1BC02E47
        48088B30 DFEF309B E595FE60 BCA7DC9D EA918356 4EE4A5B8
        005D6435 39D9976F 270DD2D2 91CCE62A E56788F8 CC1CAEB5


rnd_val is
                                                 FB5BD98D 2CB25EC4
        955CD152 04D68C49 7281CA0C E2201DAC A5E412DD FDEBAF98
        D724D216 62E45ABA 9AE200D9 41C4CF76 039808F2 9A800034
        6A6CC97D 44417737 A89F9047 2AC6088B 45C666C5 61686F19
        1745228F 11ED556A 519DA9AA 1646D15B 901382D8 7726D17D
        C5139FDE E1E8BDB0 F328D4B1 05865BD1 D815641E 6B1DBA23


################################################################

HMAC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                             808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                             C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

```
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput1 =
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    AdditionalInput2 =
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                          20212223 24252627 28292A2B 2C2D2E2F
```

```
    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


  Key is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                          01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    ------------

    V || 0x00 || provided_data is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 00000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    K = HMAC(K, V || 0x00 || provided_data) is
                          45A111E3 AB3725B8 D02D1D8C A0AED099
        D32CF71C 2CA703C8 3708DDC3 AB0BDBEC 23719C1A 4C7273A8
        EB06EC14 B05853A0 793D492D C256DD1C 7DA4D148 BE8516CD


    V = HMAC(K, V) is
                          B4F4EAD4 4D45EF54 6C9CE52C C9B0B50F
        37948762 32662A75 B91B6150 E5BB1802 C68698C7 1E5BBCEB
        2C39FB40 CE3EF53D 4F092229 4CA844A1 6E67E2B2 710250CA


    ------------

    V || 0x01 || provided_data is
        B4F4EAD4 4D45EF54 6C9CE52C C9B0B50F 37948762 32662A75
        B91B6150 E5BB1802 C68698C7 1E5BBCEB 2C39FB40 CE3EF53D
        4F092229 4CA844A1 6E67E2B2 710250CA 01000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    K = HMAC(K, V || 0x01 || provided_data) is
                          A7E118A5 31DEF956 DCFF94BB 3D801F77
        5DC68F91 696A434C C25E270E 639044E1 A7240266 D3AA202D
        46C1054B 61024753 5007DF12 CFC8DA45 982A587F C81C47D5


    V = HMAC(K, V) is
                          110793EA A60DC9DB CD420810 4088A23D
        AECC1226 EAF1D03B BA9D83A6 95999165 71907346 B15A0439
        362B9C8E E330E52D EACC639B 98E8030A 95780CD7 C24B04D5


Update (Key, V):

    Key is
                          A7E118A5 31DEF956 DCFF94BB 3D801F77
```

```
        5DC68F91 696A434C C25E270E 639044E1 A7240266 D3AA202D
        46C1054B 61024753 5007DF12 CFC8DA45 982A587F C81C47D5


    V is
                          110793EA A60DC9DB CD420810 4088A23D
        AECC1226 EAF1D03B BA9D83A6 95999165 71907346 B15A0439
        362B9C8E E330E52D EACC639B 98E8030A 95780CD7 C24B04D5


---------------------------------------------------------------

First call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


  additional_input <> NULL, call Update(additional_input, K, V)
----------------------------

  Update

    provided_data
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    ------------

    V || 0x00 || provided_data is
                                              110793EA A60DC9DB
        CD420810 4088A23D AECC1226 EAF1D03B BA9D83A6 95999165
```

```
    71907346 B15A0439 362B9C8E E330E52D EACC639B 98E8030A
    95780CD7 C24B04D5 00606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x00 || provided_data) is
                      613F9906 1E248B2D E05965D5 362A900C
    E20476AE 34433771 BD38AD34 B9307F5A EE280580 6EB35336
    9A5FB4BF 74FF9BB6 C5357745 927ACC89 99D9C257 34F9A35D


V = HMAC(K, V) is
                      0B92DBD0 91064624 8985C9F6 21C23574
    26F1E13F C24FF4CD 554DE629 A77853C8 B65D91B9 56DBC5E7
    4CE12E6A E9197529 043CA90E 0232D6A9 7F26DC5B 32E53822


------------

V || 0x01 || provided_data is
                                          0B92DBD0 91064624
    8985C9F6 21C23574 26F1E13F C24FF4CD 554DE629 A77853C8
    B65D91B9 56DBC5E7 4CE12E6A E9197529 043CA90E 0232D6A9
    7F26DC5B 32E53822 01606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x01 || provided_data) is
                      5284605C F2AFEB0D BAE2129E B7BFFE7C
    14332DB8 F74B92E9 82458FD9 32E18B0C 29F0B522 D9A02E6B
    09054ACF 9E932A02 AADD3EE3 3378E452 E2FAB625 0FB919AC


V = HMAC(K, V) is
                      0AB65B16 AE880563 F94A9459 30747960
    130144BE FA7C6298 D2BCFC44 02E29199 E5899F19 1A74F635
    727D3220 2C3300BD 48EB39F6 F9870C18 B407E507 BE14E15C


------------
```

```
    V = HMAC(K, V) is
                          0469527C F922093E 80F7C35F 96A4AA78
        D57144E0 C55E2B17 AE42BD79 FB2BE771 A19A474E EAE90D73
        E28FEA0C E1EB2ED7 EA727875 11384F8C 8033B56E F4F8545D


    temp is
                          0469527C F922093E 80F7C35F 96A4AA78
        D57144E0 C55E2B17 AE42BD79 FB2BE771 A19A474E EAE90D73
        E28FEA0C E1EB2ED7 EA727875 11384F8C 8033B56E F4F8545D


  ------------

    V = HMAC(K, V) is
                          E7AC23F4 88A8BBBE C676D614 E9572429
        F0378106 0C66A36A 604AEE6E F22E5E1F 78E5BE71 61D51308
        E1C8D6CF EF2DE302 453C4CE9 20175EDA F99664C2 339D9F07


    temp is
                                                   0469527C F922093E
        80F7C35F 96A4AA78 D57144E0 C55E2B17 AE42BD79 FB2BE771
        A19A474E EAE90D73 E28FEA0C E1EB2ED7 EA727875 11384F8C
        8033B56E F4F8545D E7AC23F4 88A8BBBE C676D614 E9572429
        F0378106 0C66A36A 604AEE6E F22E5E1F 78E5BE71 61D51308
        E1C8D6CF EF2DE302 453C4CE9 20175EDA F99664C2 339D9F07


---------------------------

  returned_bits is
                                                   0469527C F922093E
        80F7C35F 96A4AA78 D57144E0 C55E2B17 AE42BD79 FB2BE771
        A19A474E EAE90D73 E28FEA0C E1EB2ED7 EA727875 11384F8C
        8033B56E F4F8545D E7AC23F4 88A8BBBE C676D614 E9572429
        F0378106 0C66A36A 604AEE6E F22E5E1F 78E5BE71 61D51308
        E1C8D6CF EF2DE302 453C4CE9 20175EDA F99664C2 339D9F07


  call Update(additional_input, K, V)
---------------------------

  Update
```

```
provided_data
                        606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


------------

V || 0x00 || provided_data is
                                          E7AC23F4 88A8BBBE
    C676D614 E9572429 F0378106 0C66A36A 604AEE6E F22E5E1F
    78E5BE71 61D51308 E1C8D6CF EF2DE302 453C4CE9 20175EDA
    F99664C2 339D9F07 00606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x00 || provided_data) is
                       052FF2F9 9579ABDD 989F7EC2 2A8ACFA6
    5AA83978 810A2F22 41A24CA4 0FF4468A 01775B2A 36D2600E
    817FD4B3 EDFCF755 E3E4BDBC A4109F1C 7F941774 13F91D0F


V = HMAC(K, V) is
                       6EFD8779 2A059B91 9F4E190C 1FE488F6
    5138C747 C2F76CC7 06E2C8F4 181FE8E3 36B464E6 518901A5
    03BC97AB 65E83467 C8C0FE34 EF0BD9DE CBFB4063 B4A30A40


------------

V || 0x01 || provided_data is
                                          6EFD8779 2A059B91
    9F4E190C 1FE488F6 5138C747 C2F76CC7 06E2C8F4 181FE8E3
    36B464E6 518901A5 03BC97AB 65E83467 C8C0FE34 EF0BD9DE
    CBFB4063 B4A30A40 01606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

```
    K = HMAC(K, V || 0x01 || provided_data) is
                            8C1D655B 79BB63C8 591A3016 D01F8122
        06557FEC 61DC13A6 1701CD4C 6A4597BF 13B908EB 9BA30A81
        D10DCB71 8364CD6B EC343E27 3F6AD936 B2A2598E 173F61DF


    V = HMAC(K, V) is
                            53BC68C9 F6692CD1 A94C8376 AB7C076C
        5EFE2681 26197A3F 2A3045B1 4E9B1AE3 A3BD944C 254BDCF1
        94A81F9A 70EE34F9 8DCF0D92 B63C4B2C 2DFA523C DC32B6CF


rnd_val is
                                                0469527C F922093E
        80F7C35F 96A4AA78 D57144E0 C55E2B17 AE42BD79 FB2BE771
        A19A474E EAE90D73 E28FEA0C E1EB2ED7 EA727875 11384F8C
        8033B56E F4F8545D E7AC23F4 88A8BBBE C676D614 E9572429
        F0378106 0C66A36A 604AEE6E F22E5E1F 78E5BE71 61D51308
        E1C8D6CF EF2DE302 453C4CE9 20175EDA F99664C2 339D9F07


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is
                              A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  additional_input <> NULL, call Update(additional_input, K, V)
----------------------------

  Update

    provided_data
                              A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
```

```
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


------------

V || 0x00 || provided_data is
                                          53BC68C9 F6692CD1
    A94C8376 AB7C076C 5EFE2681 26197A3F 2A3045B1 4E9B1AE3
    A3BD944C 254BDCF1 94A81F9A 70EE34F9 8DCF0D92 B63C4B2C
    2DFA523C DC32B6CF 00A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


K = HMAC(K, V || 0x00 || provided_data) is
                      040A763E 76ED2B13 78C2DEF1 AB37EFAF
    0A7E261E DC0D1415 48AE54AA 04139348 65F599E4 FB22CB2E
    13A72696 DBF90774 38CA4C18 40B9F97E C68C766E B05B5951


V = HMAC(K, V) is
                      9F3CCCA2 F3A2C033 AA36E1E2 3DA30378
    0BAABBC3 4E1C3687 FC2EC11A 09F20BD5 319EA959 8EEB0865
    6AB44A9E AD95F5C0 E2B0412A F918773C 07E0EB42 76D44191


------------

V || 0x01 || provided_data is
                                          9F3CCCA2 F3A2C033
    AA36E1E2 3DA30378 0BAABBC3 4E1C3687 FC2EC11A 09F20BD5
    319EA959 8EEB0865 6AB44A9E AD95F5C0 E2B0412A F918773C
    07E0EB42 76D44191 01A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


K = HMAC(K, V || 0x01 || provided_data) is
                      D4ECAA91 73A92CA6 3E0AFB0B 827518FA
```

```
        3868168A A43E877B A66F64FC A4D1AFCD EF0CCC2E 214A2ED2
        BA11BB2F 7D611FB9 5F4D0D8E 104EE0D6 512B8FEE 0EE593C5


    V = HMAC(K, V) is
                          020FD4F6 C9F76CB6 5CD6E603 1AB79A5A
        A8230594 7D8960FD 7080DD0E B4C7B81B 6BBCB568 1C4BC066
        50E3BCAB 5DF3A7C7 8EB729A3 CB440BF5 0276F507 D3591177


  ------------

    V = HMAC(K, V) is
                          15A45211 78CE9F71 D62DF426 ED92B3DA
        BD884880 A71405D7 D37217EB 0195FEC1 3B82C599 A9D5E22D
        9E577BC8 4FCF85D7 D490798B 1F3033DB 0A86D8BB 4B5C59D4


    temp is
                          15A45211 78CE9F71 D62DF426 ED92B3DA
        BD884880 A71405D7 D37217EB 0195FEC1 3B82C599 A9D5E22D
        9E577BC8 4FCF85D7 D490798B 1F3033DB 0A86D8BB 4B5C59D4


  ------------

    V = HMAC(K, V) is
                          8733D44B 4C9D831E B844329F A0B1C6B9
        56427905 30846F3A B4019E60 D6E7241C 17AA0710 9BBB6A8E
        D1E2B917 F7A7FA86 CCEA498F F18181E6 E1BED9F0 7B2F612F


    temp is
                                               15A45211 78CE9F71
        D62DF426 ED92B3DA BD884880 A71405D7 D37217EB 0195FEC1
        3B82C599 A9D5E22D 9E577BC8 4FCF85D7 D490798B 1F3033DB
        0A86D8BB 4B5C59D4 8733D44B 4C9D831E B844329F A0B1C6B9
        56427905 30846F3A B4019E60 D6E7241C 17AA0710 9BBB6A8E
        D1E2B917 F7A7FA86 CCEA498F F18181E6 E1BED9F0 7B2F612F


---------------------------

  returned_bits is
                                               15A45211 78CE9F71
        D62DF426 ED92B3DA BD884880 A71405D7 D37217EB 0195FEC1
```

```
        3B82C599 A9D5E22D 9E577BC8 4FCF85D7 D490798B 1F3033DB
        0A86D8BB 4B5C59D4 8733D44B 4C9D831E B844329F A0B1C6B9
        56427905 30846F3A B4019E60 D6E7241C 17AA0710 9BBB6A8E
        D1E2B917 F7A7FA86 CCEA498F F18181E6 E1BED9F0 7B2F612F


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    ------------

    V || 0x00 || provided_data is
                                              8733D44B 4C9D831E
        B844329F A0B1C6B9 56427905 30846F3A B4019E60 D6E7241C
        17AA0710 9BBB6A8E D1E2B917 F7A7FA86 CCEA498F F18181E6
        E1BED9F0 7B2F612F 00A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    K = HMAC(K, V || 0x00 || provided_data) is
                           95B0CAB3 9F589D71 C81F354A 7BB3AA72
        7FDAA35D DC5CEAF4 63158597 72CDF13C 34361836 23C73D2F
        77F5DFD4 90FDF012 49F825B0 24114FCA 5465E874 8D0B8878


    V = HMAC(K, V) is
                           6F7C0C89 81F9D7F3 03E99987 4D0AC1F2
        F37E8D01 7D119FF6 06F072F8 59EB1E54 BDB3F6F6 9F4A3DAF
        D85328D7 F99ECA8F C4046803 47A33EC7 E9D017B0 735BD55E


    ------------
```

```
    V || 0x01 || provided_data is
                                                6F7C0C89 81F9D7F3
        03E99987 4D0AC1F2 F37E8D01 7D119FF6 06F072F8 59EB1E54
        BDB3F6F6 9F4A3DAF D85328D7 F99ECA8F C4046803 47A33EC7
        E9D017B0 735BD55E 01A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    K = HMAC(K, V || 0x01 || provided_data) is
                           3216E702 D2ECD57A E0FC73CE 801F088D
        6274ED97 9F0BA437 4093215F 6B53D0F1 408B0D2D 79C81EAC
        2B194436 0A940B23 457BC989 C5C24EE3 5BD24312 04F5C950


    V = HMAC(K, V) is
                           75E0C067 A35850E0 CAAA84AE 4D61B409
        8D58EFF7 1118F6B2 065DC4AA 89FA3A44 6C49E753 59DC7F5F
        E9CC26E6 CBEBB461 1142DBBA 9DD102EF 67D6E7AF 981F969A


rnd_val is
                                                15A45211 78CE9F71
        D62DF426 ED92B3DA BD884880 A71405D7 D37217EB 0195FEC1
        3B82C599 A9D5E22D 9E577BC8 4FCF85D7 D490798B 1F3033DB
        0A86D8BB 4B5C59D4 8733D44B 4C9D831E B844329F A0B1C6B9
        56427905 30846F3A B4019E60 D6E7241C 17AA0710 9BBB6A8E
        D1E2B917 F7A7FA86 CCEA498F F18181E6 E1BED9F0 7B2F612F


##############################################################

HMAC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
```

```
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString =
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    AdditionalInput = <empty>

##################################################################

******************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E
```

```
    nonce is
                          20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
                            404142 43444546 4748494A 4B4C4D4E
          4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
          6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
          7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
          9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
          16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
          2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
          46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
          5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
          2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
          4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
          6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
          7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
          9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  Key is
                          00000000 00000000 00000000 00000000
          00000000 00000000 00000000 00000000 00000000 00000000
          00000000 00000000 00000000 00000000 00000000 00000000


  V is
                          01010101 01010101 01010101 01010101
          01010101 01010101 01010101 01010101 01010101 01010101
          01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
```

```
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
    46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
    5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
    2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


------------

V || 0x00 || provided_data is
                        010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 01010101 01010101
    01000001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
    46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
    5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
    2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


K = HMAC(K, V || 0x00 || provided_data) is
                       8FE3241B 7CEC3C91 831FEBC5 664A324E
    CE7885EC 0CFB79F0 A110CDDA 5C25FBDF 2724481F E501C813
    656BAC39 9CE61ABA DA1D0D75 7B2AB666 F4C98216 C1482F59


V = HMAC(K, V) is
                       496DABED 7FE15C71 16E221B4 30EE825C
    72A53FC3 49091FBF 5060584F CF9BAA56 70592E2F BB7E0E5A
    AD170616 E98B6DC8 BC4D77A2 EA17DFDE 4E64B0DF 260D9DCB


------------

V || 0x01 || provided_data is
                        496DAB ED7FE15C 7116E221 B430EE82
    5C72A53F C349091F BF506058 4FCF9BAA 5670592E 2FBB7E0E
```

```
        5AAD1706 16E98B6D C8BC4D77 A2EA17DF DE4E64B0 DF260D9D
        CB010001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    K = HMAC(K, V || 0x01 || provided_data) is
                        96477F38 6DC67E91 FBE26228 31E00384
        E017C17F 654AD9B7 1B2395A1 870D0BC2 48378809 87061D81
        EE39A9B2 EC5E9F65 98193BB8 43F3EFA8 D82C0CA7 F5543BF1


    V = HMAC(K, V) is
                        FAE68E0C ED06928D 3D6EC078 2D3FF3ED
        D3E6D364 B11EF22B 715D26C4 4850F01D 7074E6C8 13109CD4
        8BD91FC8 678E972C 205511E4 3622F079 72ADB6BC 61BE4F7E


  Update (Key, V):

    Key is
                        96477F38 6DC67E91 FBE26228 31E00384
        E017C17F 654AD9B7 1B2395A1 870D0BC2 48378809 87061D81
        EE39A9B2 EC5E9F65 98193BB8 43F3EFA8 D82C0CA7 F5543BF1


    V is
                        FAE68E0C ED06928D 3D6EC078 2D3FF3ED
        D3E6D364 B11EF22B 715D26C4 4850F01D 7074E6C8 13109CD4
        8BD91FC8 678E972C 205511E4 3622F079 72ADB6BC 61BE4F7E


---------------------------------------------------------------

First call to Generate

***************************************************************

HMAC_DRBG_Generate
```

```
  requested_number_of_bits = 1024

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                          2A5FF652 0C20F66E D5EA431B D4AEAC58
        F975EEC9 A015137D 5C94B73A A09CB8B5 9D611DDE ECEB34A5
        2BB99942 4009EB9E AC5353F9 2A6699D2 0A02164E EBBC6492


    temp is
                          2A5FF652 0C20F66E D5EA431B D4AEAC58
        F975EEC9 A015137D 5C94B73A A09CB8B5 9D611DDE ECEB34A5
        2BB99942 4009EB9E AC5353F9 2A6699D2 0A02164E EBBC6492


  ------------

    V = HMAC(K, V) is
                          941E1042 63238984 65DFD731 C7E04730
        60A5AA89 73841FDF 3446FB6E 72A58DA8 BDA2A57A 36F3DD98
        6DF85C8A 5C6FF31C DE660BF8 A841B21D D6AA9D3A C356B87B


    temp is
                                             2A5FF652 0C20F66E
        D5EA431B D4AEAC58 F975EEC9 A015137D 5C94B73A A09CB8B5
        9D611DDE ECEB34A5 2BB99942 4009EB9E AC5353F9 2A6699D2
        0A02164E EBBC6492 941E1042 63238984 65DFD731 C7E04730
        60A5AA89 73841FDF 3446FB6E 72A58DA8 BDA2A57A 36F3DD98
        6DF85C8A 5C6FF31C DE660BF8 A841B21D D6AA9D3A C356B87B


---------------------------

  returned_bits is
                                             2A5FF652 0C20F66E
        D5EA431B D4AEAC58 F975EEC9 A015137D 5C94B73A A09CB8B5
        9D611DDE ECEB34A5 2BB99942 4009EB9E AC5353F9 2A6699D2
        0A02164E EBBC6492 941E1042 63238984 65DFD731 C7E04730
        60A5AA89 73841FDF 3446FB6E 72A58DA8 BDA2A57A 36F3DD98
        6DF85C8A 5C6FF31C DE660BF8 A841B21D D6AA9D3A C356B87B
```

```
  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                       94 1E104263 23898465 DFD731C7 E0473060
        A5AA8973 841FDF34 46FB6E72 A58DA8BD A2A57A36 F3DD986D
        F85C8A5C 6FF31CDE 660BF8A8 41B21DD6 AA9D3AC3 56B87B00


    K = HMAC(K, V || 0x00 || provided_data) is
                         C2A6A666 D6EBF5F6 A96D1EDA 13AFA820
        8D388E17 C2DAE33A F5614506 C3686998 FA9728AC 17361C26
        6FB28BB6 54D73642 DA5FD913 3B9BCA86 6920A66F 332ADE84


    V = HMAC(K, V) is
                         F644A36F 1D274552 CCA57438 296DB616
        9C727402 7367C3D2 E3BD1A99 8DD31B10 9401B2A9 E7D5E5DF
        C05F5AA4 677B3D6F 7867E944 81922620 8F607119 ED71709A


rnd_val is
                                             2A5FF652 0C20F66E
        D5EA431B D4AEAC58 F975EEC9 A015137D 5C94B73A A09CB8B5
        9D611DDE ECEB34A5 2BB99942 4009EB9E AC5353F9 2A6699D2
        0A02164E EBBC6492 941E1042 63238984 65DFD731 C7E04730
        60A5AA89 73841FDF 3446FB6E 72A58DA8 BDA2A57A 36F3DD98
        6DF85C8A 5C6FF31C DE660BF8 A841B21D D6AA9D3A C356B87B


-------------------------------------------------------------

Second call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024
```

```
    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                          0EDC8D7D 7CEEC7FE 36333FB3 0C0A9A4B
        27AA0BEC BF075568 B006C1C3 693B1C29 0F84769C 213F98EB
        5880909E DF068FDA 6BFC4350 3987BBBD 4FC23AFB E982FE4B


    temp is
                          0EDC8D7D 7CEEC7FE 36333FB3 0C0A9A4B
        27AA0BEC BF075568 B006C1C3 693B1C29 0F84769C 213F98EB
        5880909E DF068FDA 6BFC4350 3987BBBD 4FC23AFB E982FE4B


  ------------

    V = HMAC(K, V) is
                          4B007910 CC4874EE C2174054 21C8D8A1
        BA87EC68 4D0AF9A6 101D9DB7 87AE82C3 A6A25ED4 78DF1B12
        212CEC32 5466F3AC 7C48A561 66DD0B11 9C8673A1 A9D54F67


    temp is
                                              0EDC8D7D 7CEEC7FE
        36333FB3 0C0A9A4B 27AA0BEC BF075568 B006C1C3 693B1C29
        0F84769C 213F98EB 5880909E DF068FDA 6BFC4350 3987BBBD
        4FC23AFB E982FE4B 4B007910 CC4874EE C2174054 21C8D8A1
        BA87EC68 4D0AF9A6 101D9DB7 87AE82C3 A6A25ED4 78DF1B12
        212CEC32 5466F3AC 7C48A561 66DD0B11 9C8673A1 A9D54F67


---------------------------

  returned_bits is
                                              0EDC8D7D 7CEEC7FE
        36333FB3 0C0A9A4B 27AA0BEC BF075568 B006C1C3 693B1C29
        0F84769C 213F98EB 5880909E DF068FDA 6BFC4350 3987BBBD
        4FC23AFB E982FE4B 4B007910 CC4874EE C2174054 21C8D8A1
        BA87EC68 4D0AF9A6 101D9DB7 87AE82C3 A6A25ED4 78DF1B12
        212CEC32 5466F3AC 7C48A561 66DD0B11 9C8673A1 A9D54F67


  call Update(additional_input, K, V)
```

```
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                      4B 007910CC 4874EEC2 17405421 C8D8A1BA
        87EC684D 0AF9A610 1D9DB787 AE82C3A6 A25ED478 DF1B1221
        2CEC3254 66F3AC7C 48A56166 DD0B119C 8673A1A9 D54F6700


    K = HMAC(K, V || 0x00 || provided_data) is
                           AB5E2153 B7DFBE45 7FCE345B 7DADCA8D
        5BFB3C98 58C36ECD F124C147 23B4CD39 F446E749 440FE69D
        D05E625F DC4625AC 8B7A47C5 465590E6 4662DB37 986C1335


    V = HMAC(K, V) is
                           02D99E7B 03B96288 2D288D60 AF87C466
        82FB7E21 13461E2B 3652EDF4 86DCE759 1BD5BE18 A78CFD69
        5E5B5C51 F72AC509 5DB5D786 C432EE91 FE8B292C 2309E470


rnd_val is
                                                0EDC8D7D 7CEEC7FE
        36333FB3 0C0A9A4B 27AA0BEC BF075568 B006C1C3 693B1C29
        0F84769C 213F98EB 5880909E DF068FDA 6BFC4350 3987BBBD
        4FC23AFB E982FE4B 4B007910 CC4874EE C2174054 21C8D8A1
        BA87EC68 4D0AF9A6 101D9DB7 87AE82C3 A6A25ED4 78DF1B12
        212CEC32 5466F3AC 7C48A561 66DD0B11 9C8673A1 A9D54F67


##############################################################

HMAC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                             000102 03040506 0708090A 0B0C0D0E
```

```
    0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
    2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
    3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
    5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


EntropyInput1 (for Reseed1) =
                         808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


EntropyInput2 (for Reseed2) =
                         C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Nonce =
                       20212223 24252627 28292A2B 2C2D2E2F


PersonalizationString =
                         404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


AdditionalInput1 =
                         606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


AdditionalInput2 =
                         A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
```

DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E

##

****

HMAC_DRBG_Instantiate_algorithm

entropy_input is
000102 03040506 0708090A 0B0C0D0E
0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E

nonce is
20212223 24252627 28292A2B 2C2D2E2F

personal_str is
404142 43444546 4748494A 4B4C4D4E
4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE

prediction_resistance_flag = "No PredictionResistance"

Seed_Material is
0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE

Key is

```
                        00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                        01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


----------------------------

  Update

    provided_data
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    ------------

    V || 0x00 || provided_data is
                           010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01000001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
```

```
  K = HMAC(K, V || 0x00 || provided_data) is
                        8FE3241B 7CEC3C91 831FEBC5 664A324E
      CE7885EC 0CFB79F0 A110CDDA 5C25FBDF 2724481F E501C813
      656BAC39 9CE61ABA DA1D0D75 7B2AB666 F4C98216 C1482F59


  V = HMAC(K, V) is
                        496DABED 7FE15C71 16E221B4 30EE825C
      72A53FC3 49091FBF 5060584F CF9BAA56 70592E2F BB7E0E5A
      AD170616 E98B6DC8 BC4D77A2 EA17DFDE 4E64B0DF 260D9DCB


  ------------

  V || 0x01 || provided_data is
                          496DAB ED7FE15C 7116E221 B430EE82
      5C72A53F C349091F BF506058 4FCF9BAA 5670592E 2FBB7E0E
      5AAD1706 16E98B6D C8BC4D77 A2EA17DF DE4E64B0 DF260D9D
      CB010001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
      16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
      2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
      46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
      5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
      2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
      4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
      9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  K = HMAC(K, V || 0x01 || provided_data) is
                        96477F38 6DC67E91 FBE26228 31E00384
      E017C17F 654AD9B7 1B2395A1 870D0BC2 48378809 87061D81
      EE39A9B2 EC5E9F65 98193BB8 43F3EFA8 D82C0CA7 F5543BF1


  V = HMAC(K, V) is
                        FAE68E0C ED06928D 3D6EC078 2D3FF3ED
      D3E6D364 B11EF22B 715D26C4 4850F01D 7074E6C8 13109CD4
      8BD91FC8 678E972C 205511E4 3622F079 72ADB6BC 61BE4F7E


Update (Key, V):

  Key is
                        96477F38 6DC67E91 FBE26228 31E00384
```

```
        E017C17F 654AD9B7 1B2395A1 870D0BC2 48378809 87061D81
        EE39A9B2 EC5E9F65 98193BB8 43F3EFA8 D82C0CA7 F5543BF1


    V is
                            FAE68E0C ED06928D 3D6EC078 2D3FF3ED
        D3E6D364 B11EF22B 715D26C4 4850F01D 7074E6C8 13109CD4
        8BD91FC8 678E972C 205511E4 3622F079 72ADB6BC 61BE4F7E


---------------------------------------------------------------

First call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is
                              606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


  additional_input <> NULL, call Update(additional_input, K, V)
----------------------------

  Update

    provided_data
                              606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    ------------

    V || 0x00 || provided_data is
                                                FAE68E0C ED06928D
        3D6EC078 2D3FF3ED D3E6D364 B11EF22B 715D26C4 4850F01D
```

```
    7074E6C8 13109CD4 8BD91FC8 678E972C 205511E4 3622F079
    72ADB6BC 61BE4F7E 00606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x00 || provided_data) is
                      519297BD B0EDA5D1 084F8B3B C203347D
    0C930D32 CEE2E49D F4BACBC6 D83AF8D9 EBD72991 B42C248E
    CD4EFAE9 1021F388 381D8659 A2ECBEEE F3E41952 E7A2451A


V = HMAC(K, V) is
                      D7DA4ED0 3A73A57B 54BF8D1D 33A1593D
    69FFDCA4 D66D74D9 89301F48 A8922EC0 E221977F 8F470A9B
    9486B5B6 DC9D7214 59A2A371 444894DE 0C09A8C8 9E599256


------------

V || 0x01 || provided_data is
                                          D7DA4ED0 3A73A57B
    54BF8D1D 33A1593D 69FFDCA4 D66D74D9 89301F48 A8922EC0
    E221977F 8F470A9B 9486B5B6 DC9D7214 59A2A371 444894DE
    0C09A8C8 9E599256 01606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x01 || provided_data) is
                      CEFBD1FE AB9E394C 0BB8AEEA A0432A7F
    6F1B3A0B 3ECB72E9 D08AF37E 1DC7D7B9 7C173D7D B2711ECA
    EA8AFD3F 138E7097 13401FCC D1E813A9 0BFA720E 39A765CB


V = HMAC(K, V) is
                      653FED49 BF632DDF 3EC4182C 3ECB3BE1
    CE9C05A8 231E90F1 7BA624C7 366131F9 876CB3E9 C27C453C
    1DF40471 07BADDD9 81D09078 C2D9C3FC 094A2BDC 0A8405BB


------------
```

```
    V = HMAC(K, V) is
                          7AE31A2D EC31075F E5972660 C16D22EC
        C0D415C5 693001BE 5A468B59 0BC1AE2C 43F647F8 D681AEEA
        0D87B79B 0B4E5D08 9CA2C9D3 27534234 0254E6B0 4690D77A


    temp is
                          7AE31A2D EC31075F E5972660 C16D22EC
        C0D415C5 693001BE 5A468B59 0BC1AE2C 43F647F8 D681AEEA
        0D87B79B 0B4E5D08 9CA2C9D3 27534234 0254E6B0 4690D77A


  ------------

    V = HMAC(K, V) is
                          71A294DA 9568479E EF8BB2A2 110F18B6
        22F60F35 235DE0E8 F9D7E981 05D84AA2 4AF0757A F005DFD5
        2FA51DE3 F44FCE0C 5F3A27FC E8B0F6E4 A3F7C7B5 3CE34A3D


    temp is
                                              7AE31A2D EC31075F
        E5972660 C16D22EC C0D415C5 693001BE 5A468B59 0BC1AE2C
        43F647F8 D681AEEA 0D87B79B 0B4E5D08 9CA2C9D3 27534234
        0254E6B0 4690D77A 71A294DA 9568479E EF8BB2A2 110F18B6
        22F60F35 235DE0E8 F9D7E981 05D84AA2 4AF0757A F005DFD5
        2FA51DE3 F44FCE0C 5F3A27FC E8B0F6E4 A3F7C7B5 3CE34A3D


---------------------------

  returned_bits is
                                              7AE31A2D EC31075F
        E5972660 C16D22EC C0D415C5 693001BE 5A468B59 0BC1AE2C
        43F647F8 D681AEEA 0D87B79B 0B4E5D08 9CA2C9D3 27534234
        0254E6B0 4690D77A 71A294DA 9568479E EF8BB2A2 110F18B6
        22F60F35 235DE0E8 F9D7E981 05D84AA2 4AF0757A F005DFD5
        2FA51DE3 F44FCE0C 5F3A27FC E8B0F6E4 A3F7C7B5 3CE34A3D


  call Update(additional_input, K, V)
---------------------------

  Update
```

```
provided_data
                        606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


------------

V || 0x00 || provided_data is
                                          71A294DA 9568479E
    EF8BB2A2 110F18B6 22F60F35 235DE0E8 F9D7E981 05D84AA2
    4AF0757A F005DFD5 2FA51DE3 F44FCE0C 5F3A27FC E8B0F6E4
    A3F7C7B5 3CE34A3D 00606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x00 || provided_data) is
                        40587E1D 5EB9F3D1 A6811767 EFA6A242
    1122DF2D EF5CC623 0A987605 7513A4F0 0ADB49E4 4A98478F
    6ED3A236 232B748E BAD48809 19D8C114 F8B02820 35763FE2


V = HMAC(K, V) is
                        58D27756 7DFE2227 FB9D105E 672EB72B
    CB08C9B5 EBCA5F19 753AE981 FCCFA587 00DC0586 87E29642
    D7E7CC30 10C82510 079EB2F4 DF4795B8 E1FF6499 E05551F1


------------

V || 0x01 || provided_data is
                                          58D27756 7DFE2227
    FB9D105E 672EB72B CB08C9B5 EBCA5F19 753AE981 FCCFA587
    00DC0586 87E29642 D7E7CC30 10C82510 079EB2F4 DF4795B8
    E1FF6499 E05551F1 01606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

```
    K = HMAC(K, V || 0x01 || provided_data) is
                          C64282B6 5A169138 8C94D85B 470D6FB3
        9DA80F71 A59D1160 C96B1FFC 0F77EDF9 11553ADC 552FC5B9
        9BDE010F 861FB90E 1EC9CD69 BA6B0C62 490D43FD 9FA6FE19


    V = HMAC(K, V) is
                          F12FA531 40E9A7DE 07D1EA08 3E31AF42
        5836A08F B59D2B1C 463263AD D1D4FCAD 5DA77F94 BE3E1A6A
        ACFC8845 33A2B5F6 685D6F66 F77D333A 43A119D9 56577B47


rnd_val is
                                              7AE31A2D EC31075F
        E5972660 C16D22EC C0D415C5 693001BE 5A468B59 0BC1AE2C
        43F647F8 D681AEEA 0D87B79B 0B4E5D08 9CA2C9D3 27534234
        0254E6B0 4690D77A 71A294DA 9568479E EF8BB2A2 110F18B6
        22F60F35 235DE0E8 F9D7E981 05D84AA2 4AF0757A F005DFD5
        2FA51DE3 F44FCE0C 5F3A27FC E8B0F6E4 A3F7C7B5 3CE34A3D


------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
```

```
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


------------

V || 0x00 || provided_data is
                                        F12FA531 40E9A7DE
    07D1EA08 3E31AF42 5836A08F B59D2B1C 463263AD D1D4FCAD
    5DA77F94 BE3E1A6A ACFC8845 33A2B5F6 685D6F66 F77D333A
    43A119D9 56577B47 00A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


K = HMAC(K, V || 0x00 || provided_data) is
                        66CDD877 BDBC01F0 B8C593E6 DB68698D
    3EA26EC3 D7EACB28 48091406 E371CFFD DE5FD3A7 D0F689AA
    C754C53C 9F5F51B4 A876BA90 25E6812B 15DF9C94 B4513C3C


V = HMAC(K, V) is
                        CB042B0E F4D993CF 753DBDAE E68D7E0E
    1E361D00 0EEE983F E53293AB 859E90E8 B12F7C18 85AD2795
    E8D52968 48C450C2 0942DA83 130898BE 39A9FCAB 49C7D4FE


------------

V || 0x01 || provided_data is
                                        CB042B0E F4D993CF
    753DBDAE E68D7E0E 1E361D00 0EEE983F E53293AB 859E90E8
    B12F7C18 85AD2795 E8D52968 48C450C2 0942DA83 130898BE
    39A9FCAB 49C7D4FE 01A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


K = HMAC(K, V || 0x01 || provided_data) is
                        EA829A96 FF1A6598 A63F82AC 4683837D
```

```
        46957868 3AF5D469 47146C05 16A1B3BC 7F32B337 EC80B0DF
        D40F7A56 F2520441 A7EBC2F5 F449FA1C 9F80B624 189FE4DF


    V = HMAC(K, V) is
                         4A97F3E7 84A888F2 CF6ACE46 3C0AA6C1
        5F3F2E58 7AA021B7 4DB140D4 C629E42F 87D3A5CE 78BCA47A
        A30CAB16 91020EF2 A5C40821 871D9C21 343DCE92 988697BE


  ------------

    V = HMAC(K, V) is
                         D83A8084 630F286D A4DB49B9 F6F608C8
        993F7F13 97EA0D6F 4A72CF3E F2733A11 AB823C29 F2EBDEC3
        EDE962F9 3D920A1D B59C84E1 E879C29F 5F9995FC 3A6A3AF9


    temp is
                         D83A8084 630F286D A4DB49B9 F6F608C8
        993F7F13 97EA0D6F 4A72CF3E F2733A11 AB823C29 F2EBDEC3
        EDE962F9 3D920A1D B59C84E1 E879C29F 5F9995FC 3A6A3AF9


  ------------

    V = HMAC(K, V) is
                         B587CA7C 13EA197D 423E81E1 D6469942
        B6E2CA83 A97E91F6 B298266A C148A180 9776C26A F5E239A5
        5A2BEB9E 752203A6 94E1F3FE 2B3E6A0C 9C314421 CDB55FBD


    temp is
                                              D83A8084 630F286D
        A4DB49B9 F6F608C8 993F7F13 97EA0D6F 4A72CF3E F2733A11
        AB823C29 F2EBDEC3 EDE962F9 3D920A1D B59C84E1 E879C29F
        5F9995FC 3A6A3AF9 B587CA7C 13EA197D 423E81E1 D6469942
        B6E2CA83 A97E91F6 B298266A C148A180 9776C26A F5E239A5
        5A2BEB9E 752203A6 94E1F3FE 2B3E6A0C 9C314421 CDB55FBD


---------------------------

  returned_bits is
                                              D83A8084 630F286D
        A4DB49B9 F6F608C8 993F7F13 97EA0D6F 4A72CF3E F2733A11
```

```
        AB823C29 F2EBDEC3 EDE962F9 3D920A1D B59C84E1 E879C29F
        5F9995FC 3A6A3AF9 B587CA7C 13EA197D 423E81E1 D6469942
        B6E2CA83 A97E91F6 B298266A C148A180 9776C26A F5E239A5
        5A2BEB9E 752203A6 94E1F3FE 2B3E6A0C 9C314421 CDB55FBD


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    ------------

    V || 0x00 || provided_data is
                                              B587CA7C 13EA197D
        423E81E1 D6469942 B6E2CA83 A97E91F6 B298266A C148A180
        9776C26A F5E239A5 5A2BEB9E 752203A6 94E1F3FE 2B3E6A0C
        9C314421 CDB55FBD 00A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    K = HMAC(K, V || 0x00 || provided_data) is
                            715D6185 7CE5456B 7FABA13E ABA449AB
        EE0D7EA0 EA9B2530 62733A9F DAF8EB82 A2896F50 6F71B24A
        1A765247 7051C55C A3FA8C92 8D47B5B2 4EBF0FE3 144CF727


    V = HMAC(K, V) is
                            44894C5E D321DD8E 80C4171B 1C97965D
        E5BBCF20 33ECCE57 1F0EBF27 1FF4559A 42D39CFD 2473F47E
        6FB9BF00 32DB08FA 5702D025 FD52FC7D ECEAA4FB AADED3A1


    ------------
```

```
    V || 0x01 || provided_data is
                                                44894C5E D321DD8E
        80C4171B 1C97965D E5BBCF20 33ECCE57 1F0EBF27 1FF4559A
        42D39CFD 2473F47E 6FB9BF00 32DB08FA 5702D025 FD52FC7D
        ECEAA4FB AADED3A1 01A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    K = HMAC(K, V || 0x01 || provided_data) is
                           43175BC3 737F59B4 6EE92380 8CF3DA53
        68933814 772FA1E8 4EFB1B7E E0F7C62E 0525A3D7 3D951FF4
        C9BE97DA D3722D12 ACA772FB D41D5100 5E50943F C5C95D6F


    V = HMAC(K, V) is
                           5575680B D05BA728 92CB32C4 7D8288E3
        8A0746C4 A23CECA7 5DFD1573 52165638 EFFBEA34 03DD40F1
        58B7B369 663D4B8C C1D280ED C34A1AB7 621746B1 DC0B924F


rnd_val is
                                                D83A8084 630F286D
        A4DB49B9 F6F608C8 993F7F13 97EA0D6F 4A72CF3E F2733A11
        AB823C29 F2EBDEC3 EDE962F9 3D920A1D B59C84E1 E879C29F
        5F9995FC 3A6A3AF9 B587CA7C 13EA197D 423E81E1 D6469942
        B6E2CA83 A97E91F6 B298266A C148A180 9776C26A F5E239A5
        5A2BEB9E 752203A6 94E1F3FE 2B3E6A0C 9C314421 CDB55FBD


##############################################################

HMAC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
```

```
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                          20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>
```

```
    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


  Key is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                          01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    ------------

    V || 0x00 || provided_data is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 00000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
```

```
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    K = HMAC(K, V || 0x00 || provided_data) is
                          45A111E3 AB3725B8 D02D1D8C A0AED099
        D32CF71C 2CA703C8 3708DDC3 AB0BDBEC 23719C1A 4C7273A8
        EB06EC14 B05853A0 793D492D C256DD1C 7DA4D148 BE8516CD


    V = HMAC(K, V) is
                          B4F4EAD4 4D45EF54 6C9CE52C C9B0B50F
        37948762 32662A75 B91B6150 E5BB1802 C68698C7 1E5BBCEB
        2C39FB40 CE3EF53D 4F092229 4CA844A1 6E67E2B2 710250CA


    ------------

    V || 0x01 || provided_data is
        B4F4EAD4 4D45EF54 6C9CE52C C9B0B50F 37948762 32662A75
        B91B6150 E5BB1802 C68698C7 1E5BBCEB 2C39FB40 CE3EF53D
        4F092229 4CA844A1 6E67E2B2 710250CA 01000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    K = HMAC(K, V || 0x01 || provided_data) is
                          A7E118A5 31DEF956 DCFF94BB 3D801F77
        5DC68F91 696A434C C25E270E 639044E1 A7240266 D3AA202D
        46C1054B 61024753 5007DF12 CFC8DA45 982A587F C81C47D5


    V = HMAC(K, V) is
                          110793EA A60DC9DB CD420810 4088A23D
        AECC1226 EAF1D03B BA9D83A6 95999165 71907346 B15A0439
        362B9C8E E330E52D EACC639B 98E8030A 95780CD7 C24B04D5


Update (Key, V):

    Key is
                          A7E118A5 31DEF956 DCFF94BB 3D801F77
        5DC68F91 696A434C C25E270E 639044E1 A7240266 D3AA202D
```

```
        46C1054B 61024753 5007DF12 CFC8DA45 982A587F C81C47D5


    V is
                         110793EA A60DC9DB CD420810 4088A23D
        AECC1226 EAF1D03B BA9D83A6 95999165 71907346 B15A0439
        362B9C8E E330E52D EACC639B 98E8030A 95780CD7 C24B04D5


------------------------------------------------------------

First call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                           808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    additional_input is  <empty>

  Seed_Material is
                           808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  Key is
                         A7E118A5 31DEF956 DCFF94BB 3D801F77
```

```
        5DC68F91 696A434C C25E270E 639044E1 A7240266 D3AA202D
        46C1054B 61024753 5007DF12 CFC8DA45 982A587F C81C47D5


  V is
                         110793EA A60DC9DB CD420810 4088A23D
        AECC1226 EAF1D03B BA9D83A6 95999165 71907346 B15A0439
        362B9C8E E330E52D EACC639B 98E8030A 95780CD7 C24B04D5


---------------------------

  Update

    provided_data
                           808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    ------------

    V || 0x00 || provided_data is
                                              110793EA A60DC9DB
        CD420810 4088A23D AECC1226 EAF1D03B BA9D83A6 95999165
        71907346 B15A0439 362B9C8E E330E52D EACC639B 98E8030A
        95780CD7 C24B04D5 00808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    K = HMAC(K, V || 0x00 || provided_data) is
                         55630E7A 8BD664AE AA8B1CE6 1EF6BF5B
        24656B8A 9F0667C9 C81A89E7 CB1269C8 408BD712 7A0E46D2
        4C2E03EC E2B62A08 B93045CC C808DC2B 9C195647 4790C2B3


    V = HMAC(K, V) is
                         4247B361 AF91E466 DC4C3C35 86EC9F3C
        FC6DAD2A 7C46902B 7A7FFC6C C618B605 0A48953C BBA0CF78
        0CBC76D6 E60B5FC6 9965D59F 6F8B66FB 4A2EAF68 99EC5447
```

```
    ------------

    V || 0x01 || provided_data is
                                              4247B361 AF91E466
        DC4C3C35 86EC9F3C FC6DAD2A 7C46902B 7A7FFC6C C618B605
        0A48953C BBA0CF78 0CBC76D6 E60B5FC6 9965D59F 6F8B66FB
        4A2EAF68 99EC5447 01808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    K = HMAC(K, V || 0x01 || provided_data) is
                          06CE30C3 A6C36878 BDE5C626 37F9454F
        A6F034FB A6751139 1DF82E7F F076B2DE CBCAC10F 15744E3F
        075C1DDF 46E934C6 EDDADDB9 CFC68587 467E2296 1D9166DC


    V = HMAC(K, V) is
                          59133BDF 3FEFAE3C AC734B81 F307CA18
        6D6E6228 2CD1BFFE 3F48E3FE 672C81BB 1325ACED 3AE6B1FF
        C386DC6A ECC8BB03 58CE2F43 7CE38674 4014A3BC 0CFAD33B


  Update (Key, V):

    Key is
                          06CE30C3 A6C36878 BDE5C626 37F9454F
        A6F034FB A6751139 1DF82E7F F076B2DE CBCAC10F 15744E3F
        075C1DDF 46E934C6 EDDADDB9 CFC68587 467E2296 1D9166DC


    V is
                          59133BDF 3FEFAE3C AC734B81 F307CA18
        6D6E6228 2CD1BFFE 3F48E3FE 672C81BB 1325ACED 3AE6B1FF
        C386DC6A ECC8BB03 58CE2F43 7CE38674 4014A3BC 0CFAD33B


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024
```

```
    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                          28FD6060 C4F35F4D 317AB206 0EE32019
        E0DAA330 F3F5650B BCA57CB6 7EE6AF1C 6F25D1B0 1F3601ED
        A85DC2ED 29A9B2BA 4C85CF49 1CE7185F 1A2BD937 8AE3C655


    temp is
                          28FD6060 C4F35F4D 317AB206 0EE32019
        E0DAA330 F3F5650B BCA57CB6 7EE6AF1C 6F25D1B0 1F3601ED
        A85DC2ED 29A9B2BA 4C85CF49 1CE7185F 1A2BD937 8AE3C655


  ------------

    V = HMAC(K, V) is
                          BD1CEC2E E108AE7F C382989F 6D4FEA8A
        B0149969 7C2F0794 5CE02C5E D617D042 87FEAF3B A638A4CE
        F3BB6B82 7E40AF16 279580FC F1FDAD83 0930F7FD E341E2AF


    temp is
                                              28FD6060 C4F35F4D
        317AB206 0EE32019 E0DAA330 F3F5650B BCA57CB6 7EE6AF1C
        6F25D1B0 1F3601ED A85DC2ED 29A9B2BA 4C85CF49 1CE7185F
        1A2BD937 8AE3C655 BD1CEC2E E108AE7F C382989F 6D4FEA8A
        B0149969 7C2F0794 5CE02C5E D617D042 87FEAF3B A638A4CE
        F3BB6B82 7E40AF16 279580FC F1FDAD83 0930F7FD E341E2AF


---------------------------

  returned_bits is
                                              28FD6060 C4F35F4D
        317AB206 0EE32019 E0DAA330 F3F5650B BCA57CB6 7EE6AF1C
        6F25D1B0 1F3601ED A85DC2ED 29A9B2BA 4C85CF49 1CE7185F
        1A2BD937 8AE3C655 BD1CEC2E E108AE7F C382989F 6D4FEA8A
        B0149969 7C2F0794 5CE02C5E D617D042 87FEAF3B A638A4CE
        F3BB6B82 7E40AF16 279580FC F1FDAD83 0930F7FD E341E2AF


  call Update(additional_input, K, V)
---------------------------
```

```
  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                        BD 1CEC2EE1 08AE7FC3 82989F6D 4FEA8AB0
        1499697C 2F07945C E02C5ED6 17D04287 FEAF3BA6 38A4CEF3
        BB6B827E 40AF1627 9580FCF1 FDAD8309 30F7FDE3 41E2AF00


    K = HMAC(K, V || 0x00 || provided_data) is
                           744B3A07 D75D8FA7 C894A730 C642D564
        71291E34 A93CE631 8BB20CC0 576F1142 1F332C9A 2A596B2D
        410ED227 DAD3520A 9D6C8A72 2CDDC825 B4C5DEF3 87FABF86


    V = HMAC(K, V) is
                           5918A9CE AA04C275 3BD95BD2 4BDA176C
        7A73E42E A519AC98 B95BB900 5D7065AD 715D9F55 0C95D4DB
        3A4E6774 B352DBC6 5344B54A 828727F8 86D67426 DB5E1997


rnd_val is
                                              28FD6060 C4F35F4D
        317AB206 0EE32019 E0DAA330 F3F5650B BCA57CB6 7EE6AF1C
        6F25D1B0 1F3601ED A85DC2ED 29A9B2BA 4C85CF49 1CE7185F
        1A2BD937 8AE3C655 BD1CEC2E E108AE7F C382989F 6D4FEA8A
        B0149969 7C2F0794 5CE02C5E D617D042 87FEAF3B A638A4CE
        F3BB6B82 7E40AF16 279580FC F1FDAD83 0930F7FD E341E2AF


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>
```

```
Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    additional_input is  <empty>

  Seed_Material is
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  Key is
                          744B3A07 D75D8FA7 C894A730 C642D564
        71291E34 A93CE631 8BB20CC0 576F1142 1F332C9A 2A596B2D
        410ED227 DAD3520A 9D6C8A72 2CDDC825 B4C5DEF3 87FABF86


  V is
                          5918A9CE AA04C275 3BD95BD2 4BDA176C
        7A73E42E A519AC98 B95BB900 5D7065AD 715D9F55 0C95D4DB
        3A4E6774 B352DBC6 5344B54A 828727F8 86D67426 DB5E1997


---------------------------

  Update

    provided_data
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E
```

```
------------

V || 0x00 || provided_data is
                                          5918A9CE AA04C275
    3BD95BD2 4BDA176C 7A73E42E A519AC98 B95BB900 5D7065AD
    715D9F55 0C95D4DB 3A4E6774 B352DBC6 5344B54A 828727F8
    86D67426 DB5E1997 00C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


K = HMAC(K, V || 0x00 || provided_data) is
                      E21D7EEC 44625C70 56119BB4 C3D19587
    E72E44B3 CC75F1B3 0AA15AA5 69DF6CEF B25A7E73 F5C0D643
    2CEC282C 8A4223DA 10A228C1 4FF8F48F 32477C40 A0C68E3F


V = HMAC(K, V) is
                      6E7B9E62 F29C3F65 5F09DB28 9EAA8F92
    D7BD2C9E 88DB90E9 C4FEF91F 0D45F67B 6330E12F 1345BF1C
    DBE19BE6 D0017B92 CDC06E6A F84D056A 815EB4EF 2F8847F7


------------

V || 0x01 || provided_data is
                                          6E7B9E62 F29C3F65
    5F09DB28 9EAA8F92 D7BD2C9E 88DB90E9 C4FEF91F 0D45F67B
    6330E12F 1345BF1C DBE19BE6 D0017B92 CDC06E6A F84D056A
    815EB4EF 2F8847F7 01C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


K = HMAC(K, V || 0x01 || provided_data) is
                      5B7FDA36 07BFB790 442F742F 147E1722
    AB8880F3 66491ADB 3E338343 3E0D3238 F67146F6 96968B5F
    C2CF696F 3CBBE826 1167EF87 6A176071 23FE23E6 BBB8F891


V = HMAC(K, V) is
```

```
                        25069D7D 3C99972A D1816407 9061C5FC
        B12AA76F DB71519C 5C009B63 1DB75344 DB55BF4C A1080FE8
        893036DD 60C38A1B E0B8DB65 2E11B679 ACC3BD38 6DF6995B


  Update (Key, V):

    Key is
                        5B7FDA36 07BFB790 442F742F 147E1722
        AB8880F3 66491ADB 3E338343 3E0D3238 F67146F6 96968B5F
        C2CF696F 3CBBE826 1167EF87 6A176071 23FE23E6 BBB8F891


    V is
                        25069D7D 3C99972A D1816407 9061C5FC
        B12AA76F DB71519C 5C009B63 1DB75344 DB55BF4C A1080FE8
        893036DD 60C38A1B E0B8DB65 2E11B679 ACC3BD38 6DF6995B


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                        C0B1601A FE39338B 58DC2BE7 C256AEBE
        3C21C5A9 39BEEC7E 97B3528A C420F0C6 34184718 7666E0FF
        578A8EB0 A37809F8 77365A28 DF2FA0F0 6354A6F0 24967473


    temp is
                        C0B1601A FE39338B 58DC2BE7 C256AEBE
        3C21C5A9 39BEEC7E 97B3528A C420F0C6 34184718 7666E0FF
        578A8EB0 A37809F8 77365A28 DF2FA0F0 6354A6F0 24967473


  ------------

    V = HMAC(K, V) is
                        69375B9A 9D6B756F DC4A8FB3 08E08256
        9D79A85B B960F747 25662638 9A3B45B0 ABE7ECBC 39D5CD7B
```

```
        2C18DF2E 5FDE8C9B 8D43474C 54B6F983 94684459 29B438C7


    temp is
                                               C0B1601A FE39338B
        58DC2BE7 C256AEBE 3C21C5A9 39BEEC7E 97B3528A C420F0C6
        34184718 7666E0FF 578A8EB0 A37809F8 77365A28 DF2FA0F0
        6354A6F0 24967473 69375B9A 9D6B756F DC4A8FB3 08E08256
        9D79A85B B960F747 25662638 9A3B45B0 ABE7ECBC 39D5CD7B
        2C18DF2E 5FDE8C9B 8D43474C 54B6F983 94684459 29B438C7


---------------------------

  returned_bits is
                                               C0B1601A FE39338B
        58DC2BE7 C256AEBE 3C21C5A9 39BEEC7E 97B3528A C420F0C6
        34184718 7666E0FF 578A8EB0 A37809F8 77365A28 DF2FA0F0
        6354A6F0 24967473 69375B9A 9D6B756F DC4A8FB3 08E08256
        9D79A85B B960F747 25662638 9A3B45B0 ABE7ECBC 39D5CD7B
        2C18DF2E 5FDE8C9B 8D43474C 54B6F983 94684459 29B438C7


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                      69 375B9A9D 6B756FDC 4A8FB308 E082569D
        79A85BB9 60F74725 6626389A 3B45B0AB E7ECBC39 D5CD7B2C
        18DF2E5F DE8C9B8D 43474C54 B6F98394 68445929 B438C700


    K = HMAC(K, V || 0x00 || provided_data) is
                           3E88DDDE D73D0F04 35F64858 4E5FCA52
        9DD2DA82 71DD4977 48932721 71D40ACD 8F97E19B 1DC644B1
        49DFE2FB 46085F2D 62F99535 FC1C1B38 2684CFA0 1412AB09


    V = HMAC(K, V) is
                           E36E1391 DEE6220C 5CC7D84B B0D7DBB4
```

```
        1CC88316 5EF43866 E02F30C3 EE2AF4EC CF13F324 C69FF0C5
        0963BDA7 FAB59647 FC06E343 8F3A06D3 A4E48ABD 7ED1BA99


rnd_val is
                                              C0B1601A FE39338B
        58DC2BE7 C256AEBE 3C21C5A9 39BEEC7E 97B3528A C420F0C6
        34184718 7666E0FF 578A8EB0 A37809F8 77365A28 DF2FA0F0
        6354A6F0 24967473 69375B9A 9D6B756F DC4A8FB3 08E08256
        9D79A85B B960F747 25662638 9A3B45B0 ABE7ECBC 39D5CD7B
        2C18DF2E 5FDE8C9B 8D43474C 54B6F983 94684459 29B438C7


################################################################

HMAC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E
```

Nonce =
20212223 24252627 28292A2B 2C2D2E2F

PersonalizationString = <empty>

AdditionalInput1 =
606162 63646566 6768696A 6B6C6D6E
6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE

AdditionalInput2 =
A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E

##

****

HMAC_DRBG_Instantiate_algorithm

entropy_input is
000102 03040506 0708090A 0B0C0D0E
0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E

nonce is
20212223 24252627 28292A2B 2C2D2E2F

personal_str is <empty>

prediction_resistance_flag = "PredictionResistance"

Seed_Material is
000102 03040506

```
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


  Key is
                         00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                         01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    ------------

    V || 0x00 || provided_data is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 00000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    K = HMAC(K, V || 0x00 || provided_data) is
```

```
                        45A111E3 AB3725B8 D02D1D8C A0AED099
        D32CF71C 2CA703C8 3708DDC3 AB0BDBEC 23719C1A 4C7273A8
        EB06EC14 B05853A0 793D492D C256DD1C 7DA4D148 BE8516CD


    V = HMAC(K, V) is
                        B4F4EAD4 4D45EF54 6C9CE52C C9B0B50F
        37948762 32662A75 B91B6150 E5BB1802 C68698C7 1E5BBCEB
        2C39FB40 CE3EF53D 4F092229 4CA844A1 6E67E2B2 710250CA


    ------------

    V || 0x01 || provided_data is
        B4F4EAD4 4D45EF54 6C9CE52C C9B0B50F 37948762 32662A75
        B91B6150 E5BB1802 C68698C7 1E5BBCEB 2C39FB40 CE3EF53D
        4F092229 4CA844A1 6E67E2B2 710250CA 01000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    K = HMAC(K, V || 0x01 || provided_data) is
                        A7E118A5 31DEF956 DCFF94BB 3D801F77
        5DC68F91 696A434C C25E270E 639044E1 A7240266 D3AA202D
        46C1054B 61024753 5007DF12 CFC8DA45 982A587F C81C47D5


    V = HMAC(K, V) is
                        110793EA A60DC9DB CD420810 4088A23D
        AECC1226 EAF1D03B BA9D83A6 95999165 71907346 B15A0439
        362B9C8E E330E52D EACC639B 98E8030A 95780CD7 C24B04D5


Update (Key, V):

    Key is
                        A7E118A5 31DEF956 DCFF94BB 3D801F77
        5DC68F91 696A434C C25E270E 639044E1 A7240266 D3AA202D
        46C1054B 61024753 5007DF12 CFC8DA45 982A587F C81C47D5


    V is
                        110793EA A60DC9DB CD420810 4088A23D
```

AECC1226 EAF1D03B BA9D83A6 95999165 71907346 B15A0439
362B9C8E E330E52D EACC639B 98E8030A 95780CD7 C24B04D5

First call to Generate

****

HMAC_DRBG_Generate

requested_number_of_bits = 1024

additional_input is
606162 63646566 6768696A 6B6C6D6E
6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE

Generate FAILED: Reseed is required
****

HMAC_DRBG_Reseed_algorithm

entropy_input is
808182 83848586 8788898A 8B8C8D8E
8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE

additional_input is
606162 63646566 6768696A 6B6C6D6E
6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE

Seed_Material is
8081 82838485
86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D

```
        9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
        B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


  Key is
                        A7E118A5 31DEF956 DCFF94BB 3D801F77
        5DC68F91 696A434C C25E270E 639044E1 A7240266 D3AA202D
        46C1054B 61024753 5007DF12 CFC8DA45 982A587F C81C47D5


  V is
                        110793EA A60DC9DB CD420810 4088A23D
        AECC1226 EAF1D03B BA9D83A6 95999165 71907346 B15A0439
        362B9C8E E330E52D EACC639B 98E8030A 95780CD7 C24B04D5


---------------------------

  Update

    provided_data
                                                  8081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
        9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
        B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    ------------

    V || 0x00 || provided_data is
          110793 EAA60DC9 DBCD4208 104088A2 3DAECC12 26EAF1D0
        3BBA9D83 A6959991 65719073 46B15A04 39362B9C 8EE330E5
        2DEACC63 9B98E803 0A95780C D7C24B04 D5008081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
```

```
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x00 || provided_data) is
                      4886B37A A9D553BD 09ED84EF 277C1F08
    B7CE7FC5 8AB92D89 68D23154 7407016B 44402F9E 69404796
    C0FD87DB D1A9A4BE DB3247F0 900EE1EB 39DDB7CD B712EB23


V = HMAC(K, V) is
                      8EC05CF1 396D4E82 2B03E445 0859CE0F
    A9A1D9DA 3AB15FB7 7EC1B0A6 0E447853 836E64B8 34C46B04
    59DBD08F DB6EA145 AFAAD2FC 939584A2 91F141CF 55E8DFD4


------------

V || 0x01 || provided_data is
      8EC05C F1396D4E 822B03E4 450859CE 0FA9A1D9 DA3AB15F
    B77EC1B0 A60E4478 53836E64 B834C46B 0459DBD0 8FDB6EA1
    45AFAAD2 FC939584 A291F141 CF55E8DF D4018081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x01 || provided_data) is
                      91529DF9 C5C21BD7 141E05DB E7F3678C
    F4531EB0 110ED597 EBF65048 8EBEB6D1 B6D129F2 47697693
    2D2BD4CB 93F05DE7 40AAA7AF 28485952 1E06108F ABA4806C


V = HMAC(K, V) is
```

```
                        8C03B0DB 21C3F1F0 54027000 0CB3821E
        3D3C853A 90202E25 BD4AF86A 33A1A2CE 679A9006 C8A6054E
        84E2DF90 EEADDC78 EC20AC3C 7745B890 5AB4ED53 927BD958


  Update (Key, V):

    Key is
                        91529DF9 C5C21BD7 141E05DB E7F3678C
        F4531EB0 110ED597 EBF65048 8EBEB6D1 B6D129F2 47697693
        2D2BD4CB 93F05DE7 40AAA7AF 28485952 1E06108F ABA4806C


    V is
                        8C03B0DB 21C3F1F0 54027000 0CB3821E
        3D3C853A 90202E25 BD4AF86A 33A1A2CE 679A9006 C8A6054E
        84E2DF90 EEADDC78 EC20AC3C 7745B890 5AB4ED53 927BD958


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                        72691D21 03FB567C CD303707 15B36666
        F6343008 7B1C6882 81CA0974 DB456BDB A7EB5C48 CFF62EA0
        5F9508F3 B530CE99 5A272B11 EC079C13 923EEF8E 011A93C1


    temp is
                        72691D21 03FB567C CD303707 15B36666
        F6343008 7B1C6882 81CA0974 DB456BDB A7EB5C48 CFF62EA0
        5F9508F3 B530CE99 5A272B11 EC079C13 923EEF8E 011A93C1


  ------------

    V = HMAC(K, V) is
                        9B58CC67 16BC7CB8 BD886CAA 60C14D85
        C023348B D77738C4 75D6C7E1 D9BFF4B1 2C43D8CC 73F838DC
```

```
        4F8BD476 CF8328EE B71B3D87 3D6B7B85 9C9B2106 5638FF95


    temp is
                                               72691D21 03FB567C
        CD303707 15B36666 F6343008 7B1C6882 81CA0974 DB456BDB
        A7EB5C48 CFF62EA0 5F9508F3 B530CE99 5A272B11 EC079C13
        923EEF8E 011A93C1 9B58CC67 16BC7CB8 BD886CAA 60C14D85
        C023348B D77738C4 75D6C7E1 D9BFF4B1 2C43D8CC 73F838DC
        4F8BD476 CF8328EE B71B3D87 3D6B7B85 9C9B2106 5638FF95


---------------------------

  returned_bits is
                                               72691D21 03FB567C
        CD303707 15B36666 F6343008 7B1C6882 81CA0974 DB456BDB
        A7EB5C48 CFF62EA0 5F9508F3 B530CE99 5A272B11 EC079C13
        923EEF8E 011A93C1 9B58CC67 16BC7CB8 BD886CAA 60C14D85
        C023348B D77738C4 75D6C7E1 D9BFF4B1 2C43D8CC 73F838DC
        4F8BD476 CF8328EE B71B3D87 3D6B7B85 9C9B2106 5638FF95


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                       9B 58CC6716 BC7CB8BD 886CAA60 C14D85C0
        23348BD7 7738C475 D6C7E1D9 BFF4B12C 43D8CC73 F838DC4F
        8BD476CF 8328EEB7 1B3D873D 6B7B859C 9B210656 38FF9500


    K = HMAC(K, V || 0x00 || provided_data) is
                            9648218E 7084C7B9 4678C2DC 7495AC1C
        B8812E4C 7FD238E2 F1AE5C52 71649A36 8FF93E09 BD03465E
        8E11E568 7296575E 05972C3C A8F5ED9B 4D37817F 135FF5E2


    V = HMAC(K, V) is
                            509C5F6A ABABA9EA 799C530F 01EE5423
```

```
        8E6013B1 6DC1DB7A 4F6E36ED 2E0ED112 07E94187 C10AF321
        449765D1 63DFA6B8 B4A6A629 70D7D4E1 9DB67A89 F6FE098D


rnd_val is
                                            72691D21 03FB567C
        CD303707 15B36666 F6343008 7B1C6882 81CA0974 DB456BDB
        A7EB5C48 CFF62EA0 5F9508F3 B530CE99 5A272B11 EC079C13
        923EEF8E 011A93C1 9B58CC67 16BC7CB8 BD886CAA 60C14D85
        C023348B D77738C4 75D6C7E1 D9BFF4B1 2C43D8CC 73F838DC
        4F8BD476 CF8328EE B71B3D87 3D6B7B85 9C9B2106 5638FF95


------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                           C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    additional_input is
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
```

```
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  Seed_Material is
                                                C0C1 C2C3C4C5
      C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
      DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
      F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
      0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
      26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  Key is
                        9648218E 7084C7B9 4678C2DC 7495AC1C
      B8812E4C 7FD238E2 F1AE5C52 71649A36 8FF93E09 BD03465E
      8E11E568 7296575E 05972C3C A8F5ED9B 4D37817F 135FF5E2


  V is
                        509C5F6A ABABA9EA 799C530F 01EE5423
      8E6013B1 6DC1DB7A 4F6E36ED 2E0ED112 07E94187 C10AF321
      449765D1 63DFA6B8 B4A6A629 70D7D4E1 9DB67A89 F6FE098D


---------------------------

  Update

    provided_data
                                                C0C1 C2C3C4C5
      C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
      DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
      F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
      0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
      26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E
```

```
------------

V || 0x00 || provided_data is
      509C5F 6AABABA9 EA799C53 0F01EE54 238E6013 B16DC1DB
    7A4F6E36 ED2E0ED1 1207E941 87C10AF3 21449765 D163DFA6
    B8B4A6A6 2970D7D4 E19DB67A 89F6FE09 8D00C0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


K = HMAC(K, V || 0x00 || provided_data) is
                      E4550E14 6FA955BA 46A1DAA7 95A96A8A
    17603D79 BF97BA11 15445EA8 CBD036A5 4C2F1452 407A59F5
    EA0B78E8 9196552F 2C59EB4A 59424229 79F77768 905933D7


V = HMAC(K, V) is
                      C39717D6 DB739945 60D8F8B8 77E50871
    0FAEB012 07958974 7DBCD12F 8334E2EA DDEE361E 69D52AAA
    6DC0B1E3 2EF28F54 798C7DCD 8CCE64B8 773525DE DDEB4F28


------------

V || 0x01 || provided_data is
      C39717 D6DB7399 4560D8F8 B877E508 710FAEB0 12079589
    747DBCD1 2F8334E2 EADDEE36 1E69D52A AA6DC0B1 E32EF28F
    54798C7D CD8CCE64 B8773525 DEDDEB4F 2801C0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E
```

```
    K = HMAC(K, V || 0x01 || provided_data) is
                          3D8DA1FA D6F226D4 C5B8F1F1 B4A595B2
        21F33E44 62F8ABA2 F0D3CBC8 D27360C6 B295803F D893A019
        E96E4DD6 C0C56301 EB7D2DBD B67585FC 3AC3AA85 74CBC463


    V = HMAC(K, V) is
                          27E8D349 BC72C165 1861847B 585BCE91
        46D5FA9A 9FBE2820 106ECAC3 1E8B4525 A2FF70D5 2A1D25A3
        F42277B5 3564C37D D745B0F8 39D2CFD1 35B08DF6 54E68323


  Update (Key, V):

    Key is
                          3D8DA1FA D6F226D4 C5B8F1F1 B4A595B2
        21F33E44 62F8ABA2 F0D3CBC8 D27360C6 B295803F D893A019
        E96E4DD6 C0C56301 EB7D2DBD B67585FC 3AC3AA85 74CBC463


    V is
                          27E8D349 BC72C165 1861847B 585BCE91
        46D5FA9A 9FBE2820 106ECAC3 1E8B4525 A2FF70D5 2A1D25A3
        F42277B5 3564C37D D745B0F8 39D2CFD1 35B08DF6 54E68323


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                          8570DA3D 47E1E160 5CF3E44B 8D328B99
        5EFC6410 7B6292D1 B1036B5F 88CE3160 2F12BEB7 1D801C09
        42E7C086 4B3DB67A 9356DB20 3490D881 24FE86BC E38AC226


    temp is
                          8570DA3D 47E1E160 5CF3E44B 8D328B99
```

```
        5EFC6410 7B6292D1 B1036B5F 88CE3160 2F12BEB7 1D801C09
        42E7C086 4B3DB67A 9356DB20 3490D881 24FE86BC E38AC226


  ------------

    V = HMAC(K, V) is
                           9B4FDA6A BAA88403 9DF80A03 36A24D79
        1EB3067C 8F5F0CF0 F18DD73B 66A7B316 FB19E028 35CC6293
        65FCD1D3 BE640178 ED9093B9 1B36E1D6 8135F278 5BFF505C


    temp is
                                              8570DA3D 47E1E160
        5CF3E44B 8D328B99 5EFC6410 7B6292D1 B1036B5F 88CE3160
        2F12BEB7 1D801C09 42E7C086 4B3DB67A 9356DB20 3490D881
        24FE86BC E38AC226 9B4FDA6A BAA88403 9DF80A03 36A24D79
        1EB3067C 8F5F0CF0 F18DD73B 66A7B316 FB19E028 35CC6293
        65FCD1D3 BE640178 ED9093B9 1B36E1D6 8135F278 5BFF505C


---------------------------

  returned_bits is
                                              8570DA3D 47E1E160
        5CF3E44B 8D328B99 5EFC6410 7B6292D1 B1036B5F 88CE3160
        2F12BEB7 1D801C09 42E7C086 4B3DB67A 9356DB20 3490D881
        24FE86BC E38AC226 9B4FDA6A BAA88403 9DF80A03 36A24D79
        1EB3067C 8F5F0CF0 F18DD73B 66A7B316 FB19E028 35CC6293
        65FCD1D3 BE640178 ED9093B9 1B36E1D6 8135F278 5BFF505C


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                         9B 4FDA6ABA A884039D F80A0336 A24D791E
        B3067C8F 5F0CF0F1 8DD73B66 A7B316FB 19E02835 CC629365
        FCD1D3BE 640178ED 9093B91B 36E1D681 35F2785B FF505C00
```

```
    K = HMAC(K, V || 0x00 || provided_data) is
                          5ECC11F5 000DF823 E91EA756 E3F917C0
        0AD8B95C 526EABEE A1EDBCBF D38DA649 F762EBE0 B8FFA062
        B0715DD7 635206B7 A746CC4A FC7A54F4 33DB4428 F6212E53


    V = HMAC(K, V) is
                          FFA84AA8 DB1089F7 16ECEF15 9C628AF2
        48300647 39D87AF4 CBC64C48 6EB2DF2C F58EDB53 D3D3DE89
        C58E88CD DB569E57 DF32CC37 D3B3CC82 88786494 0273CB6E


rnd_val is
                                              8570DA3D 47E1E160
        5CF3E44B 8D328B99 5EFC6410 7B6292D1 B1036B5F 88CE3160
        2F12BEB7 1D801C09 42E7C086 4B3DB67A 9356DB20 3490D881
        24FE86BC E38AC226 9B4FDA6A BAA88403 9DF80A03 36A24D79
        1EB3067C 8F5F0CF0 F18DD73B 66A7B316 FB19E028 35CC6293
        65FCD1D3 BE640178 ED9093B9 1B36E1D6 8135F278 5BFF505C


################################################################

HMAC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE
```

```
    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString =
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    AdditionalInput = <empty>

###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                          20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
```

```
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  Key is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                          01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


--------------------------

  Update

    provided_data
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
```

```
------------

V || 0x00 || provided_data is
                         010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 01010101 01010101
    01000001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
    46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
    5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
    2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


K = HMAC(K, V || 0x00 || provided_data) is
                       8FE3241B 7CEC3C91 831FEBC5 664A324E
    CE7885EC 0CFB79F0 A110CDDA 5C25FBDF 2724481F E501C813
    656BAC39 9CE61ABA DA1D0D75 7B2AB666 F4C98216 C1482F59


V = HMAC(K, V) is
                       496DABED 7FE15C71 16E221B4 30EE825C
    72A53FC3 49091FBF 5060584F CF9BAA56 70592E2F BB7E0E5A
    AD170616 E98B6DC8 BC4D77A2 EA17DFDE 4E64B0DF 260D9DCB


------------

V || 0x01 || provided_data is
                         496DAB ED7FE15C 7116E221 B430EE82
    5C72A53F C349091F BF506058 4FCF9BAA 5670592E 2FBB7E0E
    5AAD1706 16E98B6D C8BC4D77 A2EA17DF DE4E64B0 DF260D9D
    CB010001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
    46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
    5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
    2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
```

```
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    K = HMAC(K, V || 0x01 || provided_data) is
                          96477F38 6DC67E91 FBE26228 31E00384
        E017C17F 654AD9B7 1B2395A1 870D0BC2 48378809 87061D81
        EE39A9B2 EC5E9F65 98193BB8 43F3EFA8 D82C0CA7 F5543BF1


    V = HMAC(K, V) is
                          FAE68E0C ED06928D 3D6EC078 2D3FF3ED
        D3E6D364 B11EF22B 715D26C4 4850F01D 7074E6C8 13109CD4
        8BD91FC8 678E972C 205511E4 3622F079 72ADB6BC 61BE4F7E


  Update (Key, V):

    Key is
                          96477F38 6DC67E91 FBE26228 31E00384
        E017C17F 654AD9B7 1B2395A1 870D0BC2 48378809 87061D81
        EE39A9B2 EC5E9F65 98193BB8 43F3EFA8 D82C0CA7 F5543BF1


    V is
                          FAE68E0C ED06928D 3D6EC078 2D3FF3ED
        D3E6D364 B11EF22B 715D26C4 4850F01D 7074E6C8 13109CD4
        8BD91FC8 678E972C 205511E4 3622F079 72ADB6BC 61BE4F7E


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm
```

```
    entropy_input is
                              808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    additional_input is  <empty>

  Seed_Material is
                              808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  Key is
                            96477F38 6DC67E91 FBE26228 31E00384
        E017C17F 654AD9B7 1B2395A1 870D0BC2 48378809 87061D81
        EE39A9B2 EC5E9F65 98193BB8 43F3EFA8 D82C0CA7 F5543BF1


  V is
                            FAE68E0C ED06928D 3D6EC078 2D3FF3ED
        D3E6D364 B11EF22B 715D26C4 4850F01D 7074E6C8 13109CD4
        8BD91FC8 678E972C 205511E4 3622F079 72ADB6BC 61BE4F7E


--------------------------

  Update

    provided_data
                              808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    ------------

    V || 0x00 || provided_data is
                                              FAE68E0C ED06928D
```

```
    3D6EC078 2D3FF3ED D3E6D364 B11EF22B 715D26C4 4850F01D
    7074E6C8 13109CD4 8BD91FC8 678E972C 205511E4 3622F079
    72ADB6BC 61BE4F7E 00808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


K = HMAC(K, V || 0x00 || provided_data) is
                      1F9C99C0 D27D726B F887D144 314EDE3B
    FB85FF51 DA2D8147 2C38432F 9592ABA2 A49E4194 A9D2EA4E
    2DF0141B B4EE22BA C263029D 8A1EA7DC 7AB8332D A48C9E66


V = HMAC(K, V) is
                      B63CF883 05CF1F68 986F1E96 3CBB5FE8
    C1ACA6B9 5DE8AFAF 4857BABE 48121DF7 42D1A6B6 1556F1B6
    09032ECA 7B4844BE 70F337FF FBECAE48 F772E2FF B1D840C2


------------

V || 0x01 || provided_data is
                                          B63CF883 05CF1F68
    986F1E96 3CBB5FE8 C1ACA6B9 5DE8AFAF 4857BABE 48121DF7
    42D1A6B6 1556F1B6 09032ECA 7B4844BE 70F337FF FBECAE48
    F772E2FF B1D840C2 01808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


K = HMAC(K, V || 0x01 || provided_data) is
                      E1E5F34B EF791518 4C9E49D1 2518A591
    C077845D 89C9DA00 A2C83950 43148800 818AE9CF 467A7A45
    DA939E96 E3064D99 1848F7AF 5911CA23 FACBD738 16ED0ED4


V = HMAC(K, V) is
                      A089C037 3C58AD2A 465E444D 33269678
    8C28F5BA FE54889B ADF0FEA3 46303EA4 F1933433 7836DB7B
    CB1FFF31 86EDE3B2 C3A8DEA7 D825D3CB 4714C0E1 90269466
```

```
  Update (Key, V):

    Key is
                          E1E5F34B EF791518 4C9E49D1 2518A591
        C077845D 89C9DA00 A2C83950 43148800 818AE9CF 467A7A45
        DA939E96 E3064D99 1848F7AF 5911CA23 FACBD738 16ED0ED4


    V is
                          A089C037 3C58AD2A 465E444D 33269678
        8C28F5BA FE54889B ADF0FEA3 46303EA4 F1933433 7836DB7B
        CB1FFF31 86EDE3B2 C3A8DEA7 D825D3CB 4714C0E1 90269466


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                          AAE4DC3C 9ECC74D9 061DD527 117EF3D2
        9E1E52B2 6853C539 D6CA797E 8DA3D0BB 171D8E30 B8B194D8
        C28F7F6B E3B986B8 8506DC6A 01B294A7 165DD1C3 470F7BE7


    temp is
                          AAE4DC3C 9ECC74D9 061DD527 117EF3D2
        9E1E52B2 6853C539 D6CA797E 8DA3D0BB 171D8E30 B8B194D8
        C28F7F6B E3B986B8 8506DC6A 01B294A7 165DD1C3 470F7BE7


  ------------

    V = HMAC(K, V) is
                          B396AA0D B7D50C40 51E7C7E1 C8A7D21A
        2B5878C0 BCB163CA A79366E7 A1162FDC 88429616 CD3E6977
        8D327520 A6BBBF71 D8AA2E03 EC4A9DAA 0E77CF93 E1EE30D2


    temp is
                                              AAE4DC3C 9ECC74D9
```

```
        061DD527 117EF3D2 9E1E52B2 6853C539 D6CA797E 8DA3D0BB
        171D8E30 B8B194D8 C28F7F6B E3B986B8 8506DC6A 01B294A7
        165DD1C3 470F7BE7 B396AA0D B7D50C40 51E7C7E1 C8A7D21A
        2B5878C0 BCB163CA A79366E7 A1162FDC 88429616 CD3E6977
        8D327520 A6BBBF71 D8AA2E03 EC4A9DAA 0E77CF93 E1EE30D2


---------------------------

  returned_bits is
                                                AAE4DC3C 9ECC74D9
        061DD527 117EF3D2 9E1E52B2 6853C539 D6CA797E 8DA3D0BB
        171D8E30 B8B194D8 C28F7F6B E3B986B8 8506DC6A 01B294A7
        165DD1C3 470F7BE7 B396AA0D B7D50C40 51E7C7E1 C8A7D21A
        2B5878C0 BCB163CA A79366E7 A1162FDC 88429616 CD3E6977
        8D327520 A6BBBF71 D8AA2E03 EC4A9DAA 0E77CF93 E1EE30D2


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                        B3 96AA0DB7 D50C4051 E7C7E1C8 A7D21A2B
        5878C0BC B163CAA7 9366E7A1 162FDC88 429616CD 3E69778D
        327520A6 BBBF71D8 AA2E03EC 4A9DAA0E 77CF93E1 EE30D200


    K = HMAC(K, V || 0x00 || provided_data) is
                            275F4A02 431A1B30 6DCA0A37 3BB9EA85
        039B1DE3 08227752 F9633D57 7854C73A 84886B9A 3C25819C
        EBDE8F16 8C1C8B06 3482BB6A 8AB54870 59A3876C 7710ACB4


    V = HMAC(K, V) is
                            FDA1F0F3 8D1D0BB7 0D29E9CC 05A4190E
        9D9D49CC 24000C8D F12CFC09 D4325714 C0F78B13 EC7A12D6
        EF1A380B 0C7B0563 0CD08D7F C77E43A8 755F47A5 B01A9E48


rnd_val is
```

```
                                                AAE4DC3C 9ECC74D9
        061DD527 117EF3D2 9E1E52B2 6853C539 D6CA797E 8DA3D0BB
        171D8E30 B8B194D8 C28F7F6B E3B986B8 8506DC6A 01B294A7
        165DD1C3 470F7BE7 B396AA0D B7D50C40 51E7C7E1 C8A7D21A
        2B5878C0 BCB163CA A79366E7 A1162FDC 88429616 CD3E6977
        8D327520 A6BBBF71 D8AA2E03 EC4A9DAA 0E77CF93 E1EE30D2


-----------------------------------------------------------

Second call to Generate

***********************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

Generate FAILED: Reseed is required
***********************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                           C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    additional_input is  <empty>

  Seed_Material is
                           C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  Key is
                         275F4A02 431A1B30 6DCA0A37 3BB9EA85
        039B1DE3 08227752 F9633D57 7854C73A 84886B9A 3C25819C
```

```
        EBDE8F16 8C1C8B06 3482BB6A 8AB54870 59A3876C 7710ACB4


  V is
                         FDA1F0F3 8D1D0BB7 0D29E9CC 05A4190E
        9D9D49CC 24000C8D F12CFC09 D4325714 C0F78B13 EC7A12D6
        EF1A380B 0C7B0563 0CD08D7F C77E43A8 755F47A5 B01A9E48


--------------------------

  Update

    provided_data
                           C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    ------------

    V || 0x00 || provided_data is
                                               FDA1F0F3 8D1D0BB7
        0D29E9CC 05A4190E 9D9D49CC 24000C8D F12CFC09 D4325714
        C0F78B13 EC7A12D6 EF1A380B 0C7B0563 0CD08D7F C77E43A8
        755F47A5 B01A9E48 00C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    K = HMAC(K, V || 0x00 || provided_data) is
                         2F4B184F 21910B66 079269B5 2708880D
        FFB6A73D 37962656 B91DB6CC 1157B4BA 65955979 373F928A
        B86269C1 DC89A604 B047B65F 5EB1AA11 D636E58A 5D13F645


    V = HMAC(K, V) is
                         2EB12A07 23BF0EE7 F0CE6B73 08510C62
        2C00D617 F3E5994E EBA9913B 87D01D28 17C82DFB FD3CB1DE
        D99E2C7D 4C9212D4 A95D492D 99E61F6E 4F9CEC02 490A6919
```

```
    ------------

    V || 0x01 || provided_data is
                                              2EB12A07 23BF0EE7
        F0CE6B73 08510C62 2C00D617 F3E5994E EBA9913B 87D01D28
        17C82DFB FD3CB1DE D99E2C7D 4C9212D4 A95D492D 99E61F6E
        4F9CEC02 490A6919 01C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    K = HMAC(K, V || 0x01 || provided_data) is
                          3C666E58 0DE3F6DB 662E8C00 EC31B6D9
        8F7DFB8A BB4DB1AD D0AA989C C2E71EF2 C5D41166 FAC63729
        E23B591C 0D1F11E7 D10AE714 6687CD2E 0ED9B738 9CD7DD35


    V = HMAC(K, V) is
                          26DBEAEF BCC48F41 D41077C2 ED286F67
        49FDC109 E24D372E 7DC20F0F 87037E4D FACCD39A 77807D5C
        8586CACE AEE75863 C9351C96 5678E46F DB77A739 FD123189


  Update (Key, V):

    Key is
                          3C666E58 0DE3F6DB 662E8C00 EC31B6D9
        8F7DFB8A BB4DB1AD D0AA989C C2E71EF2 C5D41166 FAC63729
        E23B591C 0D1F11E7 D10AE714 6687CD2E 0ED9B738 9CD7DD35


    V is
                          26DBEAEF BCC48F41 D41077C2 ED286F67
        49FDC109 E24D372E 7DC20F0F 87037E4D FACCD39A 77807D5C
        8586CACE AEE75863 C9351C96 5678E46F DB77A739 FD123189


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>
```

```
  ------------

    V = HMAC(K, V) is
                          129FF6D3 1A23FFBC 870632B3 5EE477C2
        280DDD2E CDABEDB9 00C78418 BE2D243B B9D8E509 3ECE7B6B
        F48638D8 F704D134 ADDEB7F4 E9D5C142 CD05683E 72B51648


    temp is
                          129FF6D3 1A23FFBC 870632B3 5EE477C2
        280DDD2E CDABEDB9 00C78418 BE2D243B B9D8E509 3ECE7B6B
        F48638D8 F704D134 ADDEB7F4 E9D5C142 CD05683E 72B51648


  ------------

    V = HMAC(K, V) is
                          6AF24AEC 15D61E81 E270DD4E BED91B62
        12EB8896 A6250D5C 8BC3A4A1 2F7E3068 FBDF856F 47EB23D3
        79F82C1E BCD1585F B260B9C0 C42625FB CEE68CAD 773CD5B1


    temp is
                                              129FF6D3 1A23FFBC
        870632B3 5EE477C2 280DDD2E CDABEDB9 00C78418 BE2D243B
        B9D8E509 3ECE7B6B F48638D8 F704D134 ADDEB7F4 E9D5C142
        CD05683E 72B51648 6AF24AEC 15D61E81 E270DD4E BED91B62
        12EB8896 A6250D5C 8BC3A4A1 2F7E3068 FBDF856F 47EB23D3
        79F82C1E BCD1585F B260B9C0 C42625FB CEE68CAD 773CD5B1


---------------------------

  returned_bits is
                                              129FF6D3 1A23FFBC
        870632B3 5EE477C2 280DDD2E CDABEDB9 00C78418 BE2D243B
        B9D8E509 3ECE7B6B F48638D8 F704D134 ADDEB7F4 E9D5C142
        CD05683E 72B51648 6AF24AEC 15D61E81 E270DD4E BED91B62
        12EB8896 A6250D5C 8BC3A4A1 2F7E3068 FBDF856F 47EB23D3
        79F82C1E BCD1585F B260B9C0 C42625FB CEE68CAD 773CD5B1


  call Update(additional_input, K, V)
---------------------------
```

```
  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                        6A F24AEC15 D61E81E2 70DD4EBE D91B6212
        EB8896A6 250D5C8B C3A4A12F 7E3068FB DF856F47 EB23D379
        F82C1EBC D1585FB2 60B9C0C4 2625FBCE E68CAD77 3CD5B100


    K = HMAC(K, V || 0x00 || provided_data) is
                           8AB868CE E3786F24 9731B824 583C54BE
        FBA2FC02 D3783FEB 2026E6AF 9583FF3D 4475EF98 FEEB3D7F
        8E22218B EFFD3A0D 11D81E86 4F902A39 27B0A677 B166EAA7


    V = HMAC(K, V) is
                           C4511D5E 80B125CF AF306267 21A25E01
        000E1711 077EBFE3 4EA6E58C 5F00775E 83DC13DD E2D86849
        4F3D6858 04C61BEC 70974A29 911E7C31 ACC5AA43 5AACFC0F


rnd_val is
                                              129FF6D3 1A23FFBC
        870632B3 5EE477C2 280DDD2E CDABEDB9 00C78418 BE2D243B
        B9D8E509 3ECE7B6B F48638D8 F704D134 ADDEB7F4 E9D5C142
        CD05683E 72B51648 6AF24AEC 15D61E81 E270DD4E BED91B62
        12EB8896 A6250D5C 8BC3A4A1 2F7E3068 FBDF856F 47EB23D3
        79F82C1E BCD1585F B260B9C0 C42625FB CEE68CAD 773CD5B1


##############################################################

HMAC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
```

```
    3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
    5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


EntropyInput1 (for Reseed1) =
                         808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


EntropyInput2 (for Reseed2) =
                         C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Nonce =
                       20212223 24252627 28292A2B 2C2D2E2F


PersonalizationString =
                         404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


AdditionalInput1 =
                         606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


AdditionalInput2 =
                         A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E
```

```
################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                           20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
                             404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  Key is
                           00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
```

```
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                         01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


--------------------------

  Update

    provided_data
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    ------------

    V || 0x00 || provided_data is
                           010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01000001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    K = HMAC(K, V || 0x00 || provided_data) is
                           8FE3241B 7CEC3C91 831FEBC5 664A324E
```

```
        CE7885EC 0CFB79F0 A110CDDA 5C25FBDF 2724481F E501C813
        656BAC39 9CE61ABA DA1D0D75 7B2AB666 F4C98216 C1482F59


    V = HMAC(K, V) is
                           496DABED 7FE15C71 16E221B4 30EE825C
        72A53FC3 49091FBF 5060584F CF9BAA56 70592E2F BB7E0E5A
        AD170616 E98B6DC8 BC4D77A2 EA17DFDE 4E64B0DF 260D9DCB


    ------------

    V || 0x01 || provided_data is
                             496DAB ED7FE15C 7116E221 B430EE82
        5C72A53F C349091F BF506058 4FCF9BAA 5670592E 2FBB7E0E
        5AAD1706 16E98B6D C8BC4D77 A2EA17DF DE4E64B0 DF260D9D
        CB010001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    K = HMAC(K, V || 0x01 || provided_data) is
                           96477F38 6DC67E91 FBE26228 31E00384
        E017C17F 654AD9B7 1B2395A1 870D0BC2 48378809 87061D81
        EE39A9B2 EC5E9F65 98193BB8 43F3EFA8 D82C0CA7 F5543BF1


    V = HMAC(K, V) is
                           FAE68E0C ED06928D 3D6EC078 2D3FF3ED
        D3E6D364 B11EF22B 715D26C4 4850F01D 7074E6C8 13109CD4
        8BD91FC8 678E972C 205511E4 3622F079 72ADB6BC 61BE4F7E


Update (Key, V):

    Key is
                           96477F38 6DC67E91 FBE26228 31E00384
        E017C17F 654AD9B7 1B2395A1 870D0BC2 48378809 87061D81
        EE39A9B2 EC5E9F65 98193BB8 43F3EFA8 D82C0CA7 F5543BF1
```

```
    V is
                          FAE68E0C ED06928D 3D6EC078 2D3FF3ED
        D3E6D364 B11EF22B 715D26C4 4850F01D 7074E6C8 13109CD4
        8BD91FC8 678E972C 205511E4 3622F079 72ADB6BC 61BE4F7E


---------------------------------------------------------------

First call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Generate FAILED: Reseed is required
***************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    additional_input is
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

Seed_Material is

```
                                                  8081 82838485
      86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
      9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
      B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
      CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
      E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
      6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
      8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
      9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
      B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

Key is

```
                       96477F38 6DC67E91 FBE26228 31E00384
      E017C17F 654AD9B7 1B2395A1 870D0BC2 48378809 87061D81
      EE39A9B2 EC5E9F65 98193BB8 43F3EFA8 D82C0CA7 F5543BF1
```

V is

```
                       FAE68E0C ED06928D 3D6EC078 2D3FF3ED
      D3E6D364 B11EF22B 715D26C4 4850F01D 7074E6C8 13109CD4
      8BD91FC8 678E972C 205511E4 3622F079 72ADB6BC 61BE4F7E
```

Update

provided_data

```
                                                  8081 82838485
      86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
      9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
      B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
      CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
      E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
      6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
      8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
      9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
      B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

V || 0x00 || provided_data is

```
      FAE68E 0CED0692 8D3D6EC0 782D3FF3 EDD3E6D3 64B11EF2
    2B715D26 C44850F0 1D7074E6 C813109C D48BD91F C8678E97
    2C205511 E43622F0 7972ADB6 BC61BE4F 7E008081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x00 || provided_data) is
                       1722866C 917C3B67 E5F99D7E A91045F8
    4193D957 7907CCD3 5550E52D A06D6754 0358C63B E94919BB
    C34BB792 E482A71C CECA46F3 163812E6 A66630AB 296B4C8E


V = HMAC(K, V) is
                       278B759C 8E0DA59A 0940CA85 E15715D2
    892F99C3 67D75B8C 2F990D01 1A51EB4D 18CA88EF 87CD6056
    3A92BD0C 4B43645D B79184FE FD492017 A0F57B77 7E71D53F


------------

V || 0x01 || provided_data is
      278B75 9C8E0DA5 9A0940CA 85E15715 D2892F99 C367D75B
    8C2F990D 011A51EB 4D18CA88 EF87CD60 563A92BD 0C4B4364
    5DB79184 FEFD4920 17A0F57B 777E71D5 3F018081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x01 || provided_data) is
                       220DC427 79664520 EA800878 E8337D04
    C138AE48 59D68A72 11F03A22 E9602D6E 2277FCFF 6EE81581
```

```
        FDD7A710 ABC57629 369D42A0 47713DCE 221B2267 2C911CB4


    V = HMAC(K, V) is
                         FFC9E91F D3F965DD 153465B5 F91FBD55
        40F08248 882C7100 3BC48BEC D4E1EB5F 4F14428D 4237F160
        58329A64 4E80418C F6B5800D 9AD66B93 C9BC8725 A6A16053


  Update (Key, V):

    Key is
                         220DC427 79664520 EA800878 E8337D04
        C138AE48 59D68A72 11F03A22 E9602D6E 2277FCFF 6EE81581
        FDD7A710 ABC57629 369D42A0 47713DCE 221B2267 2C911CB4


    V is
                         FFC9E91F D3F965DD 153465B5 F91FBD55
        40F08248 882C7100 3BC48BEC D4E1EB5F 4F14428D 4237F160
        58329A64 4E80418C F6B5800D 9AD66B93 C9BC8725 A6A16053


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                         B8E82765 2175E6E0 6E513C7B E94B5810
        C14ED94A D9036479 40CAEB7E E014C848 8DCBBE6D 4D6616D0
        6656A3DC 707CDAC4 F02EE6D8 408C065F CB068C07 60DA47C5


    temp is
                         B8E82765 2175E6E0 6E513C7B E94B5810
        C14ED94A D9036479 40CAEB7E E014C848 8DCBBE6D 4D6616D0
        6656A3DC 707CDAC4 F02EE6D8 408C065F CB068C07 60DA47C5


  ------------
```

```
    V = HMAC(K, V) is
                           D60E5D70 D09DC392 9B697961 5D117F7B
        EDCC661A 98514B3A 1F55B2CB ABDCA59F 11823E48 38065F1F
        8431CBF2 8A577738 234AF3F1 88C7190C C19739E7 2E9BBFFF


    temp is
                                               B8E82765 2175E6E0
        6E513C7B E94B5810 C14ED94A D9036479 40CAEB7E E014C848
        8DCBBE6D 4D6616D0 6656A3DC 707CDAC4 F02EE6D8 408C065F
        CB068C07 60DA47C5 D60E5D70 D09DC392 9B697961 5D117F7B
        EDCC661A 98514B3A 1F55B2CB ABDCA59F 11823E48 38065F1F
        8431CBF2 8A577738 234AF3F1 88C7190C C19739E7 2E9BBFFF


----------------------------

  returned_bits is
                                               B8E82765 2175E6E0
        6E513C7B E94B5810 C14ED94A D9036479 40CAEB7E E014C848
        8DCBBE6D 4D6616D0 6656A3DC 707CDAC4 F02EE6D8 408C065F
        CB068C07 60DA47C5 D60E5D70 D09DC392 9B697961 5D117F7B
        EDCC661A 98514B3A 1F55B2CB ABDCA59F 11823E48 38065F1F
        8431CBF2 8A577738 234AF3F1 88C7190C C19739E7 2E9BBFFF


  call Update(additional_input, K, V)
----------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                         D6 0E5D70D0 9DC3929B 6979615D 117F7BED
        CC661A98 514B3A1F 55B2CBAB DCA59F11 823E4838 065F1F84
        31CBF28A 57773823 4AF3F188 C7190CC1 9739E72E 9BBFFF00


    K = HMAC(K, V || 0x00 || provided_data) is
                           C0102CD0 756E55D2 FD8EA8B6 5C85B802
        C71BB175 DB898D58 B3180B1A F9DAC854 62DF83D8 127F751E
        7DBBD9C0 A1258636 B03A0886 726D9B36 B1E96414 10C3669E
```

```
    V = HMAC(K, V) is
                          44118780 B54B2EDB 5FA8B8B4 6A5BBF51
        1683D0A8 EDEF1FD0 4AA87BAB 28B3E07E FDAA0CC8 646A8830
        82500A00 33097142 75C0C8DB 1DDAF207 DA4F355B B1108AEE


rnd_val is
                                                B8E82765 2175E6E0
        6E513C7B E94B5810 C14ED94A D9036479 40CAEB7E E014C848
        8DCBBE6D 4D6616D0 6656A3DC 707CDAC4 F02EE6D8 408C065F
        CB068C07 60DA47C5 D60E5D70 D09DC392 9B697961 5D117F7B
        EDCC661A 98514B3A 1F55B2CB ABDCA59F 11823E48 38065F1F
        8431CBF2 8A577738 234AF3F1 88C7190C C19739E7 2E9BBFFF


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is
                             A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Generate FAILED: Reseed is required
***************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                             C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E
```

```
  additional_input is
                          A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  Seed_Material is
                                                 C0C1 C2C3C4C5
      C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
      DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
      F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
      0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
      26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  Key is
                         C0102CD0 756E55D2 FD8EA8B6 5C85B802
      C71BB175 DB898D58 B3180B1A F9DAC854 62DF83D8 127F751E
      7DBBD9C0 A1258636 B03A0886 726D9B36 B1E96414 10C3669E


  V is
                         44118780 B54B2EDB 5FA8B8B4 6A5BBF51
      1683D0A8 EDEF1FD0 4AA87BAB 28B3E07E FDAA0CC8 646A8830
      82500A00 33097142 75C0C8DB 1DDAF207 DA4F355B B1108AEE


---------------------------

  Update

    provided_data
                                                 C0C1 C2C3C4C5
      C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
      DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
      F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
      0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
      26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
```

```
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


------------

V || 0x00 || provided_data is
      441187 80B54B2E DB5FA8B8 B46A5BBF 511683D0 A8EDEF1F
    D04AA87B AB28B3E0 7EFDAA0C C8646A88 3082500A 00330971
    4275C0C8 DB1DDAF2 07DA4F35 5BB1108A EE00C0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


K = HMAC(K, V || 0x00 || provided_data) is
                        5E30CFA7 88DB0C81 95DE4152 3E9E19B8
    EE9BE2FB 43C318C3 09E2E68E 5157EBA5 878E1A78 A8C54423
    0062F627 34689232 ED28FC94 703294F1 BAA42834 BF7600A6


V = HMAC(K, V) is
                        60C3B3D9 63C283E4 673A221D 75F5B03F
    AD549A93 B89A86BD AD4A6326 B004CFB0 25890A60 F4037155
    689B3B51 E0DDCCBC E7FA6605 5200D88B 58F61C44 604C21B1


------------

V || 0x01 || provided_data is
      60C3B3 D963C283 E4673A22 1D75F5B0 3FAD549A 93B89A86
    BDAD4A63 26B004CF B025890A 60F40371 55689B3B 51E0DDCC
    BCE7FA66 055200D8 8B58F61C 44604C21 B101C0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
```

```
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    K = HMAC(K, V || 0x01 || provided_data) is
                            0DF49D5D E3A4A75F 3A4FD7E9 7338C252
        8DC83097 EE71926B 3DE86274 DA87D828 9A68F570 4D1D018E
        61D15233 D2A17C62 5A063A4A 0FF62A1E 192AFA8A BC6BA6FE


    V = HMAC(K, V) is
                            AB725F55 F27890A4 8194D008 FFC961F5
        14AF792D F52A1B9D CF840FC7 FB528058 9537CC05 6797523F
        70670C9D F0AA161B B735C3D0 3ECF4A52 60FB9775 AA1D69BA


  Update (Key, V):

    Key is
                            0DF49D5D E3A4A75F 3A4FD7E9 7338C252
        8DC83097 EE71926B 3DE86274 DA87D828 9A68F570 4D1D018E
        61D15233 D2A17C62 5A063A4A 0FF62A1E 192AFA8A BC6BA6FE


    V is
                            AB725F55 F27890A4 8194D008 FFC961F5
        14AF792D F52A1B9D CF840FC7 FB528058 9537CC05 6797523F
        70670C9D F0AA161B B735C3D0 3ECF4A52 60FB9775 AA1D69BA


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                            7ED41B9C FDC8C256 83BBB4C5 53CC2DC6
        1F690E62 ABC9F038 A16B8C51 9690CABE BD1B5C19 6C57CF75
        9BB9871B E0C163A5 7315EA96 F615136D 064572F0 9F26D659
```

```
    temp is
                          7ED41B9C FDC8C256 83BBB4C5 53CC2DC6
        1F690E62 ABC9F038 A16B8C51 9690CABE BD1B5C19 6C57CF75
        9BB9871B E0C163A5 7315EA96 F615136D 064572F0 9F26D659


  ------------

    V = HMAC(K, V) is
                          D24211F9 610FFCDF FDA8CE23 FFA96735
        75951826 60877766 035EED80 0B05364C E324A75E B63FD9B3
        EED956D1 47480B1D 0A42DF8A A990BB62 8666F6F6 1D60CBE2


    temp is
                                                 7ED41B9C FDC8C256
        83BBB4C5 53CC2DC6 1F690E62 ABC9F038 A16B8C51 9690CABE
        BD1B5C19 6C57CF75 9BB9871B E0C163A5 7315EA96 F615136D
        064572F0 9F26D659 D24211F9 610FFCDF FDA8CE23 FFA96735
        75951826 60877766 035EED80 0B05364C E324A75E B63FD9B3
        EED956D1 47480B1D 0A42DF8A A990BB62 8666F6F6 1D60CBE2


---------------------------

  returned_bits is
                                                 7ED41B9C FDC8C256
        83BBB4C5 53CC2DC6 1F690E62 ABC9F038 A16B8C51 9690CABE
        BD1B5C19 6C57CF75 9BB9871B E0C163A5 7315EA96 F615136D
        064572F0 9F26D659 D24211F9 610FFCDF FDA8CE23 FFA96735
        75951826 60877766 035EED80 0B05364C E324A75E B63FD9B3
        EED956D1 47480B1D 0A42DF8A A990BB62 8666F6F6 1D60CBE2


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
```

```
                    D2 4211F961 0FFCDFFD A8CE23FF A9673575
        95182660 87776603 5EED800B 05364CE3 24A75EB6 3FD9B3EE
        D956D147 480B1D0A 42DF8AA9 90BB6286 66F6F61D 60CBE200


    K = HMAC(K, V || 0x00 || provided_data) is
                        0F5F718A 5EA08533 1A00665B 781DD9CC
        0A57758A 99FD23D9 3DA2728E 714E13B7 9FB414AF AED8385D
        A5AEDF23 5B67A398 E68D15C9 76FE1083 8A672844 C1CF01FF


    V = HMAC(K, V) is
                        6DF16C1A 6B6ADD93 725F4D0E F83559CE
        0CB0EFE2 20298503 160A3AC1 16F6FCF6 79B5FF05 B6331D81
        F48796CC 5B937577 360A64F1 404DE16F D02913C6 AB7AEC44


rnd_val is
                                            7ED41B9C FDC8C256
        83BBB4C5 53CC2DC6 1F690E62 ABC9F038 A16B8C51 9690CABE
        BD1B5C19 6C57CF75 9BB9871B E0C163A5 7315EA96 F615136D
        064572F0 9F26D659 D24211F9 610FFCDF FDA8CE23 FFA96735
        75951826 60877766 035EED80 0B05364C E324A75E B63FD9B3
        EED956D1 47480B1D 0A42DF8A A990BB62 8666F6F6 1D60CBE2
```

```
###############################################################

CTR_DRBG

    Requested Security Strength = 112

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    EntropyInput1 (for Reseed1) =
                                                        80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Update

    provided_data is
```

                                                    00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000

      V is
                                                00000000 00000001

Block #1
Blockin   00000000 00000001
Blockout 166B40B4 4ABA4BD6

      output_block is
                                                166B40B4 4ABA4BD6

      temp is
                                                166B40B4 4ABA4BD6

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000

      V is
                                                00000000 00000002

Block #1
Blockin   00000000 00000002
Blockout 06E7EA22 CE92708F

      output_block is
                                                06E7EA22 CE92708F

```
      temp is
                           166B40B4 4ABA4BD6 06E7EA22 CE92708F


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                              4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000004


Block #1
Blockin   00000000 00000004
Blockout  D2FD8867 D50D2DFE
```

```
      output_block is
                                                D2FD8867 D50D2DFE


      temp is
                                                166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                    16 6A42B74E
        BF4DD10E EEE029C2 9F7E805E A082DAB6 EF008BCA E4927CC9


    Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


    V is
                                                EF008BCA E4927CC9


---------------------------------------------------------------

First call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   EF008BCA E4927CCA
Blockout  077AF02D 5209B1A5

Block #1
Blockin   EF008BCA E4927CCB
Blockout  9086A90A F689863D

---------------------------

  Update
```

```
    provided_data is
                                                          00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                              EF008BCA E4927CCC


Block #1
Blockin   EF008BCA E4927CCC
Blockout  EAB6F0C7 2B1C15A6

      output_block is
                                              EAB6F0C7 2B1C15A6


      temp is
                                              EAB6F0C7 2B1C15A6


    ------------

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                              EF008BCA E4927CCD


Block #1
Blockin   EF008BCA E4927CCD
Blockout  EE7244FC AB83AF9D

      output_block is
```

```
                                          EE7244FC AB83AF9D


      temp is
                          EAB6F0C7 2B1C15A6 EE7244FC AB83AF9D


    ------------

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                          EF008BCA E4927CCE


Block #1
Blockin   EF008BCA E4927CCE
Blockout  17590CC9 C26E5A9F

      output_block is
                                          17590CC9 C26E5A9F


      temp is
        EAB6F0C7 2B1C15A6 EE7244FC AB83AF9D 17590CC9 C26E5A9F


    ------------

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                          EF008BCA E4927CCF


Block #1
Blockin   EF008BCA E4927CCF
Blockout  4D86DE41 4EC7B6C5
```

```
      output_block is
                                              4D86DE41 4EC7B6C5


      temp is
                                              EAB6F0C7 2B1C15A6
        EE7244FC AB83AF9D 17590CC9 C26E5A9F 4D86DE41 4EC7B6C5


    temp XOR provided_data is
                                                    EA B6F0C72B
        1C15A6EE 7244FCAB 83AF9D17 590CC9C2 6E5A9F4D 86DE414E


    Key is
              EA B6F0C72B 1C15A6EE 7244FCAB 83AF9D17 590CC9C2


    V is
                                              6E5A9F4D 86DE414E


rnd_val is
                          077AF02D 5209B1A5 9086A90A F689863D


------------------------------------------------------------

Second call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   6E5A9F4D 86DE414F
Blockout  C78CC305 D0D238C9

Block #1
Blockin   6E5A9F4D 86DE4150
Blockout  AA647225 6FFFD0F9
```

```
---------------------------

  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              EA B6F0C72B 1C15A6EE 7244FCAB 83AF9D17 590CC9C2


      V is
                                            6E5A9F4D 86DE4151


Block #1
Blockin   6E5A9F4D 86DE4151
Blockout  CE5FE609 AF2D3242

      output_block is
                                            CE5FE609 AF2D3242


      temp is
                                            CE5FE609 AF2D3242


    ------------

      While loop

      Key is
              EA B6F0C72B 1C15A6EE 7244FCAB 83AF9D17 590CC9C2


      V is
                                            6E5A9F4D 86DE4152
```

```
Block #1
Blockin   6E5A9F4D 86DE4152
Blockout  7442F203 B9DDC978

      output_block is
                                            7442F203 B9DDC978


      temp is
                          CE5FE609 AF2D3242 7442F203 B9DDC978


    ------------

      While loop

      Key is
              EA B6F0C72B 1C15A6EE 7244FCAB 83AF9D17 590CC9C2


      V is
                                            6E5A9F4D 86DE4153


Block #1
Blockin   6E5A9F4D 86DE4153
Blockout  9B716E25 1D1AB17F

      output_block is
                                            9B716E25 1D1AB17F


      temp is
        CE5FE609 AF2D3242 7442F203 B9DDC978 9B716E25 1D1AB17F


    ------------

      While loop

      Key is
              EA B6F0C72B 1C15A6EE 7244FCAB 83AF9D17 590CC9C2


      V is
                                            6E5A9F4D 86DE4154
```

```
Block #1
Blockin   6E5A9F4D 86DE4154
Blockout  BF160986 91AD7250

      output_block is
                                              BF160986 91AD7250


      temp is
                                              CE5FE609 AF2D3242
        7442F203 B9DDC978 9B716E25 1D1AB17F BF160986 91AD7250


    temp XOR provided_data is
                                                    CE 5FE609AF
        2D324274 42F203B9 DDC9789B 716E251D 1AB17FBF 16098691


    Key is
              CE 5FE609AF 2D324274 42F203B9 DDC9789B 716E251D


    V is
                                              1AB17FBF 16098691


rnd_val is
                          C78CC305 D0D238C9 AA647225 6FFFD0F9


################################################################

CTR_DRBG

    Requested Security Strength = 112

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                    00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    EntropyInput1 (for Reseed1) =
                                                    80 81828384
```

```
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                        60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


    AdditionalInput2 =
                                                        A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Update

    provided_data is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    ------------
```

```
      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000001


Block #1
Blockin   00000000 00000001
Blockout  166B40B4 4ABA4BD6

      output_block is
                                              166B40B4 4ABA4BD6


      temp is
                                              166B40B4 4ABA4BD6


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000002


Block #1
Blockin   00000000 00000002
Blockout  06E7EA22 CE92708F

      output_block is
                                              06E7EA22 CE92708F


      temp is
                          166B40B4 4ABA4BD6 06E7EA22 CE92708F
```

```
    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                             00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                             4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                             00000000 00000004


Block #1
Blockin   00000000 00000004
Blockout  D2FD8867 D50D2DFE

      output_block is
                                             D2FD8867 D50D2DFE


      temp is
                                             166B40B4 4ABA4BD6
```

```
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                    16 6A42B74E
        BF4DD10E EEE029C2 9F7E805E A082DAB6 EF008BCA E4927CC9


    Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


    V is
                                               EF008BCA E4927CC9


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                    60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
                                                    60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


    ------------

      While loop

      Key is
```

```
               16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                              EF008BCA E4927CCA


Block #1
Blockin   EF008BCA E4927CCA
Blockout  077AF02D 5209B1A5

      output_block is
                                              077AF02D 5209B1A5


      temp is
                                              077AF02D 5209B1A5


    ------------

      While loop

      Key is
               16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                              EF008BCA E4927CCB


Block #1
Blockin   EF008BCA E4927CCB
Blockout  9086A90A F689863D

      output_block is
                                              9086A90A F689863D


      temp is
                           077AF02D 5209B1A5 9086A90A F689863D


    ------------

      While loop
```

```
      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                              EF008BCA E4927CCC


Block #1
Blockin   EF008BCA E4927CCC
Blockout  EAB6F0C7 2B1C15A6

      output_block is
                                              EAB6F0C7 2B1C15A6


      temp is
        077AF02D 5209B1A5 9086A90A F689863D EAB6F0C7 2B1C15A6


    ------------

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                              EF008BCA E4927CCD


Block #1
Blockin   EF008BCA E4927CCD
Blockout  EE7244FC AB83AF9D

      output_block is
                                              EE7244FC AB83AF9D


      temp is
                                              077AF02D 5209B1A5
        9086A90A F689863D EAB6F0C7 2B1C15A6 EE7244FC AB83AF9D
```

```
    temp XOR provided_data is
                                                        67 1B924E36
        6CD7C2F8 EFC3619A E4E8529A C782B45F 6963D196 0B3E87D7


    Key is
              67 1B924E36 6CD7C2F8 EFC3619A E4E8529A C782B45F


    V is
                                            6963D196 0B3E87D7


Block #1
Blockin   6963D196 0B3E87D8
Blockout  D3A44CA8 439CAC8D

Block #1
Blockin   6963D196 0B3E87D9
Blockout  9C7F4B1D B7977D4B

---------------------------

  Update

    provided_data is
                                                        60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


    ------------

      While loop

      Key is
              67 1B924E36 6CD7C2F8 EFC3619A E4E8529A C782B45F


      V is
                                            6963D196 0B3E87DA


Block #1
Blockin   6963D196 0B3E87DA
Blockout  B3A95F1C 6EC4A19F
```

```
      output_block is
                                              B3A95F1C 6EC4A19F

      temp is
                                              B3A95F1C 6EC4A19F

    ------------

      While loop

      Key is
              67 1B924E36 6CD7C2F8 EFC3619A E4E8529A C782B45F

      V is
                                              6963D196 0B3E87DB

Block #1
Blockin   6963D196 0B3E87DB
Blockout  59A27ECD AD663B97

      output_block is
                                              59A27ECD AD663B97

      temp is
                           B3A95F1C 6EC4A19F 59A27ECD AD663B97

    ------------

      While loop

      Key is
              67 1B924E36 6CD7C2F8 EFC3619A E4E8529A C782B45F

      V is
                                              6963D196 0B3E87DC

Block #1
Blockin   6963D196 0B3E87DC
```

```
Blockout  685B44F5 AD20D28D

      output_block is
                                              685B44F5 AD20D28D


      temp is
        B3A95F1C 6EC4A19F 59A27ECD AD663B97 685B44F5 AD20D28D


    ------------

      While loop

      Key is
              67 1B924E36 6CD7C2F8 EFC3619A E4E8529A C782B45F


      V is
                                              6963D196 0B3E87DD


Block #1
Blockin   6963D196 0B3E87DD
Blockout  7E4FCAB4 F9C8AA63

      output_block is
                                              7E4FCAB4 F9C8AA63


      temp is
                                              B3A95F1C 6EC4A19F
        59A27ECD AD663B97 685B44F5 AD20D28D 7E4FCAB4 F9C8AA63


    temp XOR provided_data is
                                                    D3 C83D7F0A
        A1C7F831 CB14A6C1 0B55F818 2A3686D9 55A4FA06 36B0CF85


    Key is
              D3 C83D7F0A A1C7F831 CB14A6C1 0B55F818 2A3686D9


    V is
                                              55A4FA06 36B0CF85
```

```
rnd_val is
                          D3A44CA8 439CAC8D 9C7F4B1D B7977D4B


------------------------------------------------------------

Second call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                    A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
                                                    A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


    ------------

      While loop

      Key is
              D3 C83D7F0A A1C7F831 CB14A6C1 0B55F818 2A3686D9


      V is
                                           55A4FA06 36B0CF86


Block #1
Blockin   55A4FA06 36B0CF86
Blockout  5B50FA3E 59CE4714
```

```
      output_block is
                                              5B50FA3E 59CE4714

      temp is
                                              5B50FA3E 59CE4714

    ------------

      While loop

      Key is
              D3 C83D7F0A A1C7F831 CB14A6C1 0B55F818 2A3686D9

      V is
                                              55A4FA06 36B0CF87

Block #1
Blockin   55A4FA06 36B0CF87
Blockout  2CE9013E B8892D71

      output_block is
                                              2CE9013E B8892D71

      temp is
                           5B50FA3E 59CE4714 2CE9013E B8892D71

    ------------

      While loop

      Key is
              D3 C83D7F0A A1C7F831 CB14A6C1 0B55F818 2A3686D9

      V is
                                              55A4FA06 36B0CF88

Block #1
```

```
Blockin   55A4FA06 36B0CF88
Blockout  B756CBA9 99789C53

      output_block is
                                              B756CBA9 99789C53


      temp is
        5B50FA3E 59CE4714 2CE9013E B8892D71 B756CBA9 99789C53


    ------------

      While loop

      Key is
              D3 C83D7F0A A1C7F831 CB14A6C1 0B55F818 2A3686D9


      V is
                                              55A4FA06 36B0CF89


Block #1
Blockin   55A4FA06 36B0CF89
Blockout  BD263872 5913FAC6

      output_block is
                                              BD263872 5913FAC6


      temp is
                                              5B50FA3E 59CE4714
        2CE9013E B8892D71 B756CBA9 99789C53 BD263872 5913FAC6


    temp XOR provided_data is
                                                    FB F1589DFD
        6BE1B384 40AB9514 2483DE07 E7791A2D CD2AE405 9F82C9E5


    Key is
              FB F1589DFD 6BE1B384 40AB9514 2483DE07 E7791A2D


    V is
```

```
                                                CD2AE405 9F82C9E5


Block #1
Blockin   CD2AE405 9F82C9E6
Blockout  E2810D58 E9457F8E

Block #1
Blockin   CD2AE405 9F82C9E7
Blockout  A0CA4C31 C4F5FB9B

---------------------------

  Update

    provided_data is
                                                          A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


    ------------

      While loop

      Key is
              FB F1589DFD 6BE1B384 40AB9514 2483DE07 E7791A2D


      V is
                                                CD2AE405 9F82C9E8


Block #1
Blockin   CD2AE405 9F82C9E8
Blockout  E48D768A DC9C8A48

      output_block is
                                                E48D768A DC9C8A48


      temp is
                                                E48D768A DC9C8A48


    ------------
```

```
      While loop

      Key is
              FB F1589DFD 6BE1B384 40AB9514 2483DE07 E7791A2D


      V is
                                           CD2AE405 9F82C9E9


Block #1
Blockin   CD2AE405 9F82C9E9
Blockout  EAC5967B B723FAE2

      output_block is
                                           EAC5967B B723FAE2


      temp is
                          E48D768A DC9C8A48 EAC5967B B723FAE2


    ------------

      While loop

      Key is
              FB F1589DFD 6BE1B384 40AB9514 2483DE07 E7791A2D


      V is
                                           CD2AE405 9F82C9EA


Block #1
Blockin   CD2AE405 9F82C9EA
Blockout  E53CC977 3188535E

      output_block is
                                           E53CC977 3188535E


      temp is
        E48D768A DC9C8A48 EAC5967B B723FAE2 E53CC977 3188535E
```

```
    ------------

      While loop

      Key is
              FB F1589DFD 6BE1B384 40AB9514 2483DE07 E7791A2D


      V is
                                            CD2AE405 9F82C9EB


Block #1
Blockin   CD2AE405 9F82C9EB
Blockout  C25E1469 F39D4938

      output_block is
                                            C25E1469 F39D4938


      temp is
                                            E48D768A DC9C8A48
        EAC5967B B723FAE2 E53CC977 3188535E C25E1469 F39D4938


    temp XOR provided_data is
                                                  44 2CD42978
        392CEF42 6C3CD01B 8E544D55 8D7BC485 3DE5E97A E7AED24F


    Key is
              44 2CD42978 392CEF42 6C3CD01B 8E544D55 8D7BC485


    V is
                                            3DE5E97A E7AED24F


rnd_val is
                          E2810D58 E9457F8E A0CA4C31 C4F5FB9B


################################################################

CTR_DRBG
```

```
    Requested Security Strength = 112

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    EntropyInput1 (for Reseed1) =
                                                        80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    PersonalizationString =
                                                        40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    AdditionalInput = <empty>

################################################################

****************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    personal_str is
                                                        40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Update
```

```
    provided_data is
                                                        40 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000001


Block #1
Blockin   00000000 00000001
Blockout  166B40B4 4ABA4BD6

      output_block is
                                              166B40B4 4ABA4BD6


      temp is
                                              166B40B4 4ABA4BD6


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000002


Block #1
Blockin   00000000 00000002
Blockout  06E7EA22 CE92708F
```

```
      output_block is
                                              06E7EA22 CE92708F


      temp is
                           166B40B4 4ABA4BD6 06E7EA22 CE92708F


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                              4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000004


Block #1
Blockin   00000000 00000004
```

```
Blockout  D2FD8867 D50D2DFE

      output_block is
                                              D2FD8867 D50D2DFE


      temp is
                                              166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                    56 2B00F40A
        FA0B9646 A7AA628E D230CF0E F1D089E2 BA56DC92 BDC82795


    Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


    V is
                                              BA56DC92 BDC82795


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   BA56DC92 BDC82796
Blockout  9E0082B6 B55E3596

Block #1
Blockin   BA56DC92 BDC82797
Blockout  F1A82251 90390124

---------------------------
```

```
  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                            BA56DC92 BDC82798


Block #1
Blockin   BA56DC92 BDC82798
Blockout  24C9B2C0 8D487353

      output_block is
                                            24C9B2C0 8D487353


      temp is
                                            24C9B2C0 8D487353


    ------------

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                            BA56DC92 BDC82799


Block #1
Blockin   BA56DC92 BDC82799
Blockout  32269D08 E3F6F53A
```

```
      output_block is
                                              32269D08 E3F6F53A


      temp is
                           24C9B2C0 8D487353 32269D08 E3F6F53A


    ------------

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                              BA56DC92 BDC8279A


Block #1
Blockin   BA56DC92 BDC8279A
Blockout  D10536CA 74513299

      output_block is
                                              D10536CA 74513299


      temp is
        24C9B2C0 8D487353 32269D08 E3F6F53A D10536CA 74513299


    ------------

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                              BA56DC92 BDC8279B


Block #1
```

```
Blockin   BA56DC92 BDC8279B
Blockout  632447C4 C43BCD57

      output_block is
                                              632447C4 C43BCD57


      temp is
                                              24C9B2C0 8D487353
        32269D08 E3F6F53A D10536CA 74513299 632447C4 C43BCD57


    temp XOR provided_data is
                                                    24 C9B2C08D
        48735332 269D08E3 F6F53AD1 0536CA74 51329963 2447C4C4


    Key is
              24 C9B2C08D 48735332 269D08E3 F6F53AD1 0536CA74


    V is
                                              51329963 2447C4C4


rnd_val is
                          9E0082B6 B55E3596 F1A82251 90390124


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   51329963 2447C4C5
Blockout  BA17E856 88D12FDB

Block #1
```

```
Blockin   51329963 2447C4C6
Blockout  B9296F01 C7F97982

---------------------------

  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              24 C9B2C08D 48735332 269D08E3 F6F53AD1 0536CA74


      V is
                                            51329963 2447C4C7


Block #1
Blockin   51329963 2447C4C7
Blockout  C526F53C CC8E279E

      output_block is
                                            C526F53C CC8E279E


      temp is
                                            C526F53C CC8E279E


    ------------

      While loop

      Key is
              24 C9B2C08D 48735332 269D08E3 F6F53AD1 0536CA74


      V is
                                            51329963 2447C4C8
```

```
Block #1
Blockin   51329963 2447C4C8
Blockout  9D51CA87 116B0930

      output_block is
                                              9D51CA87 116B0930


      temp is
                           C526F53C CC8E279E 9D51CA87 116B0930


    ------------

      While loop

      Key is
              24 C9B2C08D 48735332 269D08E3 F6F53AD1 0536CA74


      V is
                                              51329963 2447C4C9


Block #1
Blockin   51329963 2447C4C9
Blockout  1001A638 3943F879

      output_block is
                                              1001A638 3943F879


      temp is
        C526F53C CC8E279E 9D51CA87 116B0930 1001A638 3943F879


    ------------

      While loop

      Key is
              24 C9B2C08D 48735332 269D08E3 F6F53AD1 0536CA74
```

```
      V is
                                                51329963 2447C4CA


Block #1
Blockin   51329963 2447C4CA
Blockout  BCAC8FEB CDCF0E5C

      output_block is
                                                BCAC8FEB CDCF0E5C


      temp is
                                                C526F53C CC8E279E
        9D51CA87 116B0930 1001A638 3943F879 BCAC8FEB CDCF0E5C


    temp XOR provided_data is
                                                        C5 26F53CCC
        8E279E9D 51CA8711 6B093010 01A63839 43F879BC AC8FEBCD


    Key is
              C5 26F53CCC 8E279E9D 51CA8711 6B093010 01A63839


    V is
                                                43F879BC AC8FEBCD


rnd_val is
                          BA17E856 88D12FDB B9296F01 C7F97982


################################################################

CTR_DRBG

    Requested Security Strength = 112

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C
```

```
    EntropyInput1 (for Reseed1) =
                                                        80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    PersonalizationString =
                                                        40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    AdditionalInput1 =
                                                        60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


    AdditionalInput2 =
                                                        A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    personal_str is
                                                        40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Update
```

```
    provided_data is
                                                        40 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000001


Block #1
Blockin   00000000 00000001
Blockout  166B40B4 4ABA4BD6

      output_block is
                                              166B40B4 4ABA4BD6


      temp is
                                              166B40B4 4ABA4BD6


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000002


Block #1
Blockin   00000000 00000002
Blockout  06E7EA22 CE92708F
```

```
      output_block is
                                              06E7EA22 CE92708F


      temp is
                           166B40B4 4ABA4BD6 06E7EA22 CE92708F


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                              4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000004


Block #1
Blockin   00000000 00000004
```

```
Blockout  D2FD8867 D50D2DFE

      output_block is
                                                D2FD8867 D50D2DFE


      temp is
                                                166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                        56 2B00F40A
        FA0B9646 A7AA628E D230CF0E F1D089E2 BA56DC92 BDC82795


    Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


    V is
                                                BA56DC92 BDC82795


---------------------------------------------------------------

First call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                        60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
                                                        60 61626364
```

```
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


    ------------

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                            BA56DC92 BDC82796


Block #1
Blockin   BA56DC92 BDC82796
Blockout  9E0082B6 B55E3596

      output_block is
                                            9E0082B6 B55E3596


      temp is
                                            9E0082B6 B55E3596


    ------------

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                            BA56DC92 BDC82797


Block #1
Blockin   BA56DC92 BDC82797
Blockout  F1A82251 90390124

      output_block is
                                            F1A82251 90390124
```

```
      temp is
                          9E0082B6 B55E3596 F1A82251 90390124


    ------------

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                              BA56DC92 BDC82798


Block #1
Blockin   BA56DC92 BDC82798
Blockout  24C9B2C0 8D487353

      output_block is
                                              24C9B2C0 8D487353


      temp is
        9E0082B6 B55E3596 F1A82251 90390124 24C9B2C0 8D487353


    ------------

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                              BA56DC92 BDC82799


Block #1
Blockin   BA56DC92 BDC82799
Blockout  32269D08 E3F6F53A

      output_block is
```

```
                                                32269D08 E3F6F53A


      temp is
                                                9E0082B6 B55E3596
        F1A82251 90390124 24C9B2C0 8D487353 32269D08 E3F6F53A


    temp XOR provided_data is
                                                      FE 61E0D5D1
        3B53F199 C1483AFC 546F4B54 B8C0B3F9 3D05244A 5FE7739F


    Key is
              FE 61E0D5D1 3B53F199 C1483AFC 546F4B54 B8C0B3F9


    V is
                                                3D05244A 5FE7739F


Block #1
Blockin   3D05244A 5FE773A0
Blockout  5921C494 636A6CED

Block #1
Blockin   3D05244A 5FE773A1
Blockout  D3079514 F23B4A5B

---------------------------

  Update

    provided_data is
                                                      60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


    ------------

      While loop

      Key is
              FE 61E0D5D1 3B53F199 C1483AFC 546F4B54 B8C0B3F9
```

```
      V is
                                              3D05244A 5FE773A2


Block #1
Blockin   3D05244A 5FE773A2
Blockout  49F68905 3BC4B2CE

      output_block is
                                              49F68905 3BC4B2CE


      temp is
                                              49F68905 3BC4B2CE


    ------------

      While loop

      Key is
              FE 61E0D5D1 3B53F199 C1483AFC 546F4B54 B8C0B3F9


      V is
                                              3D05244A 5FE773A3


Block #1
Blockin   3D05244A 5FE773A3
Blockout  68B8303E 421FD382

      output_block is
                                              68B8303E 421FD382


      temp is
                           49F68905 3BC4B2CE 68B8303E 421FD382


    ------------

      While loop

      Key is
              FE 61E0D5D1 3B53F199 C1483AFC 546F4B54 B8C0B3F9
```

```
      V is
                                              3D05244A 5FE773A4


Block #1
Blockin   3D05244A 5FE773A4
Blockout  CD61931B F8341BBB

      output_block is
                                              CD61931B F8341BBB


      temp is
        49F68905 3BC4B2CE 68B8303E 421FD382 CD61931B F8341BBB


    ------------

      While loop

      Key is
              FE 61E0D5D1 3B53F199 C1483AFC 546F4B54 B8C0B3F9


      V is
                                              3D05244A 5FE773A5


Block #1
Blockin   3D05244A 5FE773A5
Blockout  F4341AF3 BC9D9757

      output_block is
                                              F4341AF3 BC9D9757


      temp is
                                              49F68905 3BC4B2CE
        68B8303E 421FD382 CD61931B F8341BBB F4341AF3 BC9D9757


    temp XOR provided_data is
                                                    29 97EB665F
        A1D4A900 D15A552E 72BDEDBD 10E1688C 416DCC8C 4D6088C0
```

```
    Key is
              29 97EB665F A1D4A900 D15A552E 72BDEDBD 10E1688C

    V is
                                           416DCC8C 4D6088C0

rnd_val is
                          5921C494 636A6CED D3079514 F23B4A5B

-------------------------------------------------------------

Second call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                    A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
                                                    A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


    ------------

      While loop

      Key is
              29 97EB665F A1D4A900 D15A552E 72BDEDBD 10E1688C
```

```
      V is
                                              416DCC8C 4D6088C1


Block #1
Blockin   416DCC8C 4D6088C1
Blockout  96BEB0B1 4A625631

      output_block is
                                              96BEB0B1 4A625631


      temp is
                                              96BEB0B1 4A625631


    ------------

      While loop

      Key is
              29 97EB665F A1D4A900 D15A552E 72BDEDBD 10E1688C


      V is
                                              416DCC8C 4D6088C2


Block #1
Blockin   416DCC8C 4D6088C2
Blockout  77B10223 8E2FAAB7

      output_block is
                                              77B10223 8E2FAAB7


      temp is
                           96BEB0B1 4A625631 77B10223 8E2FAAB7


    ------------

      While loop

      Key is
```

```
              29 97EB665F A1D4A900 D15A552E 72BDEDBD 10E1688C


      V is
                                              416DCC8C 4D6088C3


Block #1
Blockin   416DCC8C 4D6088C3
Blockout  4D4069A0 F468844C

      output_block is
                                              4D4069A0 F468844C


      temp is
        96BEB0B1 4A625631 77B10223 8E2FAAB7 4D4069A0 F468844C


    ------------

      While loop

      Key is
              29 97EB665F A1D4A900 D15A552E 72BDEDBD 10E1688C


      V is
                                              416DCC8C 4D6088C4


Block #1
Blockin   416DCC8C 4D6088C4
Blockout  6DC395B6 353CC34E

      output_block is
                                              6DC395B6 353CC34E


      temp is
                                              96BEB0B1 4A625631
        77B10223 8E2FAAB7 4D4069A0 F468844C 6DC395B6 353CC34E


    temp XOR provided_data is
                                                    36 1F1212EE
```

```
        C7F096DF 18A88822 820418FD F1DB1340 DD32FBD5 7A2F0D89


    Key is
              36 1F1212EE C7F096DF 18A88822 820418FD F1DB1340


    V is
                                              DD32FBD5 7A2F0D89


Block #1
Blockin   DD32FBD5 7A2F0D8A
Blockout  D29F87DD 6FB87281

Block #1
Blockin   DD32FBD5 7A2F0D8B
Blockout  458BADBF 4BDB0F7E

---------------------------

  Update

    provided_data is
                                                    A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


    ------------

      While loop

      Key is
              36 1F1212EE C7F096DF 18A88822 820418FD F1DB1340


      V is
                                              DD32FBD5 7A2F0D8C


Block #1
Blockin   DD32FBD5 7A2F0D8C
Blockout  44F1F033 77093092

      output_block is
                                              44F1F033 77093092
```

```
      temp is
                                              44F1F033 77093092


    ------------

      While loop

      Key is
              36 1F1212EE C7F096DF 18A88822 820418FD F1DB1340


      V is
                                              DD32FBD5 7A2F0D8D


Block #1
Blockin   DD32FBD5 7A2F0D8D
Blockout  284D9C6D 8FEC404D

      output_block is
                                              284D9C6D 8FEC404D


      temp is
                           44F1F033 77093092 284D9C6D 8FEC404D


    ------------

      While loop

      Key is
              36 1F1212EE C7F096DF 18A88822 820418FD F1DB1340


      V is
                                              DD32FBD5 7A2F0D8E


Block #1
Blockin   DD32FBD5 7A2F0D8E
Blockout  067FF694 A9067966
```

```
      output_block is
                                              067FF694 A9067966

      temp is
        44F1F033 77093092 284D9C6D 8FEC404D 067FF694 A9067966

    ------------

      While loop

      Key is
              36 1F1212EE C7F096DF 18A88822 820418FD F1DB1340

      V is
                                              DD32FBD5 7A2F0D8F


Block #1
Blockin   DD32FBD5 7A2F0D8F
Blockout  612A3FC4 914148F2

      output_block is
                                              612A3FC4 914148F2

      temp is
                                              44F1F033 77093092
        284D9C6D 8FEC404D 067FF694 A9067966 612A3FC4 914148F2

    temp XOR provided_data is
                                                    E4 505290D3
        AC963580 E436C623 41EEE2B6 CE44271D B3CFD1D9 93857F2D

    Key is
              E4 505290D3 AC963580 E436C623 41EEE2B6 CE44271D

    V is
                                              B3CFD1D9 93857F2D
```

```
rnd_val is
                          D29F87DD 6FB87281 458BADBF 4BDB0F7E


################################################################

CTR_DRBG

    Requested Security Strength = 112

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                      00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    EntropyInput1 (for Reseed1) =
                                                      80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                      C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                      00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

--------------------------
```

```
  Update

    provided_data is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000001


Block #1
Blockin   00000000 00000001
Blockout  166B40B4 4ABA4BD6

      output_block is
                                              166B40B4 4ABA4BD6


      temp is
                                              166B40B4 4ABA4BD6


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000002


Block #1
Blockin   00000000 00000002
```

```
Blockout  06E7EA22 CE92708F

      output_block is
                                              06E7EA22 CE92708F


      temp is
                           166B40B4 4ABA4BD6 06E7EA22 CE92708F


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                              4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000004
```

```
Block #1
Blockin   00000000 00000004
Blockout  D2FD8867 D50D2DFE

      output_block is
                                              D2FD8867 D50D2DFE


      temp is
                                              166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                    16 6A42B74E
        BF4DD10E EEE029C2 9F7E805E A082DAB6 EF008BCA E4927CC9


    Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


    V is
                                              EF008BCA E4927CC9


---------------------------------------------------------------

First call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Generate FAILED: Reseed is required
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                                    80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C
```

```
    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                                                        80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    ------------

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                            EF008BCA E4927CCA


Block #1
Blockin   EF008BCA E4927CCA
Blockout  077AF02D 5209B1A5

      output_block is
                                            077AF02D 5209B1A5


      temp is
                                            077AF02D 5209B1A5


    ------------

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
```

```
                                          EF008BCA E4927CCB


Block #1
Blockin   EF008BCA E4927CCB
Blockout  9086A90A F689863D

      output_block is
                                          9086A90A F689863D


      temp is
                          077AF02D 5209B1A5 9086A90A F689863D


    ------------

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                          EF008BCA E4927CCC


Block #1
Blockin   EF008BCA E4927CCC
Blockout  EAB6F0C7 2B1C15A6

      output_block is
                                          EAB6F0C7 2B1C15A6


      temp is
        077AF02D 5209B1A5 9086A90A F689863D EAB6F0C7 2B1C15A6


    ------------

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6
```

```
      V is
                                              EF008BCA E4927CCD


Block #1
Blockin   EF008BCA E4927CCD
Blockout  EE7244FC AB83AF9D

      output_block is
                                              EE7244FC AB83AF9D


      temp is
                                              077AF02D 5209B1A5
        9086A90A F689863D EAB6F0C7 2B1C15A6 EE7244FC AB83AF9D


    temp XOR provided_data is
                                                    87 FB72AED6
        8C372218 0F23817A 0408B27A 276254BF 89833176 EBDE6737


    Key is
              87 FB72AED6 8C372218 0F23817A 0408B27A 276254BF


    V is
                                              89833176 EBDE6737


*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   89833176 EBDE6738
Blockout  76FFEB64 F39FD9DC

Block #1
Blockin   89833176 EBDE6739
Blockout  F407C209 7083158B
```

```
---------------------------

  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              87 FB72AED6 8C372218 0F23817A 0408B27A 276254BF


      V is
                                            89833176 EBDE673A


Block #1
Blockin   89833176 EBDE673A
Blockout  3C51738A 731CB88E

      output_block is
                                            3C51738A 731CB88E


      temp is
                                            3C51738A 731CB88E


    ------------

      While loop

      Key is
              87 FB72AED6 8C372218 0F23817A 0408B27A 276254BF


      V is
                                            89833176 EBDE673B
```

```
Block #1
Blockin   89833176 EBDE673B
Blockout  C38C7074 F18E0A77

      output_block is
                                            C38C7074 F18E0A77


      temp is
                          3C51738A 731CB88E C38C7074 F18E0A77


    ------------

      While loop

      Key is
              87 FB72AED6 8C372218 0F23817A 0408B27A 276254BF


      V is
                                            89833176 EBDE673C


Block #1
Blockin   89833176 EBDE673C
Blockout  56212CE3 D47B1446

      output_block is
                                            56212CE3 D47B1446


      temp is
        3C51738A 731CB88E C38C7074 F18E0A77 56212CE3 D47B1446


    ------------

      While loop

      Key is
              87 FB72AED6 8C372218 0F23817A 0408B27A 276254BF


      V is
                                            89833176 EBDE673D
```

```
Block #1
Blockin   89833176 EBDE673D
Blockout  1A276E83 72B83722

      output_block is
                                              1A276E83 72B83722


      temp is
                                              3C51738A 731CB88E
        C38C7074 F18E0A77 56212CE3 D47B1446 1A276E83 72B83722


    temp XOR provided_data is
                                                    3C 51738A73
        1CB88EC3 8C7074F1 8E0A7756 212CE3D4 7B14461A 276E8372


    Key is
              3C 51738A73 1CB88EC3 8C7074F1 8E0A7756 212CE3D4


    V is
                                              7B14461A 276E8372


rnd_val is
                          76FFEB64 F39FD9DC F407C209 7083158B


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Generate FAILED: Reseed is required
***************************************************************
```

```
CTR_DRBG_Reseed

    entropy_input is
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    ------------

      While loop

      Key is
              3C 51738A73 1CB88EC3 8C7074F1 8E0A7756 212CE3D4


      V is
                                              7B14461A 276E8373


Block #1
Blockin   7B14461A 276E8373
Blockout  D866B305 601C7577

      output_block is
                                              D866B305 601C7577


      temp is
                                              D866B305 601C7577


    ------------

      While loop
```

```
      Key is
              3C 51738A73 1CB88EC3 8C7074F1 8E0A7756 212CE3D4


      V is
                                              7B14461A 276E8374


Block #1
Blockin   7B14461A 276E8374
Blockout  7ECE1C31 57A5271C

      output_block is
                                              7ECE1C31 57A5271C


      temp is
                           D866B305 601C7577 7ECE1C31 57A5271C


    ------------

      While loop

      Key is
              3C 51738A73 1CB88EC3 8C7074F1 8E0A7756 212CE3D4


      V is
                                              7B14461A 276E8375


Block #1
Blockin   7B14461A 276E8375
Blockout  B2AB9F80 619B7DE9

      output_block is
                                              B2AB9F80 619B7DE9


      temp is
        D866B305 601C7577 7ECE1C31 57A5271C B2AB9F80 619B7DE9


    ------------
```

```
      While loop

      Key is
              3C 51738A73 1CB88EC3 8C7074F1 8E0A7756 212CE3D4


      V is
                                             7B14461A 276E8376


Block #1
Blockin   7B14461A 276E8376
Blockout  89E3EDC9 23E5FAC0

      output_block is
                                             89E3EDC9 23E5FAC0


      temp is
                                             D866B305 601C7577
        7ECE1C31 57A5271C B2AB9F80 619B7DE9 89E3EDC9 23E5FAC0


    temp XOR provided_data is
                                                   18 A771C6A4
        D9B3B0B6 07D6FA9B 68E9D362 7A4D53B5 4EAB3E51 3A3712FF


    Key is
              18 A771C6A4 D9B3B0B6 07D6FA9B 68E9D362 7A4D53B5


    V is
                                             4EAB3E51 3A3712FF


************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
```

```
Blockin   4EAB3E51 3A371300
Blockout  D7A5955B 81F4EDA1

Block #1
Blockin   4EAB3E51 3A371301
Blockout  E1AE62DF 158FD0BC

---------------------------

  Update

    provided_data is
                                                      00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              18 A771C6A4 D9B3B0B6 07D6FA9B 68E9D362 7A4D53B5


      V is
                                          4EAB3E51 3A371302


Block #1
Blockin   4EAB3E51 3A371302
Blockout  3D186644 E6B3E3B2

      output_block is
                                          3D186644 E6B3E3B2


      temp is
                                          3D186644 E6B3E3B2


    ------------

      While loop

      Key is
              18 A771C6A4 D9B3B0B6 07D6FA9B 68E9D362 7A4D53B5
```

```
      V is
                                              4EAB3E51 3A371303


Block #1
Blockin   4EAB3E51 3A371303
Blockout  28A3A858 BE01177A

      output_block is
                                              28A3A858 BE01177A


      temp is
                           3D186644 E6B3E3B2 28A3A858 BE01177A


    ------------

      While loop

      Key is
              18 A771C6A4 D9B3B0B6 07D6FA9B 68E9D362 7A4D53B5


      V is
                                              4EAB3E51 3A371304


Block #1
Blockin   4EAB3E51 3A371304
Blockout  2EB41D40 2C767A9D

      output_block is
                                              2EB41D40 2C767A9D


      temp is
        3D186644 E6B3E3B2 28A3A858 BE01177A 2EB41D40 2C767A9D


    ------------

      While loop
```

```
      Key is
              18 A771C6A4 D9B3B0B6 07D6FA9B 68E9D362 7A4D53B5


      V is
                                             4EAB3E51 3A371305


Block #1
Blockin   4EAB3E51 3A371305
Blockout  A1D4FCFD 276AB6F8

      output_block is
                                             A1D4FCFD 276AB6F8


      temp is
                                             3D186644 E6B3E3B2
        28A3A858 BE01177A 2EB41D40 2C767A9D A1D4FCFD 276AB6F8


    temp XOR provided_data is
                                                   3D 186644E6
        B3E3B228 A3A858BE 01177A2E B41D402C 767A9DA1 D4FCFD27


    Key is
              3D 186644E6 B3E3B228 A3A858BE 01177A2E B41D402C


    V is
                                             767A9DA1 D4FCFD27


rnd_val is
                          D7A5955B 81F4EDA1 E1AE62DF 158FD0BC


##############################################################

CTR_DRBG

    Requested Security Strength = 112

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
```

```
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    EntropyInput1 (for Reseed1) =
                                                        80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                        60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


    AdditionalInput2 =
                                                        A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Update

    provided_data is
```

                                                    00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000

      V is
                                                00000000 00000001

Block #1
Blockin   00000000 00000001
Blockout 166B40B4 4ABA4BD6

      output_block is
                                                166B40B4 4ABA4BD6

      temp is
                                                166B40B4 4ABA4BD6

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000

      V is
                                                00000000 00000002

Block #1
Blockin   00000000 00000002
Blockout 06E7EA22 CE92708F

      output_block is
                                                06E7EA22 CE92708F

```
      temp is
                           166B40B4 4ABA4BD6 06E7EA22 CE92708F


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                              4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000004


Block #1
Blockin   00000000 00000004
Blockout  D2FD8867 D50D2DFE
```

```
      output_block is
                                                D2FD8867 D50D2DFE


      temp is
                                                166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                    16 6A42B74E
        BF4DD10E EEE029C2 9F7E805E A082DAB6 EF008BCA E4927CC9


    Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


    V is
                                                EF008BCA E4927CC9


---------------------------------------------------------------

First call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                    60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


Generate FAILED: Reseed is required
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                                    80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C
```

```
    additional_input is
                                                        60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


---------------------------

  Update

    provided_data is
                                                        E0 E0E0E0E0
        E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0

    ------------

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                              EF008BCA E4927CCA


Block #1
Blockin   EF008BCA E4927CCA
Blockout  077AF02D 5209B1A5

      output_block is
                                              077AF02D 5209B1A5


      temp is
                                              077AF02D 5209B1A5


    ------------

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6
```

```
      V is
                                              EF008BCA E4927CCB


Block #1
Blockin   EF008BCA E4927CCB
Blockout  9086A90A F689863D

      output_block is
                                              9086A90A F689863D


      temp is
                           077AF02D 5209B1A5 9086A90A F689863D


    ------------

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                              EF008BCA E4927CCC


Block #1
Blockin   EF008BCA E4927CCC
Blockout  EAB6F0C7 2B1C15A6

      output_block is
                                              EAB6F0C7 2B1C15A6


      temp is
        077AF02D 5209B1A5 9086A90A F689863D EAB6F0C7 2B1C15A6


    ------------

      While loop

      Key is
```

```
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                              EF008BCA E4927CCD


Block #1
Blockin   EF008BCA E4927CCD
Blockout  EE7244FC AB83AF9D

      output_block is
                                              EE7244FC AB83AF9D


      temp is
                                              077AF02D 5209B1A5
        9086A90A F689863D EAB6F0C7 2B1C15A6 EE7244FC AB83AF9D


    temp XOR provided_data is
                                                    E7 9A10CDB2
        E9514570 6649EA16 6966DD0A 561027CB FCF5460E 92A41C4B


    Key is
              E7 9A10CDB2 E9514570 6649EA16 6966DD0A 561027CB


    V is
                                              FCF5460E 92A41C4B


*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   FCF5460E 92A41C4C
Blockout  BA52044F 83558BC5

Block #1
```

```
Blockin   FCF5460E 92A41C4D
Blockout  2030A10E 475131CF

---------------------------

  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              E7 9A10CDB2 E9514570 6649EA16 6966DD0A 561027CB


      V is
                                            FCF5460E 92A41C4E


Block #1
Blockin   FCF5460E 92A41C4E
Blockout  2BE9E28C 8DC30D13

      output_block is
                                            2BE9E28C 8DC30D13


      temp is
                                            2BE9E28C 8DC30D13


    ------------

      While loop

      Key is
              E7 9A10CDB2 E9514570 6649EA16 6966DD0A 561027CB


      V is
                                            FCF5460E 92A41C4F
```

```
Block #1
Blockin   FCF5460E 92A41C4F
Blockout  2259089D 9A42987D

      output_block is
                                              2259089D 9A42987D


      temp is
                           2BE9E28C 8DC30D13 2259089D 9A42987D


    ------------

      While loop

      Key is
              E7 9A10CDB2 E9514570 6649EA16 6966DD0A 561027CB


      V is
                                              FCF5460E 92A41C50


Block #1
Blockin   FCF5460E 92A41C50
Blockout  FCAE2830 99B4966B

      output_block is
                                              FCAE2830 99B4966B


      temp is
        2BE9E28C 8DC30D13 2259089D 9A42987D FCAE2830 99B4966B


    ------------

      While loop

      Key is
              E7 9A10CDB2 E9514570 6649EA16 6966DD0A 561027CB
```

```
      V is
                                                FCF5460E 92A41C51


Block #1
Blockin   FCF5460E 92A41C51
Blockout  4072AF99 75399510

      output_block is
                                                4072AF99 75399510


      temp is
                                                2BE9E28C 8DC30D13
        2259089D 9A42987D FCAE2830 99B4966B 4072AF99 75399510


    temp XOR provided_data is
                                                      2B E9E28C8D
        C30D1322 59089D9A 42987DFC AE283099 B4966B40 72AF9975


    Key is
              2B E9E28C8D C30D1322 59089D9A 42987DFC AE283099


    V is
                                                B4966B40 72AF9975


rnd_val is
                           BA52044F 83558BC5 2030A10E 475131CF


------------------------------------------------------------

Second call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                      A0 A1A2A3A4
```

```
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                                    C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    additional_input is
                                                    A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


---------------------------

  Update

    provided_data is
                                                    60 60606060
        60606060 60606060 60606060 60606060 60606060 60606060


    ------------

      While loop

      Key is
              2B E9E28C8D C30D1322 59089D9A 42987DFC AE283099


      V is
                                            B4966B40 72AF9976


Block #1
Blockin   B4966B40 72AF9976
Blockout  EB82D768 1174B314

      output_block is
                                            EB82D768 1174B314
```

```
      temp is
                                              EB82D768 1174B314


    ------------

      While loop

      Key is
              2B E9E28C8D C30D1322 59089D9A 42987DFC AE283099


      V is
                                              B4966B40 72AF9977


Block #1
Blockin   B4966B40 72AF9977
Blockout  298A9A80 7F7BBBE0

      output_block is
                                              298A9A80 7F7BBBE0


      temp is
                           EB82D768 1174B314 298A9A80 7F7BBBE0


    ------------

      While loop

      Key is
              2B E9E28C8D C30D1322 59089D9A 42987DFC AE283099


      V is
                                              B4966B40 72AF9978


Block #1
Blockin   B4966B40 72AF9978
Blockout  B670F4C1 C1EB4DD0

      output_block is
```

```
                                              B670F4C1 C1EB4DD0

      temp is
        EB82D768 1174B314 298A9A80 7F7BBBE0 B670F4C1 C1EB4DD0

    ------------

      While loop

      Key is
              2B E9E28C8D C30D1322 59089D9A 42987DFC AE283099

      V is
                                              B4966B40 72AF9979

Block #1
Blockin   B4966B40 72AF9979
Blockout  3EDD8281 FD1FCA15

      output_block is
                                              3EDD8281 FD1FCA15

      temp is
                                              EB82D768 1174B314
        298A9A80 7F7BBBE0 B670F4C1 C1EB4DD0 3EDD8281 FD1FCA15

    temp XOR provided_data is
                                                    8B E2B70871
        14D37449 EAFAE01F 1BDB80D6 1094A1A1 8B2DB05E BDE2E19D

    Key is
              8B E2B70871 14D37449 EAFAE01F 1BDB80D6 1094A1A1

    V is
                                              8B2DB05E BDE2E19D

**************************************************************
```

```
CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   8B2DB05E BDE2E19E
Blockout  D6EC2A7F B7375E40

Block #1
Blockin   8B2DB05E BDE2E19F
Blockout  C3E6B5C3 6484B2DF

---------------------------

  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              8B E2B70871 14D37449 EAFAE01F 1BDB80D6 1094A1A1


      V is
                                            8B2DB05E BDE2E1A0


Block #1
Blockin   8B2DB05E BDE2E1A0
Blockout  687373F9 F19EB7FE

      output_block is
                                            687373F9 F19EB7FE


      temp is
                                            687373F9 F19EB7FE
```

```
    ------------

      While loop

      Key is
              8B E2B70871 14D37449 EAFAE01F 1BDB80D6 1094A1A1


      V is
                                              8B2DB05E BDE2E1A1


Block #1
Blockin   8B2DB05E BDE2E1A1
Blockout  08960325 F0D6C998

      output_block is
                                              08960325 F0D6C998


      temp is
                           687373F9 F19EB7FE 08960325 F0D6C998


    ------------

      While loop

      Key is
              8B E2B70871 14D37449 EAFAE01F 1BDB80D6 1094A1A1


      V is
                                              8B2DB05E BDE2E1A2


Block #1
Blockin   8B2DB05E BDE2E1A2
Blockout  08AAEFEB 487B3B15

      output_block is
                                              08AAEFEB 487B3B15
```

```
      temp is
        687373F9 F19EB7FE 08960325 F0D6C998 08AAEFEB 487B3B15


    ------------

      While loop

      Key is
              8B E2B70871 14D37449 EAFAE01F 1BDB80D6 1094A1A1


      V is
                                            8B2DB05E BDE2E1A3


Block #1
Blockin   8B2DB05E BDE2E1A3
Blockout  12A4EE6F 2A6B5AC9

      output_block is
                                            12A4EE6F 2A6B5AC9


      temp is
                                            687373F9 F19EB7FE
        08960325 F0D6C998 08AAEFEB 487B3B15 12A4EE6F 2A6B5AC9


    temp XOR provided_data is
                                                  68 7373F9F1
        9EB7FE08 960325F0 D6C99808 AAEFEB48 7B3B1512 A4EE6F2A


    Key is
              68 7373F9F1 9EB7FE08 960325F0 D6C99808 AAEFEB48


    V is
                                            7B3B1512 A4EE6F2A


rnd_val is
                         D6EC2A7F B7375E40 C3E6B5C3 6484B2DF
```

```
###############################################################

CTR_DRBG

    Requested Security Strength = 112

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    EntropyInput1 (for Reseed1) =
                                                        80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    PersonalizationString =
                                                        40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    AdditionalInput = <empty>

###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    personal_str is
                                                        40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    prediction_resistance_flag = "PredictionResistance"
```

```
---------------------------

  Update

    provided_data is
                                                        40 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000001


Block #1
Blockin   00000000 00000001
Blockout  166B40B4 4ABA4BD6

      output_block is
                                              166B40B4 4ABA4BD6


      temp is
                                              166B40B4 4ABA4BD6


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000002
```

```
Block #1
Blockin   00000000 00000002
Blockout  06E7EA22 CE92708F

      output_block is
                                            06E7EA22 CE92708F


      temp is
                          166B40B4 4ABA4BD6 06E7EA22 CE92708F


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                            00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                            4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                            00000000 00000004
```

```
Block #1
Blockin   00000000 00000004
Blockout  D2FD8867 D50D2DFE

      output_block is
                                              D2FD8867 D50D2DFE


      temp is
                                              166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                    56 2B00F40A
        FA0B9646 A7AA628E D230CF0E F1D089E2 BA56DC92 BDC82795


    Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


    V is
                                              BA56DC92 BDC82795


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

CTR_DRBG_Reseed

    entropy_input is
```

```
                                                        80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                                                        80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    ------------

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                            BA56DC92 BDC82796


Block #1
Blockin   BA56DC92 BDC82796
Blockout  9E0082B6 B55E3596

      output_block is
                                            9E0082B6 B55E3596


      temp is
                                            9E0082B6 B55E3596


    ------------

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2
```

```
      V is
                                              BA56DC92 BDC82797


Block #1
Blockin   BA56DC92 BDC82797
Blockout  F1A82251 90390124

      output_block is
                                              F1A82251 90390124


      temp is
                           9E0082B6 B55E3596 F1A82251 90390124


    ------------

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                              BA56DC92 BDC82798


Block #1
Blockin   BA56DC92 BDC82798
Blockout  24C9B2C0 8D487353

      output_block is
                                              24C9B2C0 8D487353


      temp is
        9E0082B6 B55E3596 F1A82251 90390124 24C9B2C0 8D487353


    ------------

      While loop

      Key is
```

```
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                              BA56DC92 BDC82799


Block #1
Blockin   BA56DC92 BDC82799
Blockout  32269D08 E3F6F53A

      output_block is
                                              32269D08 E3F6F53A


      temp is
                                              9E0082B6 B55E3596
        F1A82251 90390124 24C9B2C0 8D487353 32269D08 E3F6F53A


    temp XOR provided_data is
                                                    1E 81003531
        DBB31179 21A8DA1C B48FABB4 58205319 DDE5C4AA BF07937F


    Key is
              1E 81003531 DBB31179 21A8DA1C B48FABB4 58205319


    V is
                                              DDE5C4AA BF07937F


************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   DDE5C4AA BF079380
Blockout  9AF00447 842ADA5C

Block #1
```

```
Blockin   DDE5C4AA BF079381
Blockout  26AAE321 F0707EAB

---------------------------

  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              1E 81003531 DBB31179 21A8DA1C B48FABB4 58205319


      V is
                                            DDE5C4AA BF079382


Block #1
Blockin   DDE5C4AA BF079382
Blockout  910C6503 F2C38D10

      output_block is
                                            910C6503 F2C38D10


      temp is
                                            910C6503 F2C38D10


    ------------

      While loop

      Key is
              1E 81003531 DBB31179 21A8DA1C B48FABB4 58205319


      V is
                                            DDE5C4AA BF079383
```

```
Block #1
Blockin   DDE5C4AA BF079383
Blockout  11C9D57A D32E1393

      output_block is
                                            11C9D57A D32E1393


      temp is
                          910C6503 F2C38D10 11C9D57A D32E1393


    ------------

      While loop

      Key is
              1E 81003531 DBB31179 21A8DA1C B48FABB4 58205319


      V is
                                            DDE5C4AA BF079384


Block #1
Blockin   DDE5C4AA BF079384
Blockout  8B4223C3 EB3DA759

      output_block is
                                            8B4223C3 EB3DA759


      temp is
        910C6503 F2C38D10 11C9D57A D32E1393 8B4223C3 EB3DA759


    ------------

      While loop

      Key is
              1E 81003531 DBB31179 21A8DA1C B48FABB4 58205319
```

```
      V is
                                              DDE5C4AA BF079385


Block #1
Blockin   DDE5C4AA BF079385
Blockout  B37E305E 79F946EF

      output_block is
                                              B37E305E 79F946EF


      temp is
                                              910C6503 F2C38D10
        11C9D57A D32E1393 8B4223C3 EB3DA759 B37E305E 79F946EF


    temp XOR provided_data is
                                                    91 0C6503F2
        C38D1011 C9D57AD3 2E13938B 4223C3EB 3DA759B3 7E305E79


    Key is
              91 0C6503F2 C38D1011 C9D57AD3 2E13938B 4223C3EB


    V is
                                              3DA759B3 7E305E79


rnd_val is
                          9AF00447 842ADA5C 26AAE321 F0707EAB


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>
```

```
Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    ------------

      While loop

      Key is
              91 0C6503F2 C38D1011 C9D57AD3 2E13938B 4223C3EB


      V is
                                            3DA759B3 7E305E7A


Block #1
Blockin   3DA759B3 7E305E7A
Blockout  81A533D1 D557C36F

      output_block is
                                            81A533D1 D557C36F


      temp is
                                            81A533D1 D557C36F


    ------------
```

```
      While loop

      Key is
              91 0C6503F2 C38D1011 C9D57AD3 2E13938B 4223C3EB


      V is
                                             3DA759B3 7E305E7B


Block #1
Blockin   3DA759B3 7E305E7B
Blockout  CB17A484 D1AA94ED

      output_block is
                                             CB17A484 D1AA94ED


      temp is
                           81A533D1 D557C36F CB17A484 D1AA94ED


    ------------

      While loop

      Key is
              91 0C6503F2 C38D1011 C9D57AD3 2E13938B 4223C3EB


      V is
                                             3DA759B3 7E305E7C


Block #1
Blockin   3DA759B3 7E305E7C
Blockout  6E226341 0E9181B2

      output_block is
                                             6E226341 0E9181B2


      temp is
        81A533D1 D557C36F CB17A484 D1AA94ED 6E226341 0E9181B2
```

```
    ------------

      While loop

      Key is
              91 0C6503F2 C38D1011 C9D57AD3 2E13938B 4223C3EB


      V is
                                            3DA759B3 7E305E7D


Block #1
Blockin   3DA759B3 7E305E7D
Blockout  94D47C0A 5C1EA253

      output_block is
                                            94D47C0A 5C1EA253


      temp is
                                            81A533D1 D557C36F
        CB17A484 D1AA94ED 6E226341 0E9181B2 94D47C0A 5C1EA253


    temp XOR provided_data is
                                                  41 64F11211
        9205A803 DE6E4F1D 675A22BE F3B192DA 4457654C 0DA6D180


    Key is
              41 64F11211 9205A803 DE6E4F1D 675A22BE F3B192DA


    V is
                                            4457654C 0DA6D180


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>
```

```
Block #1
Blockin   4457654C 0DA6D181
Blockout  B1C2B79F 8D857055

Block #1
Blockin   4457654C 0DA6D182
Blockout  7B650EE3 B1F3A674

---------------------------

  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              41 64F11211 9205A803 DE6E4F1D 675A22BE F3B192DA


      V is
                                            4457654C 0DA6D183


Block #1
Blockin   4457654C 0DA6D183
Blockout  81AD00BD 39189E1D

      output_block is
                                            81AD00BD 39189E1D


      temp is
                                            81AD00BD 39189E1D


    ------------

      While loop
```

```
      Key is
              41 64F11211 9205A803 DE6E4F1D 675A22BE F3B192DA


      V is
                                              4457654C 0DA6D184


Block #1
Blockin   4457654C 0DA6D184
Blockout  250F9C5C 79DFDAC3

      output_block is
                                              250F9C5C 79DFDAC3


      temp is
                           81AD00BD 39189E1D 250F9C5C 79DFDAC3


    ------------

      While loop

      Key is
              41 64F11211 9205A803 DE6E4F1D 675A22BE F3B192DA


      V is
                                              4457654C 0DA6D185


Block #1
Blockin   4457654C 0DA6D185
Blockout  9AFB6A1D 0C2928D1

      output_block is
                                              9AFB6A1D 0C2928D1


      temp is
        81AD00BD 39189E1D 250F9C5C 79DFDAC3 9AFB6A1D 0C2928D1


    ------------
```

```
      While loop

      Key is
              41 64F11211 9205A803 DE6E4F1D 675A22BE F3B192DA


      V is
                                            4457654C 0DA6D186


Block #1
Blockin   4457654C 0DA6D186
Blockout  E6EB7429 1551530A

      output_block is
                                            E6EB7429 1551530A


      temp is
                                            81AD00BD 39189E1D
        250F9C5C 79DFDAC3 9AFB6A1D 0C2928D1 E6EB7429 1551530A


    temp XOR provided_data is
                                                  81 AD00BD39
        189E1D25 0F9C5C79 DFDAC39A FB6A1D0C 2928D1E6 EB742915


    Key is
              81 AD00BD39 189E1D25 0F9C5C79 DFDAC39A FB6A1D0C


    V is
                                            2928D1E6 EB742915


rnd_val is
                         B1C2B79F 8D857055 7B650EE3 B1F3A674


###############################################################

CTR_DRBG

    Requested Security Strength = 112
```

```
    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    EntropyInput1 (for Reseed1) =
                                                        80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    PersonalizationString =
                                                        40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    AdditionalInput1 =
                                                        60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


    AdditionalInput2 =
                                                        A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    personal_str is
                                                        40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C
```

```
    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Update

    provided_data is
                                                        40 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                            00000000 00000001


Block #1
Blockin   00000000 00000001
Blockout  166B40B4 4ABA4BD6

      output_block is
                                            166B40B4 4ABA4BD6


      temp is
                                            166B40B4 4ABA4BD6


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                            00000000 00000002
```

```
Block #1
Blockin   00000000 00000002
Blockout  06E7EA22 CE92708F

      output_block is
                                            06E7EA22 CE92708F


      temp is
                          166B40B4 4ABA4BD6 06E7EA22 CE92708F


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                            00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                            4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000
```

```
      V is
                                                00000000 00000004


Block #1
Blockin   00000000 00000004
Blockout  D2FD8867 D50D2DFE

      output_block is
                                                D2FD8867 D50D2DFE


      temp is
                                                166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                        56 2B00F40A
        FA0B9646 A7AA628E D230CF0E F1D089E2 BA56DC92 BDC82795


    Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


    V is
                                                BA56DC92 BDC82795


------------------------------------------------------------

First call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                        60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


Generate FAILED: Reseed is required
```

```
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                                        80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    additional_input is
                                                        60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


----------------------------

  Update

    provided_data is
                                                        E0 E0E0E0E0
        E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0


    ------------

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                              BA56DC92 BDC82796


Block #1
Blockin   BA56DC92 BDC82796
Blockout  9E0082B6 B55E3596

      output_block is
                                              9E0082B6 B55E3596


      temp is
                                              9E0082B6 B55E3596
```

```
    ------------

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                           BA56DC92 BDC82797


Block #1
Blockin   BA56DC92 BDC82797
Blockout  F1A82251 90390124

      output_block is
                                           F1A82251 90390124


      temp is
                           9E0082B6 B55E3596 F1A82251 90390124


    ------------

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                           BA56DC92 BDC82798


Block #1
Blockin   BA56DC92 BDC82798
Blockout  24C9B2C0 8D487353

      output_block is
                                           24C9B2C0 8D487353


      temp is
```

```
        9E0082B6 B55E3596 F1A82251 90390124 24C9B2C0 8D487353


    ------------

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                            BA56DC92 BDC82799


Block #1
Blockin   BA56DC92 BDC82799
Blockout  32269D08 E3F6F53A

      output_block is
                                            32269D08 E3F6F53A


      temp is
                                            9E0082B6 B55E3596
        F1A82251 90390124 24C9B2C0 8D487353 32269D08 E3F6F53A


    temp XOR provided_data is
                                                  7E E0625655
        BED57611 48C2B170 D9E1C4C4 2952206D A893B3D2 C67DE803


    Key is
              7E E0625655 BED57611 48C2B170 D9E1C4C4 2952206D


    V is
                                            A893B3D2 C67DE803


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128
```

```
    additional_input is  <empty>

Block #1
Blockin   A893B3D2 C67DE804
Blockout  58674F0B CD88A4F5

Block #1
Blockin   A893B3D2 C67DE805
Blockout  107F6E91 FCFC477C

---------------------------

  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              7E E0625655 BED57611 48C2B170 D9E1C4C4 2952206D


      V is
                                            A893B3D2 C67DE806


Block #1
Blockin   A893B3D2 C67DE806
Blockout  65697455 25220EB7

      output_block is
                                            65697455 25220EB7


      temp is
                                            65697455 25220EB7


    ------------
```

```
      While loop

      Key is
              7E E0625655 BED57611 48C2B170 D9E1C4C4 2952206D


      V is
                                            A893B3D2 C67DE807


Block #1
Blockin   A893B3D2 C67DE807
Blockout  F4F55A13 656ADFDF

      output_block is
                                            F4F55A13 656ADFDF


      temp is
                           65697455 25220EB7 F4F55A13 656ADFDF


    ------------

      While loop

      Key is
              7E E0625655 BED57611 48C2B170 D9E1C4C4 2952206D


      V is
                                            A893B3D2 C67DE808


Block #1
Blockin   A893B3D2 C67DE808
Blockout  8C5A56BA 299916BC

      output_block is
                                            8C5A56BA 299916BC


      temp is
        65697455 25220EB7 F4F55A13 656ADFDF 8C5A56BA 299916BC
```

```
    ------------

      While loop

      Key is
              7E E0625655 BED57611 48C2B170 D9E1C4C4 2952206D


      V is
                                            A893B3D2 C67DE809


Block #1
Blockin   A893B3D2 C67DE809
Blockout  6D65AF83 8CC02CDA

      output_block is
                                            6D65AF83 8CC02CDA


      temp is
                                            65697455 25220EB7
        F4F55A13 656ADFDF 8C5A56BA 299916BC 6D65AF83 8CC02CDA


    temp XOR provided_data is
                                                   65 69745525
        220EB7F4 F55A1365 6ADFDF8C 5A56BA29 9916BC6D 65AF838C


    Key is
              65 69745525 220EB7F4 F55A1365 6ADFDF8C 5A56BA29


    V is
                                            9916BC6D 65AF838C


rnd_val is
                          58674F0B CD88A4F5 107F6E91 FCFC477C


---------------------------------------------------------------

Second call to Generate
```

```
***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                        A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


Generate FAILED: Reseed is required
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    additional_input is
                                                        A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


---------------------------

  Update

    provided_data is
                                                        60 60606060
        60606060 60606060 60606060 60606060 60606060 60606060


    ------------

      While loop

      Key is
              65 69745525 220EB7F4 F55A1365 6ADFDF8C 5A56BA29


      V is
                                              9916BC6D 65AF838D
```

```
Block #1
Blockin   9916BC6D 65AF838D
Blockout  43055D6A DBC6F3D9

      output_block is
                                              43055D6A DBC6F3D9


      temp is
                                              43055D6A DBC6F3D9


    ------------

      While loop

      Key is
              65 69745525 220EB7F4 F55A1365 6ADFDF8C 5A56BA29


      V is
                                              9916BC6D 65AF838E


Block #1
Blockin   9916BC6D 65AF838E
Blockout  54F1A12F 32EFF9EA

      output_block is
                                              54F1A12F 32EFF9EA


      temp is
                           43055D6A DBC6F3D9 54F1A12F 32EFF9EA


    ------------

      While loop

      Key is
              65 69745525 220EB7F4 F55A1365 6ADFDF8C 5A56BA29


      V is
```

```
                                                9916BC6D 65AF838F


Block #1
Blockin   9916BC6D 65AF838F
Blockout  586C4927 579F889F

      output_block is
                                                586C4927 579F889F


      temp is
        43055D6A DBC6F3D9 54F1A12F 32EFF9EA 586C4927 579F889F


    ------------

      While loop

      Key is
              65 69745525 220EB7F4 F55A1365 6ADFDF8C 5A56BA29


      V is
                                                9916BC6D 65AF8390


Block #1
Blockin   9916BC6D 65AF8390
Blockout  5526CF26 D53D3D01

      output_block is
                                                5526CF26 D53D3D01


      temp is
                                                43055D6A DBC6F3D9
        54F1A12F 32EFF9EA 586C4927 579F889F 5526CF26 D53D3D01


    temp XOR provided_data is
                                                       23 653D0ABB
        A693B934 91C14F52 8F998A38 0C294737 FFE8FF35 46AF46B5


    Key is
```

```
              23 653D0ABB A693B934 91C14F52 8F998A38 0C294737


    V is
                                            FFE8FF35 46AF46B5

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   FFE8FF35 46AF46B6
Blockout  65DD535E 768645BF

Block #1
Blockin   FFE8FF35 46AF46B7
Blockout  23701A88 93BA9AFB

---------------------------

  Update

    provided_data is
                                                    00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              23 653D0ABB A693B934 91C14F52 8F998A38 0C294737


      V is
                                            FFE8FF35 46AF46B8


Block #1
Blockin   FFE8FF35 46AF46B8
```

```
Blockout  3957588B 002DE9AC

      output_block is
                                              3957588B 002DE9AC


      temp is
                                              3957588B 002DE9AC


    ------------

      While loop

      Key is
              23 653D0ABB A693B934 91C14F52 8F998A38 0C294737


      V is
                                              FFE8FF35 46AF46B9


Block #1
Blockin   FFE8FF35 46AF46B9
Blockout  0A9737D8 D1F906D4

      output_block is
                                              0A9737D8 D1F906D4


      temp is
                           3957588B 002DE9AC 0A9737D8 D1F906D4


    ------------

      While loop

      Key is
              23 653D0ABB A693B934 91C14F52 8F998A38 0C294737


      V is
                                              FFE8FF35 46AF46BA
```

```
Block #1
Blockin   FFE8FF35 46AF46BA
Blockout  D6362C4D 53DB11D2

      output_block is
                                              D6362C4D 53DB11D2


      temp is
        3957588B 002DE9AC 0A9737D8 D1F906D4 D6362C4D 53DB11D2


    ------------

      While loop

      Key is
              23 653D0ABB A693B934 91C14F52 8F998A38 0C294737


      V is
                                              FFE8FF35 46AF46BB


Block #1
Blockin   FFE8FF35 46AF46BB
Blockout  A0CC9C70 49FA167F

      output_block is
                                              A0CC9C70 49FA167F


      temp is
                                              3957588B 002DE9AC
        0A9737D8 D1F906D4 D6362C4D 53DB11D2 A0CC9C70 49FA167F


    temp XOR provided_data is
                                                    39 57588B00
        2DE9AC0A 9737D8D1 F906D4D6 362C4D53 DB11D2A0 CC9C7049


    Key is
              39 57588B00 2DE9AC0A 9737D8D1 F906D4D6 362C4D53
```

```
    V is
                                                DB11D2A0 CC9C7049


rnd_val is
                           65DD535E 768645BF 23701A88 93BA9AFB


################################################################

CTR_DRBG

    Requested Security Strength = 128

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    personal_str is  <empty>
```

```
    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Update

    provided_data is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    ------------

      While loop

      Key is
                          00000000 00000000 00000000 00000000


      V is
                          00000000 00000000 00000000 00000001


      output_block is
                          58E2FCCE FA7E3061 367F1D57 A4E7455A


      temp is
                          58E2FCCE FA7E3061 367F1D57 A4E7455A


    ------------

      While loop

      Key is
                          00000000 00000000 00000000 00000000


      V is
                          00000000 00000000 00000000 00000002


      output_block is
                          0388DACE 60B6A392 F328C2B9 71B2FE78
```

```
      temp is
                                                58E2FCCE FA7E3061
        367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78


    temp XOR provided_data is
                                                58E3FECD FE7B3666
        3E76175C A8EA4B55 1399C8DD 74A3B585 EB31D8A2 6DAFE067


    Key is
                           58E3FECD FE7B3666 3E76175C A8EA4B55


    V is
                           1399C8DD 74A3B585 EB31D8A2 6DAFE067


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
```

```
                    58E3FECD FE7B3666 3E76175C A8EA4B55

  V is
                    1399C8DD 74A3B585 EB31D8A2 6DAFE06A

  output_block is
                    14810C15 D85DA566 5C2518B4 553FB155

  temp is
                    14810C15 D85DA566 5C2518B4 553FB155

------------

  While loop

  Key is
                    58E3FECD FE7B3666 3E76175C A8EA4B55

  V is
                    1399C8DD 74A3B585 EB31D8A2 6DAFE06B

  output_block is
                    B85442C7 900E7D82 7A11C60D 18F424E5

  temp is
                                      14810C15 D85DA566
    5C2518B4 553FB155 B85442C7 900E7D82 7A11C60D 18F424E5

temp XOR provided_data is
                                      14810C15 D85DA566
    5C2518B4 553FB155 B85442C7 900E7D82 7A11C60D 18F424E5

Key is
                    14810C15 D85DA566 5C2518B4 553FB155

V is
```

```
                        B85442C7 900E7D82 7A11C60D 18F424E5


rnd_val is
                                                 1686FFCF 9F358BE7
        4452E647 BA156AAB 05135797 117FD1AB 317D318C 660E3D18


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                                                 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                        14810C15 D85DA566 5C2518B4 553FB155


      V is
                        B85442C7 900E7D82 7A11C60D 18F424E8


      output_block is
                        F75ECD8C D778C71E F4DC13AC 0779723F


      temp is
```

F75ECD8C D778C71E F4DC13AC 0779723F

While loop

Key is
14810C15 D85DA566 5C2518B4 553FB155

V is
B85442C7 900E7D82 7A11C60D 18F424E9

output_block is
2AE70FAB CD77683C DC921607 9C291D5B

temp is
F75ECD8C D778C71E
F4DC13AC 0779723F 2AE70FAB CD77683C DC921607 9C291D5B

temp XOR provided_data is
F75ECD8C D778C71E
F4DC13AC 0779723F 2AE70FAB CD77683C DC921607 9C291D5B

Key is
F75ECD8C D778C71E F4DC13AC 0779723F

V is
2AE70FAB CD77683C DC921607 9C291D5B

rnd_val is
F89A638F 026010CF
B9DCC706 B34C789C 07B94FD4 6DAB90EC 866A523B D05EF2CA

##

CTR_DRBG

```
    Requested Security Strength = 128

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    AdditionalInput2 =
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

--------------------------
```

```
Update

  provided_data is
                                          00010203 04050607
      08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


  ------------

    While loop

    Key is
                        00000000 00000000 00000000 00000000


    V is
                        00000000 00000000 00000000 00000001


    output_block is
                        58E2FCCE FA7E3061 367F1D57 A4E7455A


    temp is
                        58E2FCCE FA7E3061 367F1D57 A4E7455A


  ------------

    While loop

    Key is
                        00000000 00000000 00000000 00000000


    V is
                        00000000 00000000 00000000 00000002


    output_block is
                        0388DACE 60B6A392 F328C2B9 71B2FE78


    temp is
                                          58E2FCCE FA7E3061
```

```
        367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78


    temp XOR provided_data is
                                              58E3FECD FE7B3666
        3E76175C A8EA4B55 1399C8DD 74A3B585 EB31D8A2 6DAFE067


    Key is
                          58E3FECD FE7B3666 3E76175C A8EA4B55


    V is
                          1399C8DD 74A3B585 EB31D8A2 6DAFE067


---------------------------------------------------------------

First call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                              60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
                                              60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    ------------

      While loop

      Key is
```

```
                    58E3FECD FE7B3666 3E76175C A8EA4B55

  V is
                    1399C8DD 74A3B585 EB31D8A2 6DAFE068

  output_block is
                    1686FFCF 9F358BE7 4452E647 BA156AAB

  temp is
                    1686FFCF 9F358BE7 4452E647 BA156AAB

------------

  While loop

  Key is
                    58E3FECD FE7B3666 3E76175C A8EA4B55

  V is
                    1399C8DD 74A3B585 EB31D8A2 6DAFE069

  output_block is
                    05135797 117FD1AB 317D318C 660E3D18

  temp is
                                      1686FFCF 9F358BE7
    4452E647 BA156AAB 05135797 117FD1AB 317D318C 660E3D18

temp XOR provided_data is
                                      76E79DAC FB50ED80
    2C3B8C2C D67804C4 756225E4 650AA7DC 49044BF7 1A734367

Key is
                    76E79DAC FB50ED80 2C3B8C2C D67804C4

V is
```

```
                          756225E4 650AA7DC 49044BF7 1A734367


---------------------------

  Update

    provided_data is
                                                 60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    ------------

      While loop

      Key is
                          76E79DAC FB50ED80 2C3B8C2C D67804C4


      V is
                          756225E4 650AA7DC 49044BF7 1A73436A


      output_block is
                          04E81A0B 49D43C63 DD088CA7 02467720


      temp is
                          04E81A0B 49D43C63 DD088CA7 02467720


    ------------

      While loop

      Key is
                          76E79DAC FB50ED80 2C3B8C2C D67804C4


      V is
                          756225E4 650AA7DC 49044BF7 1A73436B


      output_block is
                          2929B2BC F2CFDA80 A358BBC8 543103C9
```

```
      temp is
                                                04E81A0B 49D43C63
        DD088CA7 02467720 2929B2BC F2CFDA80 A358BBC8 543103C9


    temp XOR provided_data is
                                                64897868 2DB15A04
        B561E6CC 6E2B194F 5958C0CF 86BAACF7 DB21C1B3 284C7DB6


    Key is
                           64897868 2DB15A04 B561E6CC 6E2B194F


    V is
                           5958C0CF 86BAACF7 DB21C1B3 284C7DB6


rnd_val is
                                                CBFD7872 46E49C1C
        98569F68 5B808D8B 916F747C 09D419BE 60AF0735 2C60274A


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
```

```
                                          A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


------------

  While loop

  Key is
                      64897868 2DB15A04 B561E6CC 6E2B194F


  V is
                      5958C0CF 86BAACF7 DB21C1B3 284C7DB7


  output_block is
                      2B9AFD91 EF659E4D BBE23AF5 22244A27


  temp is
                      2B9AFD91 EF659E4D BBE23AF5 22244A27


------------

  While loop

  Key is
                      64897868 2DB15A04 B561E6CC 6E2B194F


  V is
                      5958C0CF 86BAACF7 DB21C1B3 284C7DB8


  output_block is
                      AC0565F4 30E74EA4 A9FA4FBF 50B048F1


  temp is
                                          2B9AFD91 EF659E4D
    BBE23AF5 22244A27 AC0565F4 30E74EA4 A9FA4FBF 50B048F1


temp XOR provided_data is
```

```
                                                8B3B5F32 4BC038EA
        134B905E 8E89E488 1CB4D747 8452F813 1143F504 EC0DF64E


    Key is
                          8B3B5F32 4BC038EA 134B905E 8E89E488


    V is
                          1CB4D747 8452F813 1143F504 EC0DF64E


---------------------------

  Update

    provided_data is
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    ------------

      While loop

      Key is
                          8B3B5F32 4BC038EA 134B905E 8E89E488


      V is
                          1CB4D747 8452F813 1143F504 EC0DF651


      output_block is
                          924095AD 1828265A EFBCC516 A8BBFD25


      temp is
                          924095AD 1828265A EFBCC516 A8BBFD25


    ------------

      While loop

      Key is
```

```
                        8B3B5F32 4BC038EA 134B905E 8E89E488

      V is
                        1CB4D747 8452F813 1143F504 EC0DF652

      output_block is
                        F9811209 0A5F536D E0FFEBD2 FDCFAE56

      temp is
                                                 924095AD 1828265A
        EFBCC516 A8BBFD25 F9811209 0A5F536D E0FFEBD2 FDCFAE56

    temp XOR provided_data is
                                                 32E1370E BC8D80FD
        47156FBD 0416538A 4930A0BA BEEAE5DA 58465169 417210E9

    Key is
                        32E1370E BC8D80FD 47156FBD 0416538A

    V is
                        4930A0BA BEEAE5DA 58465169 417210E9

rnd_val is
                                                 3911B096 E12EE1C9
        DF59DD91 73BA0A49 6C39B748 705891B8 E08C1F36 E039BCE1

################################################################

CTR_DRBG

    Requested Security Strength = 128

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
```

```
    EntropyInput1 (for Reseed1) =
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    PersonalizationString =
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    AdditionalInput = <empty>

#################################################################

*****************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    personal_str is
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Update

    provided_data is
                                                40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


    ------------
```

```
  While loop

  Key is
                      00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000001

  output_block is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A

  temp is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A

------------

  While loop

  Key is
                      00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000002

  output_block is
                      0388DACE 60B6A392 F328C2B9 71B2FE78

  temp is
                                        58E2FCCE FA7E3061
    367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78

temp XOR provided_data is
                                        18A2BC8E BA3E7021
    763F5D17 E4A7051A 43C89A8E 20F6E3D2 B36882F9 31F2BE38

Key is
                      18A2BC8E BA3E7021 763F5D17 E4A7051A
```

```
    V is
                          43C89A8E 20F6E3D2 B36882F9 31F2BE38

------------------------------------------------------------

First call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                                                 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                          18A2BC8E BA3E7021 763F5D17 E4A7051A


      V is
                          43C89A8E 20F6E3D2 B36882F9 31F2BE3B


      output_block is
                          FD9E5A45 0FBEACBA C48AE96E A7E0B6EB


      temp is
                          FD9E5A45 0FBEACBA C48AE96E A7E0B6EB
```

```
    ------------

      While loop

      Key is
                           18A2BC8E BA3E7021 763F5D17 E4A7051A


      V is
                           43C89A8E 20F6E3D2 B36882F9 31F2BE3C


      output_block is
                           33CED475 402EF666 C064E09E A9FD86B7


      temp is
                                             FD9E5A45 0FBEACBA
        C48AE96E A7E0B6EB 33CED475 402EF666 C064E09E A9FD86B7


    temp XOR provided_data is
                                             FD9E5A45 0FBEACBA
        C48AE96E A7E0B6EB 33CED475 402EF666 C064E09E A9FD86B7


    Key is
                           FD9E5A45 0FBEACBA C48AE96E A7E0B6EB


    V is
                           33CED475 402EF666 C064E09E A9FD86B7


rnd_val is
                                             FA1DF743 5039C649
        3B14D8C8 F9715BA5 CE6EE312 20EEDEE3 65A4B6B7 2FD68554


---------------------------------------------------------------

Second call to Generate

***************************************************************
```

```
CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                          FD9E5A45 0FBEACBA C48AE96E A7E0B6EB


      V is
                          33CED475 402EF666 C064E09E A9FD86BA


      output_block is
                          C2A75EEC 1593F3C0 11831516 F32115D9


      temp is
                          C2A75EEC 1593F3C0 11831516 F32115D9


    ------------

      While loop

      Key is
                          FD9E5A45 0FBEACBA C48AE96E A7E0B6EB


      V is
                          33CED475 402EF666 C064E09E A9FD86BB
```

```
      output_block is
                          FE3B7B8C 420F4BC7 9EAFC24A 4E4F54ED


      temp is
                                              C2A75EEC 1593F3C0
        11831516 F32115D9 FE3B7B8C 420F4BC7 9EAFC24A 4E4F54ED


    temp XOR provided_data is
                                              C2A75EEC 1593F3C0
        11831516 F32115D9 FE3B7B8C 420F4BC7 9EAFC24A 4E4F54ED


    Key is
                          C2A75EEC 1593F3C0 11831516 F32115D9


    V is
                          FE3B7B8C 420F4BC7 9EAFC24A 4E4F54ED


rnd_val is
                                              021F0DA0 6944CB4B
        20A5E7CD 3740B1E6 AB90B3AA 66638A03 5BAC12CC F29C148A


################################################################

CTR_DRBG

    Requested Security Strength = 128

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                              00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                              80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
```

```
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    PersonalizationString =
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    AdditionalInput1 =
                                                60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    AdditionalInput2 =
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    personal_str is
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Update

    provided_data is
                                                40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040
```

```
------------

  While loop

  Key is
                      00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000001

  output_block is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A

  temp is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A

------------

  While loop

  Key is
                      00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000002

  output_block is
                      0388DACE 60B6A392 F328C2B9 71B2FE78

  temp is
                                        58E2FCCE FA7E3061
    367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78

temp XOR provided_data is
                                        18A2BC8E BA3E7021
    763F5D17 E4A7051A 43C89A8E 20F6E3D2 B36882F9 31F2BE38
```

```
    Key is
                          18A2BC8E BA3E7021 763F5D17 E4A7051A

    V is
                          43C89A8E 20F6E3D2 B36882F9 31F2BE38

-----------------------------------------------------------

First call to Generate

***********************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                              60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
                                              60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    ------------

      While loop

      Key is
                          18A2BC8E BA3E7021 763F5D17 E4A7051A


      V is
                          43C89A8E 20F6E3D2 B36882F9 31F2BE39


      output_block is
```

```
                        FA1DF743 5039C649 3B14D8C8 F9715BA5

      temp is
                        FA1DF743 5039C649 3B14D8C8 F9715BA5

    ------------

      While loop

      Key is
                        18A2BC8E BA3E7021 763F5D17 E4A7051A

      V is
                        43C89A8E 20F6E3D2 B36882F9 31F2BE3A

      output_block is
                        CE6EE312 20EEDEE3 65A4B6B7 2FD68554

      temp is
                                          FA1DF743 5039C649
        3B14D8C8 F9715BA5 CE6EE312 20EEDEE3 65A4B6B7 2FD68554

    temp XOR provided_data is
                                          9A7C9520 345CA02E
       537DB2A3 951C35CA BE1F9161 549BA894 1DDDCCCC 53ABFB2B

    Key is
                        9A7C9520 345CA02E 537DB2A3 951C35CA

    V is
                        BE1F9161 549BA894 1DDDCCCC 53ABFB2B

---------------------------

  Update

    provided_data is
```

```
                                          60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F

------------

  While loop

  Key is
                     9A7C9520 345CA02E 537DB2A3 951C35CA

  V is
                     BE1F9161 549BA894 1DDDCCCC 53ABFB2E

  output_block is
                     BB26AF64 4DFF74EF 86BE7D45 7D176B7D

  temp is
                     BB26AF64 4DFF74EF 86BE7D45 7D176B7D

------------

  While loop

  Key is
                     9A7C9520 345CA02E 537DB2A3 951C35CA

  V is
                     BE1F9161 549BA894 1DDDCCCC 53ABFB2F

  output_block is
                     F463EBC4 F2456A66 28274CC5 1569216E

  temp is
                                          BB26AF64 4DFF74EF
    86BE7D45 7D176B7D F463EBC4 F2456A66 28274CC5 1569216E

temp XOR provided_data is
```

```
                                                DB47CD07 299A1288
        EED7172E 117A0512 841299B7 86301C11 505E36BE 69145F11


    Key is
                          DB47CD07 299A1288 EED7172E 117A0512


    V is
                          841299B7 86301C11 505E36BE 69145F11


rnd_val is
                                                CBCA7021 E6E00F5C
        E8F499CA 8E566B48 05094A95 91DEDA27 47191006 3A6DA790


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    ------------

      While loop
```

```
  Key is
                      DB47CD07 299A1288 EED7172E 117A0512

  V is
                      841299B7 86301C11 505E36BE 69145F12

  output_block is
                      8283CC8B 341C8A7F 6C4A7D82 477E7EA2

  temp is
                      8283CC8B 341C8A7F 6C4A7D82 477E7EA2

------------

  While loop

  Key is
                      DB47CD07 299A1288 EED7172E 117A0512

  V is
                      841299B7 86301C11 505E36BE 69145F13

  output_block is
                      04E254CC 86E2E651 0D6F26C8 A2547E78

  temp is
                                        8283CC8B 341C8A7F
    6C4A7D82 477E7EA2 04E254CC 86E2E651 0D6F26C8 A2547E78

temp XOR provided_data is
                                        22226E28 90B92CD8
    C4E3D729 EBD3D00D B453E67F 325750E6 B5D69C73 1EE9C0C7

Key is
                      22226E28 90B92CD8 C4E3D729 EBD3D00D
```

```
    V is
                          B453E67F 325750E6 B5D69C73 1EE9C0C7


----------------------------

  Update

    provided_data is
                                                 A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    ------------

      While loop

      Key is
                          22226E28 90B92CD8 C4E3D729 EBD3D00D


      V is
                          B453E67F 325750E6 B5D69C73 1EE9C0CA


      output_block is
                          328F23F8 54E627F9 EB672EBC 79A7EA84


      temp is
                          328F23F8 54E627F9 EB672EBC 79A7EA84


    ------------

      While loop

      Key is
                          22226E28 90B92CD8 C4E3D729 EBD3D00D


      V is
                          B453E67F 325750E6 B5D69C73 1EE9C0CB


      output_block is
```

```
                        844E2773 02ED019C 212C2D7F 41A89738


      temp is
                                             328F23F8 54E627F9
        EB672EBC 79A7EA84 844E2773 02ED019C 212C2D7F 41A89738


    temp XOR provided_data is
                                             922E815B F043815E
        43CE8417 D50A442B 34FF95C0 B658B72B 999597C4 FD152987


    Key is
                        922E815B F043815E 43CE8417 D50A442B


    V is
                        34FF95C0 B658B72B 999597C4 FD152987


rnd_val is
                                             CB502773 1CCD0686
        04478567 64A3D2F1 909E1AB1 2FF39EF7 004390C3 F645ED70


################################################################

CTR_DRBG

    Requested Security Strength = 128

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                             00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                             80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                             C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
```

```
    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Update

    provided_data is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    ------------

      While loop

      Key is
                          00000000 00000000 00000000 00000000


      V is
                          00000000 00000000 00000000 00000001


      output_block is
                          58E2FCCE FA7E3061 367F1D57 A4E7455A
```

```
      temp is
                          58E2FCCE FA7E3061 367F1D57 A4E7455A


    ------------

      While loop

      Key is
                          00000000 00000000 00000000 00000000


      V is
                          00000000 00000000 00000000 00000002


      output_block is
                          0388DACE 60B6A392 F328C2B9 71B2FE78


      temp is
                                            58E2FCCE FA7E3061
        367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78


    temp XOR provided_data is
                                            58E3FECD FE7B3666
        3E76175C A8EA4B55 1399C8DD 74A3B585 EB31D8A2 6DAFE067


    Key is
                          58E3FECD FE7B3666 3E76175C A8EA4B55


    V is
                          1399C8DD 74A3B585 EB31D8A2 6DAFE067


----------------------------------------------------------------

First call to Generate

****************************************************************

CTR_DRBG_Generate
```

```
  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    ------------

      While loop

      Key is
                          58E3FECD FE7B3666 3E76175C A8EA4B55


      V is
                          1399C8DD 74A3B585 EB31D8A2 6DAFE068


      output_block is
                          1686FFCF 9F358BE7 4452E647 BA156AAB


      temp is
                          1686FFCF 9F358BE7 4452E647 BA156AAB


    ------------
```

```
      While loop

      Key is
                           58E3FECD FE7B3666 3E76175C A8EA4B55

      V is
                           1399C8DD 74A3B585 EB31D8A2 6DAFE069

      output_block is
                           05135797 117FD1AB 317D318C 660E3D18

      temp is
                                                 1686FFCF 9F358BE7
        4452E647 BA156AAB 05135797 117FD1AB 317D318C 660E3D18

    temp XOR provided_data is
                                                 96077D4C 1BB00D60
       CCDB6CCC 3698E424 9582C504 85EA473C A9E4AB17 FA93A387

    Key is
                           96077D4C 1BB00D60 CCDB6CCC 3698E424

    V is
                           9582C504 85EA473C A9E4AB17 FA93A387

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
```

```
                                          00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


------------

  While loop

  Key is
                      96077D4C 1BB00D60 CCDB6CCC 3698E424


  V is
                      9582C504 85EA473C A9E4AB17 FA93A38A


  output_block is
                      D816A3CD B36E3A01 AF11BA58 76F49516


  temp is
                      D816A3CD B36E3A01 AF11BA58 76F49516


------------

  While loop

  Key is
                      96077D4C 1BB00D60 CCDB6CCC 3698E424


  V is
                      9582C504 85EA473C A9E4AB17 FA93A38B


  output_block is
                      8017C913 B23F851E 24425356 1474D074


  temp is
                                          D816A3CD B36E3A01
    AF11BA58 76F49516 8017C913 B23F851E 24425356 1474D074


temp XOR provided_data is
```

```
                                                D816A3CD B36E3A01
        AF11BA58 76F49516 8017C913 B23F851E 24425356 1474D074


    Key is
                           D816A3CD B36E3A01 AF11BA58 76F49516


    V is
                           8017C913 B23F851E 24425356 1474D074


rnd_val is
                                                89935DB7 5FC4ED67
        7F166E49 CAEDB105 48BB5B5E 7F8B32D6 44DFD3B7 CCDE3B60


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    additional_input is  <empty>

---------------------------

  Update

    provided_data is
```

```
                                          C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


------------

  While loop

  Key is
                     D816A3CD B36E3A01 AF11BA58 76F49516


  V is
                     8017C913 B23F851E 24425356 1474D075


  output_block is
                     C1660382 61B1D710 80C0CD6A 769A810B


  temp is
                     C1660382 61B1D710 80C0CD6A 769A810B


------------

  While loop

  Key is
                     D816A3CD B36E3A01 AF11BA58 76F49516


  V is
                     8017C913 B23F851E 24425356 1474D076


  output_block is
                     5ADEAAA6 72E03BDC BFF96166 14BBBEDC


  temp is
                                          C1660382 61B1D710
    80C0CD6A 769A810B 5ADEAAA6 72E03BDC BFF96166 14BBBEDC


temp XOR provided_data is
```

```
                                                  01A7C141 A57411D7
        480907A1 BA574FC4 8A0F7875 A635ED0B 6720BBBD C8666003


    Key is
                          01A7C141 A57411D7 480907A1 BA574FC4


    V is
                          8A0F7875 A635ED0B 6720BBBD C8666003


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                                                  00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                          01A7C141 A57411D7 480907A1 BA574FC4


      V is
                          8A0F7875 A635ED0B 6720BBBD C8666006


      output_block is
                          00B84831 ABFBE616 8FE6D0BD 4784ED4E


      temp is
```

```
                        00B84831 ABFBE616 8FE6D0BD 4784ED4E


    ------------

      While loop

      Key is
                        01A7C141 A57411D7 480907A1 BA574FC4


      V is
                        8A0F7875 A635ED0B 6720BBBD C8666007


      output_block is
                        948ABF15 132F7F78 1ED83609 0ACA9F6E


      temp is
                                            00B84831 ABFBE616
        8FE6D0BD 4784ED4E 948ABF15 132F7F78 1ED83609 0ACA9F6E


    temp XOR provided_data is
                                            00B84831 ABFBE616
        8FE6D0BD 4784ED4E 948ABF15 132F7F78 1ED83609 0ACA9F6E


    Key is
                        00B84831 ABFBE616 8FE6D0BD 4784ED4E


    V is
                        948ABF15 132F7F78 1ED83609 0ACA9F6E


rnd_val is
                                            B5795CE0 AFADFBA6
        0C337129 8D105500 531853E4 65548878 9847E053 147D5C15


################################################################

CTR_DRBG
```

```
    Requested Security Strength = 128

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    AdditionalInput2 =
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

--------------------------
```

```
Update

  provided_data is
                                          00010203 04050607
      08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


  ------------

    While loop

    Key is
                        00000000 00000000 00000000 00000000


    V is
                        00000000 00000000 00000000 00000001


    output_block is
                        58E2FCCE FA7E3061 367F1D57 A4E7455A


    temp is
                        58E2FCCE FA7E3061 367F1D57 A4E7455A


  ------------

    While loop

    Key is
                        00000000 00000000 00000000 00000000


    V is
                        00000000 00000000 00000000 00000002


    output_block is
                        0388DACE 60B6A392 F328C2B9 71B2FE78


    temp is
                                          58E2FCCE FA7E3061
```

```
        367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78


    temp XOR provided_data is
                                            58E3FECD FE7B3666
        3E76175C A8EA4B55 1399C8DD 74A3B585 EB31D8A2 6DAFE067


    Key is
                          58E3FECD FE7B3666 3E76175C A8EA4B55


    V is
                          1399C8DD 74A3B585 EB31D8A2 6DAFE067


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                            60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


Generate FAILED: Reseed is required
*************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                            80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    additional_input is
                                            60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
```

```
---------------------------

  Update

    provided_data is
                                                E0E0E0E0 E0E0E0E0
        E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0


    ------------

      While loop

      Key is
                          58E3FECD FE7B3666 3E76175C A8EA4B55


      V is
                          1399C8DD 74A3B585 EB31D8A2 6DAFE068


      output_block is
                          1686FFCF 9F358BE7 4452E647 BA156AAB


      temp is
                          1686FFCF 9F358BE7 4452E647 BA156AAB


    ------------

      While loop

      Key is
                          58E3FECD FE7B3666 3E76175C A8EA4B55


      V is
                          1399C8DD 74A3B585 EB31D8A2 6DAFE069


      output_block is
                          05135797 117FD1AB 317D318C 660E3D18


      temp is
```

```
                                                1686FFCF 9F358BE7
        4452E647 BA156AAB 05135797 117FD1AB 317D318C 660E3D18


    temp XOR provided_data is
                                                F6661F2F 7FD56B07
        A4B206A7 5AF58A4B E5F3B777 F19F314B D19DD16C 86EEDDF8


    Key is
                          F6661F2F 7FD56B07 A4B206A7 5AF58A4B


    V is
                          E5F3B777 F19F314B D19DD16C 86EEDDF8


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                          F6661F2F 7FD56B07 A4B206A7 5AF58A4B


      V is
                          E5F3B777 F19F314B D19DD16C 86EEDDFB
```

```
      output_block is
                          00D9D257 6D398E76 0057DAD3 6F462A0D

      temp is
                          00D9D257 6D398E76 0057DAD3 6F462A0D

    ------------

      While loop

      Key is
                          F6661F2F 7FD56B07 A4B206A7 5AF58A4B

      V is
                          E5F3B777 F19F314B D19DD16C 86EEDDFC

      output_block is
                          A3C3633D 964C6D0B 148D435C 7EF870A4

      temp is
                                               00D9D257 6D398E76
        0057DAD3 6F462A0D A3C3633D 964C6D0B 148D435C 7EF870A4

    temp XOR provided_data is
                                               00D9D257 6D398E76
        0057DAD3 6F462A0D A3C3633D 964C6D0B 148D435C 7EF870A4

    Key is
                          00D9D257 6D398E76 0057DAD3 6F462A0D

    V is
                          A3C3633D 964C6D0B 148D435C 7EF870A4

rnd_val is
                                               7A95EE54 39D83828
        95B53929 3789D040 BAAF9751 C73B1F0E 66CE39AA 0E4DE0FC
```

```
------------------------------------------------------------

Second call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                              A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                              C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    additional_input is
                                              A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


---------------------------

  Update

    provided_data is
                                              60606060 60606060
        60606060 60606060 60606060 60606060 60606060 60606060


    ------------

      While loop

      Key is
                           00D9D257 6D398E76 0057DAD3 6F462A0D
```

```
  V is
                      A3C3633D 964C6D0B 148D435C 7EF870A5

  output_block is
                      30A7280C 9DF010F7 C2876DA1 A7341E79

  temp is
                      30A7280C 9DF010F7 C2876DA1 A7341E79

------------

  While loop

  Key is
                      00D9D257 6D398E76 0057DAD3 6F462A0D

  V is
                      A3C3633D 964C6D0B 148D435C 7EF870A6

  output_block is
                      49FCC388 3DF830EC 6667AB5D FB849096

  temp is
                                        30A7280C 9DF010F7
    C2876DA1 A7341E79 49FCC388 3DF830EC 6667AB5D FB849096

temp XOR provided_data is
                                        50C7486C FD907097
    A2E70DC1 C7547E19 299CA3E8 5D98508C 0607CB3D 9BE4F0F6

Key is
                      50C7486C FD907097 A2E70DC1 C7547E19

V is
                      299CA3E8 5D98508C 0607CB3D 9BE4F0F6
```

```
****************************************************************
CTR_DRBG_Generate
  requested_number_of_bits = 256
    additional_input is  <empty>
----------------------------
  Update
    provided_data is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000

    ------------
      While loop
      Key is
                          50C7486C FD907097 A2E70DC1 C7547E19

      V is
                          299CA3E8 5D98508C 0607CB3D 9BE4F0F9

      output_block is
                          9FD6CA5D C8B39E75 8ADCB5CF CB4012D1

      temp is
                          9FD6CA5D C8B39E75 8ADCB5CF CB4012D1

    ------------
      While loop
      Key is
                          50C7486C FD907097 A2E70DC1 C7547E19
```

```
      V is
                          299CA3E8 5D98508C 0607CB3D 9BE4F0FA


      output_block is
                          81E4EA7A AFA955AA DB506F01 E3F27EAE


      temp is
                                                 9FD6CA5D C8B39E75
        8ADCB5CF CB4012D1 81E4EA7A AFA955AA DB506F01 E3F27EAE


    temp XOR provided_data is
                                                 9FD6CA5D C8B39E75
        8ADCB5CF CB4012D1 81E4EA7A AFA955AA DB506F01 E3F27EAE


    Key is
                          9FD6CA5D C8B39E75 8ADCB5CF CB4012D1


    V is
                          81E4EA7A AFA955AA DB506F01 E3F27EAE


rnd_val is
                                                 598F7694 08F56946
        EB720776 1263BABC 964F306B E99BBA5A E329E01C FA100EC2


################################################################

CTR_DRBG

    Requested Security Strength = 128

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                                 80818283 84858687
```

```
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    PersonalizationString =
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    AdditionalInput = <empty>

###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    personal_str is
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Update

    provided_data is
                                                40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


    ------------

      While loop
```

```
  Key is
                      00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000001

  output_block is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A

  temp is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A

------------

  While loop

  Key is
                      00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000002

  output_block is
                      0388DACE 60B6A392 F328C2B9 71B2FE78

  temp is
                                        58E2FCCE FA7E3061
    367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78

temp XOR provided_data is
                                        18A2BC8E BA3E7021
    763F5D17 E4A7051A 43C89A8E 20F6E3D2 B36882F9 31F2BE38

Key is
                      18A2BC8E BA3E7021 763F5D17 E4A7051A
```

```
    V is
                          43C89A8E 20F6E3D2 B36882F9 31F2BE38


---------------------------------------------------------------

First call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    ------------

      While loop

      Key is
                          18A2BC8E BA3E7021 763F5D17 E4A7051A


      V is
```

```
                        43C89A8E 20F6E3D2 B36882F9 31F2BE39

      output_block is
                        FA1DF743 5039C649 3B14D8C8 F9715BA5

      temp is
                        FA1DF743 5039C649 3B14D8C8 F9715BA5

    ------------

      While loop

      Key is
                        18A2BC8E BA3E7021 763F5D17 E4A7051A

      V is
                        43C89A8E 20F6E3D2 B36882F9 31F2BE3A

      output_block is
                        CE6EE312 20EEDEE3 65A4B6B7 2FD68554

      temp is
                                            FA1DF743 5039C649
        3B14D8C8 F9715BA5 CE6EE312 20EEDEE3 65A4B6B7 2FD68554

    temp XOR provided_data is
                                            7A9C75C0 D4BC40CE
        B39D5243 75FCD52A 5EFF7181 B47B4874 FD3D2C2C B34B1BCB

    Key is
                        7A9C75C0 D4BC40CE B39D5243 75FCD52A

    V is
                        5EFF7181 B47B4874 FD3D2C2C B34B1BCB

**************************************************************
```

```
CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                          7A9C75C0 D4BC40CE B39D5243 75FCD52A


      V is
                          5EFF7181 B47B4874 FD3D2C2C B34B1BCE


      output_block is
                          0B983A61 CA075354 1C9BC0C6 6AB5CE59


      temp is
                          0B983A61 CA075354 1C9BC0C6 6AB5CE59


    ------------

      While loop

      Key is
                          7A9C75C0 D4BC40CE B39D5243 75FCD52A


      V is
                          5EFF7181 B47B4874 FD3D2C2C B34B1BCF
```

```
      output_block is
                           A6E4E62F 7A9B71B8 194B3BC2 475AF1B1


      temp is
                                             0B983A61 CA075354
        1C9BC0C6 6AB5CE59 A6E4E62F 7A9B71B8 194B3BC2 475AF1B1


    temp XOR provided_data is
                                             0B983A61 CA075354
        1C9BC0C6 6AB5CE59 A6E4E62F 7A9B71B8 194B3BC2 475AF1B1


    Key is
                           0B983A61 CA075354 1C9BC0C6 6AB5CE59


    V is
                           A6E4E62F 7A9B71B8 194B3BC2 475AF1B1


rnd_val is
                                             C7C914C1 AF21B9D0
        0002C9F2 11A9AB4A 3E7C3871 2779687A 03DFFD32 645CB4CD


-------------------------------------------------------------

Second call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

CTR_DRBG_Reseed
```

```
    entropy_input is
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    ------------

      While loop

      Key is
                          0B983A61 CA075354 1C9BC0C6 6AB5CE59


      V is
                          A6E4E62F 7A9B71B8 194B3BC2 475AF1B2


      output_block is
                          457D7BE0 6EC8D5F1 B712CFD2 5F1544F1


      temp is
                          457D7BE0 6EC8D5F1 B712CFD2 5F1544F1


    ------------

      While loop

      Key is
                          0B983A61 CA075354 1C9BC0C6 6AB5CE59


      V is
                          A6E4E62F 7A9B71B8 194B3BC2 475AF1B3
```

```
      output_block is
                           F930608A 207776B5 A2B87C93 A513D3FC


      temp is
                                                 457D7BE0 6EC8D5F1
        B712CFD2 5F1544F1 F930608A 207776B5 A2B87C93 A513D3FC


    temp XOR provided_data is
                                                 85BCB923 AA0D1336
        7FDB0519 93D88A3E 29E1B259 F4A2A062 7A61A648 79CE0D23


    Key is
                           85BCB923 AA0D1336 7FDB0519 93D88A3E


    V is
                           29E1B259 F4A2A062 7A61A648 79CE0D23


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                                                 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
```

```
                    85BCB923 AA0D1336 7FDB0519 93D88A3E

  V is
                    29E1B259 F4A2A062 7A61A648 79CE0D26

  output_block is
                    21F5F987 37C498DE F25C78C3 50447DAC

  temp is
                    21F5F987 37C498DE F25C78C3 50447DAC

------------

  While loop

  Key is
                    85BCB923 AA0D1336 7FDB0519 93D88A3E

  V is
                    29E1B259 F4A2A062 7A61A648 79CE0D27

  output_block is
                    53D4BFA2 99CFBC0E 9D741ECA 610DAE5F

  temp is
                                      21F5F987 37C498DE
    F25C78C3 50447DAC 53D4BFA2 99CFBC0E 9D741ECA 610DAE5F

temp XOR provided_data is
                                      21F5F987 37C498DE
    F25C78C3 50447DAC 53D4BFA2 99CFBC0E 9D741ECA 610DAE5F

Key is
                    21F5F987 37C498DE F25C78C3 50447DAC

V is
```

```
                          53D4BFA2 99CFBC0E 9D741ECA 610DAE5F


rnd_val is
                                                35AF6092 8E3ED896
        20DE692D 9660289A 2D321CBC 0F1E0A58 724B393B 7735D445


###############################################################

CTR_DRBG

    Requested Security Strength = 128

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    PersonalizationString =
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    AdditionalInput1 =
                                                60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    AdditionalInput2 =
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


###############################################################
```

```
***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    personal_str is
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Update

    provided_data is
                                                40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


    ------------

      While loop

      Key is
                          00000000 00000000 00000000 00000000


      V is
                          00000000 00000000 00000000 00000001


      output_block is
                          58E2FCCE FA7E3061 367F1D57 A4E7455A


      temp is
                          58E2FCCE FA7E3061 367F1D57 A4E7455A
```

```
    ------------

      While loop

      Key is
                           00000000 00000000 00000000 00000000

      V is
                           00000000 00000000 00000000 00000002

      output_block is
                           0388DACE 60B6A392 F328C2B9 71B2FE78

      temp is
                                                 58E2FCCE FA7E3061
        367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78

    temp XOR provided_data is
                                                 18A2BC8E BA3E7021
        763F5D17 E4A7051A 43C89A8E 20F6E3D2 B36882F9 31F2BE38

    Key is
                           18A2BC8E BA3E7021 763F5D17 E4A7051A

    V is
                           43C89A8E 20F6E3D2 B36882F9 31F2BE38


---------------------------------------------------------------

First call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                                 60616263 64656667
```

```
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                               80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    additional_input is
                                               60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


---------------------------

  Update

    provided_data is
                                               E0E0E0E0 E0E0E0E0
        E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0


    ------------

      While loop

      Key is
                          18A2BC8E BA3E7021 763F5D17 E4A7051A


      V is
                          43C89A8E 20F6E3D2 B36882F9 31F2BE39


      output_block is
                          FA1DF743 5039C649 3B14D8C8 F9715BA5


      temp is
                          FA1DF743 5039C649 3B14D8C8 F9715BA5
```

```
    ------------

      While loop

      Key is
                           18A2BC8E BA3E7021 763F5D17 E4A7051A


      V is
                           43C89A8E 20F6E3D2 B36882F9 31F2BE3A


      output_block is
                           CE6EE312 20EEDEE3 65A4B6B7 2FD68554


      temp is
                                             FA1DF743 5039C649
        3B14D8C8 F9715BA5 CE6EE312 20EEDEE3 65A4B6B7 2FD68554


    temp XOR provided_data is
                                             1AFD17A3 B0D926A9
       DBF43828 1991BB45 2E8E03F2 C00E3E03 85445657 CF3665B4


    Key is
                           1AFD17A3 B0D926A9 DBF43828 1991BB45


    V is
                           2E8E03F2 C00E3E03 85445657 CF3665B4


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update
```

```
provided_data is
                                                00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


------------

  While loop

  Key is
                      1AFD17A3 B0D926A9 DBF43828 1991BB45


  V is
                      2E8E03F2 C00E3E03 85445657 CF3665B7


  output_block is
                      47B3433E 78449967 B66DE6DD 5212883D


  temp is
                      47B3433E 78449967 B66DE6DD 5212883D


------------

  While loop

  Key is
                      1AFD17A3 B0D926A9 DBF43828 1991BB45


  V is
                      2E8E03F2 C00E3E03 85445657 CF3665B8


  output_block is
                      561936F4 ADBD65A6 43E50E2F D753F120


  temp is
                                                47B3433E 78449967
    B66DE6DD 5212883D 561936F4 ADBD65A6 43E50E2F D753F120
```

```
    temp XOR provided_data is
                                            47B3433E 78449967
        B66DE6DD 5212883D 561936F4 ADBD65A6 43E50E2F D753F120


    Key is
                         47B3433E 78449967 B66DE6DD 5212883D


    V is
                         561936F4 ADBD65A6 43E50E2F D753F120


rnd_val is
                                            DCC71C5D 851228E5
        EEF37E18 6AECBDAE A081040E 0EC04DBE 3328B5AB E3249D2D


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


Generate FAILED: Reseed is required
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                            C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    additional_input is
                                            A0A1A2A3 A4A5A6A7
```

```
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


---------------------------

  Update

    provided_data is
                                                 60606060 60606060
        60606060 60606060 60606060 60606060 60606060 60606060


    ------------

      While loop

      Key is
                          47B3433E 78449967 B66DE6DD 5212883D


      V is
                          561936F4 ADBD65A6 43E50E2F D753F121


      output_block is
                          605C7D97 F28AAD7B E85763BC 91432D98


      temp is
                          605C7D97 F28AAD7B E85763BC 91432D98


    ------------

      While loop

      Key is
                          47B3433E 78449967 B66DE6DD 5212883D


      V is
                          561936F4 ADBD65A6 43E50E2F D753F122


      output_block is
                          05E5B36D AD934227 DD99A526 76689DD2
```

```
      temp is
                                                605C7D97 F28AAD7B
        E85763BC 91432D98 05E5B36D AD934227 DD99A526 76689DD2


    temp XOR provided_data is
                                                003C1DF7 92EACD1B
        883703DC F1234DF8 6585D30D CDF32247 BDF9C546 1608FDB2


    Key is
                          003C1DF7 92EACD1B 883703DC F1234DF8


    V is
                          6585D30D CDF32247 BDF9C546 1608FDB2

****************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                          003C1DF7 92EACD1B 883703DC F1234DF8


      V is
```

```
                        6585D30D CDF32247 BDF9C546 1608FDB5

      output_block is
                        2CECDB8B 151A48A7 6473908D F85FFFB2

      temp is
                        2CECDB8B 151A48A7 6473908D F85FFFB2

    ------------

      While loop

      Key is
                        003C1DF7 92EACD1B 883703DC F1234DF8

      V is
                        6585D30D CDF32247 BDF9C546 1608FDB6

      output_block is
                        3CD321D9 6DA4981F AEFC26D2 B9DEC7FC

      temp is
                                            2CECDB8B 151A48A7
        6473908D F85FFFB2 3CD321D9 6DA4981F AEFC26D2 B9DEC7FC

    temp XOR provided_data is
                                            2CECDB8B 151A48A7
        6473908D F85FFFB2 3CD321D9 6DA4981F AEFC26D2 B9DEC7FC

    Key is
                        2CECDB8B 151A48A7 6473908D F85FFFB2

    V is
                        3CD321D9 6DA4981F AEFC26D2 B9DEC7FC

rnd_val is
```

```
                                                15800389 9C6FCB09
        97B58522 B0AE5071 97CFE7B7 1B2D4CF0 F2E3334D 00491C12


###############################################################

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

--------------------------
```

```
Update

  provided_data is
                         00010203 04050607 08090A0B 0C0D0E0F
      10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


  ------------

    While loop

    Key is
      00000000 00000000 00000000 00000000 00000000 00000000


    V is
                         00000000 00000000 00000000 00000001


    output_block is
                         CD33B28A C773F74B A00ED1F3 12572435


    temp is
                         CD33B28A C773F74B A00ED1F3 12572435


  ------------

    While loop

    Key is
      00000000 00000000 00000000 00000000 00000000 00000000


    V is
                         00000000 00000000 00000000 00000002


    output_block is
                         98E7247C 07F0FE41 1C267E43 84B0F600


    temp is
                                            CD33B28A C773F74B
```

```
        A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


    ------------

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000003


      output_block is
                           2A3493E6 6235EE67 DEECCD2F 3B393BD8


      temp is
        CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
        1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8


    temp XOR provided_data is
                           CD32B089 C376F14C A807DBF8 1E5A2A3A
        88F6366F 13E5E856 043F6458 98ADE81F 0A15B1C5 4610C840


    Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


    V is
                           043F6458 98ADE81F 0A15B1C5 4610C840


------------------------------------------------------------

First call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256
```

```
    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


      V is
                          043F6458 98ADE81F 0A15B1C5 4610C843


      output_block is
                          685C8679 5A13E060 4CA155CA 4D9BF978


      temp is
                          685C8679 5A13E060 4CA155CA 4D9BF978


    ------------

      While loop

      Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


      V is
                          043F6458 98ADE81F 0A15B1C5 4610C844


      output_block is
                          2D689829 7F86953C A13FD9F3 D499D39C
```

```
      temp is
                                              685C8679 5A13E060
        4CA155CA 4D9BF978 2D689829 7F86953C A13FD9F3 D499D39C


    ------------

      While loop

      Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


      V is
                           043F6458 98ADE81F 0A15B1C5 4610C845


      output_block is
                           04C3FDEF A12684E0 F4DE317D DCA8DA26


      temp is
        685C8679 5A13E060 4CA155CA 4D9BF978 2D689829 7F86953C
        A13FD9F3 D499D39C 04C3FDEF A12684E0 F4DE317D DCA8DA26


    temp XOR provided_data is
                           685C8679 5A13E060 4CA155CA 4D9BF978
        2D689829 7F86953C A13FD9F3 D499D39C 04C3FDEF A12684E0


    Key is
        685C8679 5A13E060 4CA155CA 4D9BF978 2D689829 7F86953C


    V is
                           A13FD9F3 D499D39C 04C3FDEF A12684E0


rnd_val is
                                              01E0793E 6C7464FA
        FE1F6CF9 B7466A8A C4841737 9CBAA104 13DBCD98 E1977019
```

```
-------------------------------------------------------------

Second call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
        685C8679 5A13E060 4CA155CA 4D9BF978 2D689829 7F86953C


      V is
                          A13FD9F3 D499D39C 04C3FDEF A12684E3


      output_block is
                          8190E9BB FDFDDE79 E5264E86 6871234C


      temp is
                          8190E9BB FDFDDE79 E5264E86 6871234C


    ------------

      While loop

      Key is
```

```
    685C8679 5A13E060 4CA155CA 4D9BF978 2D689829 7F86953C


  V is
                     A13FD9F3 D499D39C 04C3FDEF A12684E4


  output_block is
                     3CE8504E 14EF7C8A F4DE516E 7DB043D1


  temp is
                                          8190E9BB FDFDDE79
    E5264E86 6871234C 3CE8504E 14EF7C8A F4DE516E 7DB043D1


------------

  While loop

  Key is
    685C8679 5A13E060 4CA155CA 4D9BF978 2D689829 7F86953C


  V is
                     A13FD9F3 D499D39C 04C3FDEF A12684E5


  output_block is
                     9A487B3A F1909DC3 169D374E C0B0D991


  temp is
    8190E9BB FDFDDE79 E5264E86 6871234C 3CE8504E 14EF7C8A
    F4DE516E 7DB043D1 9A487B3A F1909DC3 169D374E C0B0D991


temp XOR provided_data is
                     8190E9BB FDFDDE79 E5264E86 6871234C
    3CE8504E 14EF7C8A F4DE516E 7DB043D1 9A487B3A F1909DC3


Key is
    8190E9BB FDFDDE79 E5264E86 6871234C 3CE8504E 14EF7C8A
```

```
    V is
                          F4DE516E 7DB043D1 9A487B3A F1909DC3


rnd_val is
                                               88CE7B6C 16365EEA
        6FEE02BF BAE2DF4D 93AB03B9 CF8807E5 BEAD31D4 FB721DC9


##############################################################

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    PersonalizationString = <empty>

    AdditionalInput1 =
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


    AdditionalInput2 =
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


##############################################################

**************************************************************
```

```
CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                            00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Update

    provided_data is
                            00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    ------------

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                            00000000 00000000 00000000 00000001


      output_block is
                            CD33B28A C773F74B A00ED1F3 12572435


      temp is
                            CD33B28A C773F74B A00ED1F3 12572435


    ------------

      While loop

      Key is
```

```
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000002


  output_block is
                      98E7247C 07F0FE41 1C267E43 84B0F600


  temp is
                                        CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000003


  output_block is
                      2A3493E6 6235EE67 DEECCD2F 3B393BD8


  temp is
    CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
    1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8


temp XOR provided_data is
                      CD32B089 C376F14C A807DBF8 1E5A2A3A
    88F6366F 13E5E856 043F6458 98ADE81F 0A15B1C5 4610C840


Key is
    CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856
```

```
    V is
                          043F6458 98ADE81F 0A15B1C5 4610C840


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


    ------------

      While loop

      Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


      V is
                          043F6458 98ADE81F 0A15B1C5 4610C841


      output_block is
                          01E0793E 6C7464FA FE1F6CF9 B7466A8A


      temp is
```

```
                    01E0793E 6C7464FA FE1F6CF9 B7466A8A


------------

  While loop

  Key is
    CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


  V is
                    043F6458 98ADE81F 0A15B1C5 4610C842


  output_block is
                    C4841737 9CBAA104 13DBCD98 E1977019


  temp is
                                       01E0793E 6C7464FA
    FE1F6CF9 B7466A8A C4841737 9CBAA104 13DBCD98 E1977019


------------

  While loop

  Key is
    CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


  V is
                    043F6458 98ADE81F 0A15B1C5 4610C843


  output_block is
                    685C8679 5A13E060 4CA155CA 4D9BF978


  temp is
    01E0793E 6C7464FA FE1F6CF9 B7466A8A C4841737 9CBAA104
    13DBCD98 E1977019 685C8679 5A13E060 4CA155CA 4D9BF978


temp XOR provided_data is
```

```
                        61811B5D 0811029D 96760692 DB2B04E5
        B4F56544 E8CFD773 6BA2B7E3 9DEA0E66 E8DD04FA DE9666E7


    Key is
        61811B5D 0811029D 96760692 DB2B04E5 B4F56544 E8CFD773


    V is
                        6BA2B7E3 9DEA0E66 E8DD04FA DE9666E7


---------------------------

  Update

    provided_data is
                        60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


    ------------

      While loop

      Key is
        61811B5D 0811029D 96760692 DB2B04E5 B4F56544 E8CFD773


      V is
                        6BA2B7E3 9DEA0E66 E8DD04FA DE9666EA


      output_block is
                        C6FB2B83 812E5D99 7087CA64 E19A1ACD


      temp is
                        C6FB2B83 812E5D99 7087CA64 E19A1ACD


    ------------

      While loop

      Key is
```

```
    61811B5D 0811029D 96760692 DB2B04E5 B4F56544 E8CFD773


  V is
                     6BA2B7E3 9DEA0E66 E8DD04FA DE9666EB


  output_block is
                     48AAF49B 9E8359A3 35B3B157 05F7C99E


  temp is
                                       C6FB2B83 812E5D99
    7087CA64 E19A1ACD 48AAF49B 9E8359A3 35B3B157 05F7C99E


------------

  While loop

  Key is
    61811B5D 0811029D 96760692 DB2B04E5 B4F56544 E8CFD773


  V is
                     6BA2B7E3 9DEA0E66 E8DD04FA DE9666EC


  output_block is
                     C7F5365C 0BFF94EA 87BE9358 FDC201BA


  temp is
    C6FB2B83 812E5D99 7087CA64 E19A1ACD 48AAF49B 9E8359A3
    35B3B157 05F7C99E C7F5365C 0BFF94EA 87BE9358 FDC201BA


temp XOR provided_data is
                     A69A49E0 E54B3BFE 18EEA00F 8DF774A2
    38DB86E8 EAF62FD4 4DCACB2C 798AB7E1 4774B4DF 8F7A126D


Key is
    A69A49E0 E54B3BFE 18EEA00F 8DF774A2 38DB86E8 EAF62FD4
```

```
    V is
                          4DCACB2C 798AB7E1 4774B4DF 8F7A126D


rnd_val is
                                               3A298716 7FF43CD7
        94A9778F 3932A2E9 AA7C9518 24C82924 C7324560 4B0BEFA5


------------------------------------------------------------

Second call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


    ------------

      While loop

      Key is
        A69A49E0 E54B3BFE 18EEA00F 8DF774A2 38DB86E8 EAF62FD4


      V is
                          4DCACB2C 798AB7E1 4774B4DF 8F7A126E
```

```
  output_block is
                      433A5A5C ECFD33CD FA67D7D6 5607CD48

  temp is
                      433A5A5C ECFD33CD FA67D7D6 5607CD48

------------

  While loop

  Key is
    A69A49E0 E54B3BFE 18EEA00F 8DF774A2 38DB86E8 EAF62FD4

  V is
                      4DCACB2C 798AB7E1 4774B4DF 8F7A126F

  output_block is
                      BECC799D AAF47F22 CFD9EEF1 AD8B178D

  temp is
                                        433A5A5C ECFD33CD
    FA67D7D6 5607CD48 BECC799D AAF47F22 CFD9EEF1 AD8B178D

------------

  While loop

  Key is
    A69A49E0 E54B3BFE 18EEA00F 8DF774A2 38DB86E8 EAF62FD4

  V is
                      4DCACB2C 798AB7E1 4774B4DF 8F7A1270

  output_block is
                      2D368884 3376F6BD D14EE304 9FA8BFEB

  temp is
```

```
        433A5A5C ECFD33CD FA67D7D6 5607CD48 BECC799D AAF47F22
        CFD9EEF1 AD8B178D 2D368884 3376F6BD D14EE304 9FA8BFEB


    temp XOR provided_data is
                          E39BF8FF 4858956A 52CE7D7D FAAA63E7
        0E7DCB2E 1E41C995 7760544A 1136A932 EDF74A47 F7B3307A


    Key is
        E39BF8FF 4858956A 52CE7D7D FAAA63E7 0E7DCB2E 1E41C995


    V is
                          7760544A 1136A932 EDF74A47 F7B3307A


----------------------------

  Update

    provided_data is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


    ------------

      While loop

      Key is
        E39BF8FF 4858956A 52CE7D7D FAAA63E7 0E7DCB2E 1E41C995


      V is
                          7760544A 1136A932 EDF74A47 F7B3307D


      output_block is
                          76216733 654CD5AA 4F1756AB 4683568B


      temp is
                          76216733 654CD5AA 4F1756AB 4683568B
```

```
------------

  While loop

  Key is
    E39BF8FF 4858956A 52CE7D7D FAAA63E7 0E7DCB2E 1E41C995


  V is
                      7760544A 1136A932 EDF74A47 F7B3307E


  output_block is
                      0D8A7249 375AA6BE 0EDC3CBD 26FF8E9C


  temp is
                                           76216733 654CD5AA
    4F1756AB 4683568B 0D8A7249 375AA6BE 0EDC3CBD 26FF8E9C


------------

  While loop

  Key is
    E39BF8FF 4858956A 52CE7D7D FAAA63E7 0E7DCB2E 1E41C995


  V is
                      7760544A 1136A932 EDF74A47 F7B3307F


  output_block is
                      9413F800 3CC5FF4D 852CA338 AB836A1C


  temp is
    76216733 654CD5AA 4F1756AB 4683568B 0D8A7249 375AA6BE
    0EDC3CBD 26FF8E9C 9413F800 3CC5FF4D 852CA338 AB836A1C


temp XOR provided_data is
                      D680C590 C1E9730D E7BEFC00 EA2EF824
    BD3BC0FA 83EF1009 B6658606 9A423023 54D23AC3 F800398A
```

```
    Key is
        D680C590 C1E9730D E7BEFC00 EA2EF824 BD3BC0FA 83EF1009


    V is
                            B6658606 9A423023 54D23AC3 F800398A


rnd_val is
                                                A963857B 976F18FD
        1F1B3301 DA08E8E8 4694AAFB 55EA2B10 196BEE84 77570853


###############################################################

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                            80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                            C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    PersonalizationString =
                            40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    AdditionalInput = <empty>

###############################################################

***************************************************************
```

```
CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                           00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    personal_str is
                           40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Update

    provided_data is
                           40404040 40404040 40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


    ------------

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001


      output_block is
                           CD33B28A C773F74B A00ED1F3 12572435


      temp is
                           CD33B28A C773F74B A00ED1F3 12572435


    ------------
```

```
  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                       00000000 00000000 00000000 00000002


  output_block is
                       98E7247C 07F0FE41 1C267E43 84B0F600


  temp is
                                         CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                       00000000 00000000 00000000 00000003


  output_block is
                       2A3493E6 6235EE67 DEECCD2F 3B393BD8


  temp is
    CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
    1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8


temp XOR provided_data is
                       8D73F2CA 8733B70B E04E91B3 52176475
    D8A7643C 47B0BE01 5C663E03 C4F0B640 6A74D3A6 2275AE27


Key is
```

```
        8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01

    V is
                        5C663E03 C4F0B640 6A74D3A6 2275AE27

-----------------------------------------------------------

First call to Generate

***********************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                        00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
        8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


      V is
                        5C663E03 C4F0B640 6A74D3A6 2275AE2A


      output_block is
                        2D882249 1114B01B 2208E492 F0F35C54


      temp is
                        2D882249 1114B01B 2208E492 F0F35C54
```

```
------------

  While loop

  Key is
    8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


  V is
                       5C663E03 C4F0B640 6A74D3A6 2275AE2B


  output_block is
                       86555AB1 87E3784E 74F52A4A B2A563EE


  temp is
                                         2D882249 1114B01B
    2208E492 F0F35C54 86555AB1 87E3784E 74F52A4A B2A563EE


------------

  While loop

  Key is
    8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


  V is
                       5C663E03 C4F0B640 6A74D3A6 2275AE2C


  output_block is
                       005240DE 5857A85A 45E4B451 D42DAF2D


  temp is
    2D882249 1114B01B 2208E492 F0F35C54 86555AB1 87E3784E
    74F52A4A B2A563EE 005240DE 5857A85A 45E4B451 D42DAF2D


temp XOR provided_data is
                       2D882249 1114B01B 2208E492 F0F35C54
```

```
        86555AB1 87E3784E 74F52A4A B2A563EE 005240DE 5857A85A


    Key is
        2D882249 1114B01B 2208E492 F0F35C54 86555AB1 87E3784E


    V is
                         74F52A4A B2A563EE 005240DE 5857A85A


rnd_val is
                                           517150FF D52BD344
        DE78992B A224930C 98FC9FAC 541236E8 D199A476 B960B301


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                         00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
        2D882249 1114B01B 2208E492 F0F35C54 86555AB1 87E3784E


      V is
```

74F52A4A B2A563EE 005240DE 5857A85D

output_block is
7EEB7C54 20128FEA C6BA2019 E6BBBEFC

temp is
7EEB7C54 20128FEA C6BA2019 E6BBBEFC

While loop

Key is
2D882249 1114B01B 2208E492 F0F35C54 86555AB1 87E3784E

V is
74F52A4A B2A563EE 005240DE 5857A85E

output_block is
54E9AE9E 6DF3C90C E1D395C3 E87F03BD

temp is
7EEB7C54 20128FEA
C6BA2019 E6BBBEFC 54E9AE9E 6DF3C90C E1D395C3 E87F03BD

While loop

Key is
2D882249 1114B01B 2208E492 F0F35C54 86555AB1 87E3784E

V is
74F52A4A B2A563EE 005240DE 5857A85F

output_block is
000D5096 45D19E8E 40EE54D9 A2D151B4

```
      temp is
        7EEB7C54 20128FEA C6BA2019 E6BBBEFC 54E9AE9E 6DF3C90C
        E1D395C3 E87F03BD 000D5096 45D19E8E 40EE54D9 A2D151B4


    temp XOR provided_data is
                          7EEB7C54 20128FEA C6BA2019 E6BBBEFC
        54E9AE9E 6DF3C90C E1D395C3 E87F03BD 000D5096 45D19E8E


    Key is
        7EEB7C54 20128FEA C6BA2019 E6BBBEFC 54E9AE9E 6DF3C90C


    V is
                          E1D395C3 E87F03BD 000D5096 45D19E8E


rnd_val is
                                             1F46912D 4DEA17B8
        6500AA70 836A5076 24C090C5 C440EB07 D46A05AE 4822113D


################################################################

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7
```

```
    PersonalizationString =
                          40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    AdditionalInput1 =
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


    AdditionalInput2 =
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    personal_str is
                          40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Update

    provided_data is
                          40404040 40404040 40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


    ------------

      While loop
```

```
  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                       00000000 00000000 00000000 00000001


  output_block is
                       CD33B28A C773F74B A00ED1F3 12572435


  temp is
                       CD33B28A C773F74B A00ED1F3 12572435


------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                       00000000 00000000 00000000 00000002


  output_block is
                       98E7247C 07F0FE41 1C267E43 84B0F600


  temp is
                                         CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000
```

```
      V is
                          00000000 00000000 00000000 00000003


      output_block is
                          2A3493E6 6235EE67 DEECCD2F 3B393BD8


      temp is
        CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
        1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8


    temp XOR provided_data is
                          8D73F2CA 8733B70B E04E91B3 52176475
        D8A7643C 47B0BE01 5C663E03 C4F0B640 6A74D3A6 2275AE27


    Key is
        8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


    V is
                          5C663E03 C4F0B640 6A74D3A6 2275AE27


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


  additional_input <> NULL, process appropriately
---------------------------

  Update
```

```
provided_data is
                      60616263 64656667 68696A6B 6C6D6E6F
    70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


------------

  While loop

  Key is
    8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


  V is
                      5C663E03 C4F0B640 6A74D3A6 2275AE28


  output_block is
                      517150FF D52BD344 DE78992B A224930C


  temp is
                      517150FF D52BD344 DE78992B A224930C


------------

  While loop

  Key is
    8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


  V is
                      5C663E03 C4F0B640 6A74D3A6 2275AE29


  output_block is
                      98FC9FAC 541236E8 D199A476 B960B301


  temp is
                                        517150FF D52BD344
    DE78992B A224930C 98FC9FAC 541236E8 D199A476 B960B301
```

```
    ------------

      While loop

      Key is
        8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


      V is
                           5C663E03 C4F0B640 6A74D3A6 2275AE2A


      output_block is
                           2D882249 1114B01B 2208E492 F0F35C54


      temp is
        517150FF D52BD344 DE78992B A224930C 98FC9FAC 541236E8
        D199A476 B960B301 2D882249 1114B01B 2208E492 F0F35C54


    temp XOR provided_data is
                           3110329C B14EB523 B611F340 CE49FD63
        E88DEDDF 2067409F A9E0DE0D C51DCD7E AD09A0CA 9591369C


    Key is
        3110329C B14EB523 B611F340 CE49FD63 E88DEDDF 2067409F


    V is
                           A9E0DE0D C51DCD7E AD09A0CA 9591369C


---------------------------

  Update

    provided_data is
                           60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


    ------------

      While loop
```

```
  Key is
    3110329C B14EB523 B611F340 CE49FD63 E88DEDDF 2067409F


  V is
                      A9E0DE0D C51DCD7E AD09A0CA 9591369F


  output_block is
                      5DD0E3F8 4FBC38F3 B20AE469 CE505605


  temp is
                      5DD0E3F8 4FBC38F3 B20AE469 CE505605


------------

  While loop

  Key is
    3110329C B14EB523 B611F340 CE49FD63 E88DEDDF 2067409F


  V is
                      A9E0DE0D C51DCD7E AD09A0CA 959136A0


  output_block is
                      54EDA5FB 1641935C 6E667BDA 293E7ED9


  temp is
                                        5DD0E3F8 4FBC38F3
    B20AE469 CE505605 54EDA5FB 1641935C 6E667BDA 293E7ED9


------------

  While loop

  Key is
    3110329C B14EB523 B611F340 CE49FD63 E88DEDDF 2067409F
```

```
      V is
                          A9E0DE0D C51DCD7E AD09A0CA 959136A1


      output_block is
                          E7A75AA5 60343055 4D6FB178 58794471


      temp is
        5DD0E3F8 4FBC38F3 B20AE469 CE505605 54EDA5FB 1641935C
        6E667BDA 293E7ED9 E7A75AA5 60343055 4D6FB178 58794471


    temp XOR provided_data is
                          3DB1819B 2BD95E94 DA638E02 A23D386A
        249CD788 6234E52B 161F01A1 554300A6 6726D826 E4B1B6D2


    Key is
        3DB1819B 2BD95E94 DA638E02 A23D386A 249CD788 6234E52B


    V is
                          161F01A1 554300A6 6726D826 E4B1B6D2


rnd_val is
                                             ABB31FC6 61357CEB
        BCAE1E1C AEAA2E20 2F391044 9C5033B4 8FD3A23B DB7EA158


------------------------------------------------------------

Second call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7
```

```
  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


    ------------

      While loop

      Key is
        3DB1819B 2BD95E94 DA638E02 A23D386A 249CD788 6234E52B


      V is
                          161F01A1 554300A6 6726D826 E4B1B6D3


      output_block is
                          BF216E90 8D69EC04 9E25BAB5 738BA1B4


      temp is
                          BF216E90 8D69EC04 9E25BAB5 738BA1B4


    ------------

      While loop

      Key is
        3DB1819B 2BD95E94 DA638E02 A23D386A 249CD788 6234E52B


      V is
                          161F01A1 554300A6 6726D826 E4B1B6D4


      output_block is
                          830F8CC5 6B61D025 DE9BEC72 D8631655
```

```
      temp is
                                                BF216E90 8D69EC04
        9E25BAB5 738BA1B4 830F8CC5 6B61D025 DE9BEC72 D8631655


    ------------

      While loop

      Key is
        3DB1819B 2BD95E94 DA638E02 A23D386A 249CD788 6234E52B


      V is
                           161F01A1 554300A6 6726D826 E4B1B6D5


      output_block is
                           C7D7EA9B A10168F8 AAC66626 259B5C4F


      temp is
        BF216E90 8D69EC04 9E25BAB5 738BA1B4 830F8CC5 6B61D025
        DE9BEC72 D8631655 C7D7EA9B A10168F8 AAC66626 259B5C4F


    temp XOR provided_data is
                           1F80CC33 29CC4AA3 368C101E DF260F1B
        33BE3E76 DFD46692 662256C9 64DEA8EA 07162858 65C4AE3F


    Key is
        1F80CC33 29CC4AA3 368C101E DF260F1B 33BE3E76 DFD46692


    V is
                           662256C9 64DEA8EA 07162858 65C4AE3F


---------------------------

  Update

    provided_data is
                           A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7
```

```
------------

  While loop

  Key is
    1F80CC33 29CC4AA3 368C101E DF260F1B 33BE3E76 DFD46692


  V is
                       662256C9 64DEA8EA 07162858 65C4AE42


  output_block is
                       19F7F6A1 528CBEE6 3F9CBF4F 1AB3408F


  temp is
                       19F7F6A1 528CBEE6 3F9CBF4F 1AB3408F


------------

  While loop

  Key is
    1F80CC33 29CC4AA3 368C101E DF260F1B 33BE3E76 DFD46692


  V is
                       662256C9 64DEA8EA 07162858 65C4AE43


  output_block is
                       F239F9F4 A8AFC42D D4A50A9D 3DE4C243


  temp is
                                          19F7F6A1 528CBEE6
    3F9CBF4F 1AB3408F F239F9F4 A8AFC42D D4A50A9D 3DE4C243


------------

  While loop
```

```
      Key is
        1F80CC33 29CC4AA3 368C101E DF260F1B 33BE3E76 DFD46692


      V is
                           662256C9 64DEA8EA 07162858 65C4AE44


      output_block is
                           4B4E6879 44DCF4AB ACACB343 D6B9EB4D


      temp is
        19F7F6A1 528CBEE6 3F9CBF4F 1AB3408F F239F9F4 A8AFC42D
        D4A50A9D 3DE4C243 4B4E6879 44DCF4AB ACACB343 D6B9EB4D


    temp XOR provided_data is
                           B9565402 F6291841 973515E4 B61EEE20
        42884B47 1C1A729A 6C1CB026 81597CFC 8B8FAABA 8019326C


    Key is
        B9565402 F6291841 973515E4 B61EEE20 42884B47 1C1A729A


    V is
                           6C1CB026 81597CFC 8B8FAABA 8019326C


rnd_val is
                                              08C0521E BC9871E9
        DC055DA1 B79E2FF0 DCE28C18 9E83156F F3D71586 21F5675A


##############################################################

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                           00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
```

```
    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Update

    provided_data is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    ------------

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000
```

```
  V is
                      00000000 00000000 00000000 00000001


  output_block is
                      CD33B28A C773F74B A00ED1F3 12572435


  temp is
                      CD33B28A C773F74B A00ED1F3 12572435


------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000002


  output_block is
                      98E7247C 07F0FE41 1C267E43 84B0F600


  temp is
                                          CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000003
```

```
      output_block is
                          2A3493E6 6235EE67 DEECCD2F 3B393BD8


      temp is
        CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
        1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8


    temp XOR provided_data is
                          CD32B089 C376F14C A807DBF8 1E5A2A3A
        88F6366F 13E5E856 043F6458 98ADE81F 0A15B1C5 4610C840


    Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


    V is
                          043F6458 98ADE81F 0A15B1C5 4610C840


-------------------------------------------------------------

First call to Generate

**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
**************************************************************

CTR_DRBG_Reseed

    entropy_input is
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    additional_input is  <empty>
```

```
---------------------------

  Update

    provided_data is
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    ------------

      While loop

      Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


      V is
                          043F6458 98ADE81F 0A15B1C5 4610C841


      output_block is
                          01E0793E 6C7464FA FE1F6CF9 B7466A8A


      temp is
                          01E0793E 6C7464FA FE1F6CF9 B7466A8A


    ------------

      While loop

      Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


      V is
                          043F6458 98ADE81F 0A15B1C5 4610C842


      output_block is
                          C4841737 9CBAA104 13DBCD98 E1977019
```

```
      temp is
                                                01E0793E 6C7464FA
        FE1F6CF9 B7466A8A C4841737 9CBAA104 13DBCD98 E1977019


    ------------

      While loop

      Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


      V is
                           043F6458 98ADE81F 0A15B1C5 4610C843


      output_block is
                           685C8679 5A13E060 4CA155CA 4D9BF978


      temp is
        01E0793E 6C7464FA FE1F6CF9 B7466A8A C4841737 9CBAA104
        13DBCD98 E1977019 685C8679 5A13E060 4CA155CA 4D9BF978


    temp XOR provided_data is
                           8161FBBD E8F1E27D 7696E672 3BCBE405
        541585A4 082F3793 8B425703 7D0AEE86 C8FD24DA FEB646C7


    Key is
        8161FBBD E8F1E27D 7696E672 3BCBE405 541585A4 082F3793


    V is
                           8B425703 7D0AEE86 C8FD24DA FEB646C7


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>
```

```
---------------------------

  Update

    provided_data is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
        8161FBBD E8F1E27D 7696E672 3BCBE405 541585A4 082F3793


      V is
                          8B425703 7D0AEE86 C8FD24DA FEB646CA


      output_block is
                          D22454A5 C69A88BB 9F794ECD BE269F00


      temp is
                          D22454A5 C69A88BB 9F794ECD BE269F00


    ------------

      While loop

      Key is
        8161FBBD E8F1E27D 7696E672 3BCBE405 541585A4 082F3793


      V is
                          8B425703 7D0AEE86 C8FD24DA FEB646CB


      output_block is
                          A5A864D8 F73455B5 AF08CFCB 5A692D38
```

```
      temp is
                                                D22454A5 C69A88BB
        9F794ECD BE269F00 A5A864D8 F73455B5 AF08CFCB 5A692D38


    ------------

      While loop

      Key is
        8161FBBD E8F1E27D 7696E672 3BCBE405 541585A4 082F3793


      V is
                           8B425703 7D0AEE86 C8FD24DA FEB646CC


      output_block is
                           E7E12D86 FC49BC02 8EC6F12C CD5D8AEB


      temp is
        D22454A5 C69A88BB 9F794ECD BE269F00 A5A864D8 F73455B5
        AF08CFCB 5A692D38 E7E12D86 FC49BC02 8EC6F12C CD5D8AEB


    temp XOR provided_data is
                           D22454A5 C69A88BB 9F794ECD BE269F00
        A5A864D8 F73455B5 AF08CFCB 5A692D38 E7E12D86 FC49BC02


    Key is
        D22454A5 C69A88BB 9F794ECD BE269F00 A5A864D8 F73455B5


    V is
                           AF08CFCB 5A692D38 E7E12D86 FC49BC02


rnd_val is
                                                2A63138E AC6C8BD5
        AFDBEA16 C751A239 24A5C5C3 63452EF1 8259D96F EA6D6334


------------------------------------------------------------
```

```
Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    ------------

      While loop

      Key is
        D22454A5 C69A88BB 9F794ECD BE269F00 A5A864D8 F73455B5


      V is
                          AF08CFCB 5A692D38 E7E12D86 FC49BC03


      output_block is
                          B361741A 22BDF0A6 B4FC7A25 36750B6D
```

```
  temp is
                      B361741A 22BDF0A6 B4FC7A25 36750B6D


------------

  While loop

  Key is
    D22454A5 C69A88BB 9F794ECD BE269F00 A5A864D8 F73455B5


  V is
                      AF08CFCB 5A692D38 E7E12D86 FC49BC04


  output_block is
                      CD76540C 799278F1 511ACBAD F835DFAF


  temp is
                                        B361741A 22BDF0A6
    B4FC7A25 36750B6D CD76540C 799278F1 511ACBAD F835DFAF


------------

  While loop

  Key is
    D22454A5 C69A88BB 9F794ECD BE269F00 A5A864D8 F73455B5


  V is
                      AF08CFCB 5A692D38 E7E12D86 FC49BC05


  output_block is
                      33D4CE1B C9CE5AE7 572F5244 41F61501


  temp is
    B361741A 22BDF0A6 B4FC7A25 36750B6D CD76540C 799278F1
    511ACBAD F835DFAF 33D4CE1B C9CE5AE7 572F5244 41F61501
```

```
    temp XOR provided_data is
                          73A0B6D9 E6783661 7C35B0EE FAB8C5A2
        1DA786DF AD47AE26 89C31176 24E80170 D3352CF8 2D2BBC00


    Key is
        73A0B6D9 E6783661 7C35B0EE FAB8C5A2 1DA786DF AD47AE26


    V is
                          89C31176 24E80170 D3352CF8 2D2BBC00


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
        73A0B6D9 E6783661 7C35B0EE FAB8C5A2 1DA786DF AD47AE26


      V is
                          89C31176 24E80170 D3352CF8 2D2BBC03


      output_block is
                          29BC0399 0071959E 1B1883BE 6CFB8491
```

```
  temp is
                      29BC0399 0071959E 1B1883BE 6CFB8491


------------

  While loop

  Key is
    73A0B6D9 E6783661 7C35B0EE FAB8C5A2 1DA786DF AD47AE26


  V is
                      89C31176 24E80170 D3352CF8 2D2BBC04


  output_block is
                      137879F8 D65054CA FE54B28E D4893A5F


  temp is
                                        29BC0399 0071959E
    1B1883BE 6CFB8491 137879F8 D65054CA FE54B28E D4893A5F


------------

  While loop

  Key is
    73A0B6D9 E6783661 7C35B0EE FAB8C5A2 1DA786DF AD47AE26


  V is
                      89C31176 24E80170 D3352CF8 2D2BBC05


  output_block is
                      4A792EC9 5BAE9624 D529E396 88DE671D


  temp is
    29BC0399 0071959E 1B1883BE 6CFB8491 137879F8 D65054CA
    FE54B28E D4893A5F 4A792EC9 5BAE9624 D529E396 88DE671D
```

```
    temp XOR provided_data is
                          29BC0399 0071959E 1B1883BE 6CFB8491
        137879F8 D65054CA FE54B28E D4893A5F 4A792EC9 5BAE9624


    Key is
        29BC0399 0071959E 1B1883BE 6CFB8491 137879F8 D65054CA


    V is
                          FE54B28E D4893A5F 4A792EC9 5BAE9624


rnd_val is
                                            7B737A56 AD339224
        EA513F69 F7D4253E 832B6B48 A82AFA53 28C8E061 7F55AB54


################################################################

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    PersonalizationString = <empty>

    AdditionalInput1 =
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687
```

```
    AdditionalInput2 =
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


################################################################

****************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Update

    provided_data is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    ------------

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                          00000000 00000000 00000000 00000001


      output_block is
                          CD33B28A C773F74B A00ED1F3 12572435
```

```
  temp is
                      CD33B28A C773F74B A00ED1F3 12572435


------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000002


  output_block is
                      98E7247C 07F0FE41 1C267E43 84B0F600


  temp is
                                        CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000003


  output_block is
                      2A3493E6 6235EE67 DEECCD2F 3B393BD8


  temp is
    CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
    1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8
```

```
    temp XOR provided_data is
                          CD32B089 C376F14C A807DBF8 1E5A2A3A
        88F6366F 13E5E856 043F6458 98ADE81F 0A15B1C5 4610C840


    Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


    V is
                          043F6458 98ADE81F 0A15B1C5 4610C840


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


Generate FAILED: Reseed is required
*************************************************************

CTR_DRBG_Reseed

    entropy_input is
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


---------------------------
```

```
Update

  provided_data is
                        E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0
      E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 20202020 20202020


  ------------

    While loop

    Key is
      CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


    V is
                        043F6458 98ADE81F 0A15B1C5 4610C841


    output_block is
                        01E0793E 6C7464FA FE1F6CF9 B7466A8A


    temp is
                        01E0793E 6C7464FA FE1F6CF9 B7466A8A


  ------------

    While loop

    Key is
      CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


    V is
                        043F6458 98ADE81F 0A15B1C5 4610C842


    output_block is
                        C4841737 9CBAA104 13DBCD98 E1977019


    temp is
                                             01E0793E 6C7464FA
      FE1F6CF9 B7466A8A C4841737 9CBAA104 13DBCD98 E1977019
```

```
    ------------

      While loop

      Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


      V is
                           043F6458 98ADE81F 0A15B1C5 4610C843


      output_block is
                           685C8679 5A13E060 4CA155CA 4D9BF978


      temp is
        01E0793E 6C7464FA FE1F6CF9 B7466A8A C4841737 9CBAA104
        13DBCD98 E1977019 685C8679 5A13E060 4CA155CA 4D9BF978


    temp XOR provided_data is
                           E10099DE 8C94841A 1EFF8C19 57A68A6A
        2464F7D7 7C5A41E4 F33B2D78 017790F9 487CA659 7A33C040


    Key is
        E10099DE 8C94841A 1EFF8C19 57A68A6A 2464F7D7 7C5A41E4


    V is
                           F33B2D78 017790F9 487CA659 7A33C040


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------
```

```
Update

  provided_data is
                        00000000 00000000 00000000 00000000
      00000000 00000000 00000000 00000000 00000000 00000000


  ------------

    While loop

    Key is
      E10099DE 8C94841A 1EFF8C19 57A68A6A 2464F7D7 7C5A41E4


    V is
                        F33B2D78 017790F9 487CA659 7A33C043


    output_block is
                        8634F673 A82114CB 4A44F2FE A27931AC


    temp is
                        8634F673 A82114CB 4A44F2FE A27931AC


  ------------

    While loop

    Key is
      E10099DE 8C94841A 1EFF8C19 57A68A6A 2464F7D7 7C5A41E4


    V is
                        F33B2D78 017790F9 487CA659 7A33C044


    output_block is
                        A63249E0 C3BC126A 9EA4A87C 1E175989


    temp is
                                            8634F673 A82114CB
      4A44F2FE A27931AC A63249E0 C3BC126A 9EA4A87C 1E175989
```

```
    ------------

      While loop

      Key is
        E10099DE 8C94841A 1EFF8C19 57A68A6A 2464F7D7 7C5A41E4


      V is
                           F33B2D78 017790F9 487CA659 7A33C045


      output_block is
                           DA056F63 F4FDE170 DC496497 1DEB4607


      temp is
        8634F673 A82114CB 4A44F2FE A27931AC A63249E0 C3BC126A
        9EA4A87C 1E175989 DA056F63 F4FDE170 DC496497 1DEB4607


    temp XOR provided_data is
                           8634F673 A82114CB 4A44F2FE A27931AC
        A63249E0 C3BC126A 9EA4A87C 1E175989 DA056F63 F4FDE170


    Key is
        8634F673 A82114CB 4A44F2FE A27931AC A63249E0 C3BC126A


    V is
                           9EA4A87C 1E175989 DA056F63 F4FDE170


rnd_val is
                                              771B1F40 BFCE49D0
        9CFF56F8 9B171066 B07B6F07 BDFEAD61 04A5DCDA 011F2C68


------------------------------------------------------------

Second call to Generate

************************************************************
```

```
CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


---------------------------

  Update

    provided_data is
                          60606060 60606060 60606060 60606060
        60606060 60606060 60606060 60606060 20202020 20202020


    ------------

      While loop

      Key is
        8634F673 A82114CB 4A44F2FE A27931AC A63249E0 C3BC126A


      V is
                          9EA4A87C 1E175989 DA056F63 F4FDE171
```

```
  output_block is
                      ECAAFA28 34FD5CD0 1CBBE049 55247EE9

  temp is
                      ECAAFA28 34FD5CD0 1CBBE049 55247EE9

------------

  While loop

  Key is
    8634F673 A82114CB 4A44F2FE A27931AC A63249E0 C3BC126A

  V is
                      9EA4A87C 1E175989 DA056F63 F4FDE172

  output_block is
                      A167A122 6E3FAB97 76DDA1B2 BEC2CC85

  temp is
                                        ECAAFA28 34FD5CD0
    1CBBE049 55247EE9 A167A122 6E3FAB97 76DDA1B2 BEC2CC85

------------

  While loop

  Key is
    8634F673 A82114CB 4A44F2FE A27931AC A63249E0 C3BC126A

  V is
                      9EA4A87C 1E175989 DA056F63 F4FDE173

  output_block is
                      26683FD2 A0E12C4C 11AE83C9 69EA69C6

  temp is
```

```
        ECAAFA28 34FD5CD0 1CBBE049 55247EE9 A167A122 6E3FAB97
        76DDA1B2 BEC2CC85 26683FD2 A0E12C4C 11AE83C9 69EA69C6


    temp XOR provided_data is
                         8CCA9A48 549D3CB0 7CDB8029 35441E89
        C107C142 0E5FCBF7 16BDC1D2 DEA2ACE5 06481FF2 80C10C6C


    Key is
        8CCA9A48 549D3CB0 7CDB8029 35441E89 C107C142 0E5FCBF7


    V is
                         16BDC1D2 DEA2ACE5 06481FF2 80C10C6C


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                         00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
        8CCA9A48 549D3CB0 7CDB8029 35441E89 C107C142 0E5FCBF7


      V is
                         16BDC1D2 DEA2ACE5 06481FF2 80C10C6F
```

```
  output_block is
                      298EC2BE BC7DAE53 F88D67DE 7125CB97

  temp is
                      298EC2BE BC7DAE53 F88D67DE 7125CB97

------------

  While loop

  Key is
    8CCA9A48 549D3CB0 7CDB8029 35441E89 C107C142 0E5FCBF7

  V is
                      16BDC1D2 DEA2ACE5 06481FF2 80C10C70

  output_block is
                      E06FA0E8 A20A15A1 FC155364 07F4A3E9

  temp is
                                        298EC2BE BC7DAE53
    F88D67DE 7125CB97 E06FA0E8 A20A15A1 FC155364 07F4A3E9

------------

  While loop

  Key is
    8CCA9A48 549D3CB0 7CDB8029 35441E89 C107C142 0E5FCBF7

  V is
                      16BDC1D2 DEA2ACE5 06481FF2 80C10C71

  output_block is
                      9036A585 5D5D1DA7 5D0BE6B0 404CA1B9

  temp is
```

```
        298EC2BE BC7DAE53 F88D67DE 7125CB97 E06FA0E8 A20A15A1
        FC155364 07F4A3E9 9036A585 5D5D1DA7 5D0BE6B0 404CA1B9


    temp XOR provided_data is
                         298EC2BE BC7DAE53 F88D67DE 7125CB97
        E06FA0E8 A20A15A1 FC155364 07F4A3E9 9036A585 5D5D1DA7


    Key is
        298EC2BE BC7DAE53 F88D67DE 7125CB97 E06FA0E8 A20A15A1


    V is
                         FC155364 07F4A3E9 9036A585 5D5D1DA7


rnd_val is
                                            E2F2D79B 95699645
        125E327B 6E277ADE 061CA509 70E25CD3 7F42347E 371D3A24


################################################################

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                         00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                         80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                         C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    PersonalizationString =
                         40414243 44454647 48494A4B 4C4D4E4F
```

```
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    AdditionalInput = <empty>

###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                         00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    personal_str is
                         40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Update

    provided_data is
                         40404040 40404040 40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


    ------------

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                         00000000 00000000 00000000 00000001


      output_block is
                         CD33B28A C773F74B A00ED1F3 12572435
```

```
  temp is
                      CD33B28A C773F74B A00ED1F3 12572435


------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000002


  output_block is
                      98E7247C 07F0FE41 1C267E43 84B0F600


  temp is
                                        CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000003


  output_block is
                      2A3493E6 6235EE67 DEECCD2F 3B393BD8


  temp is
    CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
    1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8
```

```
    temp XOR provided_data is
                          8D73F2CA 8733B70B E04E91B3 52176475
        D8A7643C 47B0BE01 5C663E03 C4F0B640 6A74D3A6 2275AE27


    Key is
        8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


    V is
                          5C663E03 C4F0B640 6A74D3A6 2275AE27


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

CTR_DRBG_Reseed

    entropy_input is
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
```

```
------------

  While loop

  Key is
    8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


  V is
                       5C663E03 C4F0B640 6A74D3A6 2275AE28


  output_block is
                       517150FF D52BD344 DE78992B A224930C


  temp is
                       517150FF D52BD344 DE78992B A224930C


------------

  While loop

  Key is
    8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


  V is
                       5C663E03 C4F0B640 6A74D3A6 2275AE29


  output_block is
                       98FC9FAC 541236E8 D199A476 B960B301


  temp is
                                          517150FF D52BD344
    DE78992B A224930C 98FC9FAC 541236E8 D199A476 B960B301


------------

  While loop
```

```
      Key is
        8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


      V is
                           5C663E03 C4F0B640 6A74D3A6 2275AE2A


      output_block is
                           2D882249 1114B01B 2208E492 F0F35C54


      temp is
        517150FF D52BD344 DE78992B A224930C 98FC9FAC 541236E8
        D199A476 B960B301 2D882249 1114B01B 2208E492 F0F35C54


    temp XOR provided_data is
                           D1F0D27C 51AE55C3 56F113A0 2EA91D83
        086D0D3F C087A07F 49003EED 25FD2D9E 8D2980EA B5B116BC


    Key is
        D1F0D27C 51AE55C3 56F113A0 2EA91D83 086D0D3F C087A07F


    V is
                           49003EED 25FD2D9E 8D2980EA B5B116BC


***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                           00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
```

```
------------

  While loop

  Key is
    D1F0D27C 51AE55C3 56F113A0 2EA91D83 086D0D3F C087A07F


  V is
                       49003EED 25FD2D9E 8D2980EA B5B116BF


  output_block is
                       A56D4CE9 FD170AE7 82685E09 9032604C


  temp is
                       A56D4CE9 FD170AE7 82685E09 9032604C


------------

  While loop

  Key is
    D1F0D27C 51AE55C3 56F113A0 2EA91D83 086D0D3F C087A07F


  V is
                       49003EED 25FD2D9E 8D2980EA B5B116C0


  output_block is
                       6E29C59B 2273C047 5F34F3BF 7703D618


  temp is
                                            A56D4CE9 FD170AE7
    82685E09 9032604C 6E29C59B 2273C047 5F34F3BF 7703D618


------------

  While loop
```

```
      Key is
        D1F0D27C 51AE55C3 56F113A0 2EA91D83 086D0D3F C087A07F


      V is
                           49003EED 25FD2D9E 8D2980EA B5B116C1


      output_block is
                           2A65FBCB E232DB6C 99F15760 4D61C485


      temp is
        A56D4CE9 FD170AE7 82685E09 9032604C 6E29C59B 2273C047
        5F34F3BF 7703D618 2A65FBCB E232DB6C 99F15760 4D61C485


    temp XOR provided_data is
                           A56D4CE9 FD170AE7 82685E09 9032604C
        6E29C59B 2273C047 5F34F3BF 7703D618 2A65FBCB E232DB6C


    Key is
        A56D4CE9 FD170AE7 82685E09 9032604C 6E29C59B 2273C047


    V is
                           5F34F3BF 7703D618 2A65FBCB E232DB6C


rnd_val is
                                              77562EBE 8EECDF9E
        DB9A2E88 640D8DFF 9F2A5E99 20B30313 DC33D3A8 CE3BAB41


------------------------------------------------------------

Second call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256
```

```
    additional_input is  <empty>

Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    ------------

      While loop

      Key is
        A56D4CE9 FD170AE7 82685E09 9032604C 6E29C59B 2273C047


      V is
                          5F34F3BF 7703D618 2A65FBCB E232DB6D


      output_block is
                          05A1EDE5 719ACDE6 47A89FB9 87921D0E


      temp is
                          05A1EDE5 719ACDE6 47A89FB9 87921D0E


    ------------

      While loop
```

```
  Key is
    A56D4CE9 FD170AE7 82685E09 9032604C 6E29C59B 2273C047


  V is
                       5F34F3BF 7703D618 2A65FBCB E232DB6E


  output_block is
                       325735D9 1CCAA935 6DCA4C7E B58663A3


  temp is
                                         05A1EDE5 719ACDE6
    47A89FB9 87921D0E 325735D9 1CCAA935 6DCA4C7E B58663A3


------------

  While loop

  Key is
    A56D4CE9 FD170AE7 82685E09 9032604C 6E29C59B 2273C047


  V is
                       5F34F3BF 7703D618 2A65FBCB E232DB6F


  output_block is
                       763ECAA0 2113F3A2 7A47C858 C9A54596


  temp is
    05A1EDE5 719ACDE6 47A89FB9 87921D0E 325735D9 1CCAA935
    6DCA4C7E B58663A3 763ECAA0 2113F3A2 7A47C858 C9A54596


temp XOR provided_data is
                       C5602F26 B55F0B21 8F615572 4B5FD3C1
    E286E70A C81F7FE2 B51396A5 695BBD7C 96DF2843 C5F61545


Key is
    C5602F26 B55F0B21 8F615572 4B5FD3C1 E286E70A C81F7FE2
```

```
    V is
                          B51396A5 695BBD7C 96DF2843 C5F61545

***************************************************************
CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
        C5602F26 B55F0B21 8F615572 4B5FD3C1 E286E70A C81F7FE2


      V is
                          B51396A5 695BBD7C 96DF2843 C5F61548


      output_block is
                          602034D1 338F663B 0C0D138A D6C6901E


      temp is
                          602034D1 338F663B 0C0D138A D6C6901E


    ------------

      While loop
```

```
  Key is
    C5602F26 B55F0B21 8F615572 4B5FD3C1 E286E70A C81F7FE2


  V is
                      B51396A5 695BBD7C 96DF2843 C5F61549


  output_block is
                      E54548F7 E8C639EE 17A732EB 53C51B24


  temp is
                                          602034D1 338F663B
    0C0D138A D6C6901E E54548F7 E8C639EE 17A732EB 53C51B24


------------

  While loop

  Key is
    C5602F26 B55F0B21 8F615572 4B5FD3C1 E286E70A C81F7FE2


  V is
                      B51396A5 695BBD7C 96DF2843 C5F6154A


  output_block is
                      8C2513B5 1E0959B7 8B678503 5C1C486D


  temp is
    602034D1 338F663B 0C0D138A D6C6901E E54548F7 E8C639EE
    17A732EB 53C51B24 8C2513B5 1E0959B7 8B678503 5C1C486D


temp XOR provided_data is
                      602034D1 338F663B 0C0D138A D6C6901E
    E54548F7 E8C639EE 17A732EB 53C51B24 8C2513B5 1E0959B7


Key is
    602034D1 338F663B 0C0D138A D6C6901E E54548F7 E8C639EE
```

```
    V is
                          17A732EB 53C51B24 8C2513B5 1E0959B7


rnd_val is
                                                1BB94DB5 81E84F96
         37933BE7 81749070 62F0E95F 7AA30739 EC6FB059 6B74CFFD


##############################################################

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    PersonalizationString =
                          40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    AdditionalInput1 =
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


    AdditionalInput2 =
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7
```

```
###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    personal_str is
                          40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Update

    provided_data is
                          40404040 40404040 40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


    ------------

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                          00000000 00000000 00000000 00000001


      output_block is
                          CD33B28A C773F74B A00ED1F3 12572435


      temp is
```

```
                     CD33B28A C773F74B A00ED1F3 12572435


------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                     00000000 00000000 00000000 00000002


  output_block is
                     98E7247C 07F0FE41 1C267E43 84B0F600


  temp is
                                        CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                     00000000 00000000 00000000 00000003


  output_block is
                     2A3493E6 6235EE67 DEECCD2F 3B393BD8


  temp is
    CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
    1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8


temp XOR provided_data is
```

```
                        8D73F2CA 8733B70B E04E91B3 52176475
        D8A7643C 47B0BE01 5C663E03 C4F0B640 6A74D3A6 2275AE27


    Key is
        8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


    V is
                        5C663E03 C4F0B640 6A74D3A6 2275AE27


------------------------------------------------------------

First call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                        60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
                        80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    additional_input is
                        60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


--------------------------

  Update
```

```
provided_data is
                        E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0
    E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 20202020 20202020


------------

  While loop

  Key is
    8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


  V is
                        5C663E03 C4F0B640 6A74D3A6 2275AE28


  output_block is
                        517150FF D52BD344 DE78992B A224930C


  temp is
                        517150FF D52BD344 DE78992B A224930C


------------

  While loop

  Key is
    8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


  V is
                        5C663E03 C4F0B640 6A74D3A6 2275AE29


  output_block is
                        98FC9FAC 541236E8 D199A476 B960B301


  temp is
                                          517150FF D52BD344
    DE78992B A224930C 98FC9FAC 541236E8 D199A476 B960B301
```

```
    ------------

      While loop

      Key is
        8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


      V is
                           5C663E03 C4F0B640 6A74D3A6 2275AE2A


      output_block is
                           2D882249 1114B01B 2208E492 F0F35C54


      temp is
        517150FF D52BD344 DE78992B A224930C 98FC9FAC 541236E8
        D199A476 B960B301 2D882249 1114B01B 2208E492 F0F35C54


    temp XOR provided_data is
                           B191B01F 35CB33A4 3E9879CB 42C473EC
        781C7F4C B4F2D608 31794496 598053E1 0DA80269 3134903B


    Key is
        B191B01F 35CB33A4 3E9879CB 42C473EC 781C7F4C B4F2D608


    V is
                           31794496 598053E1 0DA80269 3134903B


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update
```

```
provided_data is
                      00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


------------

  While loop

  Key is
    B191B01F 35CB33A4 3E9879CB 42C473EC 781C7F4C B4F2D608


  V is
                      31794496 598053E1 0DA80269 3134903E


  output_block is
                      912734C5 1650B758 E174DF45 FE78D27C


  temp is
                      912734C5 1650B758 E174DF45 FE78D27C


------------

  While loop

  Key is
    B191B01F 35CB33A4 3E9879CB 42C473EC 781C7F4C B4F2D608


  V is
                      31794496 598053E1 0DA80269 3134903F


  output_block is
                      607F2F46 44BA4BDE E94EA700 CFA1A761


  temp is
                                        912734C5 1650B758
    E174DF45 FE78D27C 607F2F46 44BA4BDE E94EA700 CFA1A761
```

```
    ------------

      While loop

      Key is
        B191B01F 35CB33A4 3E9879CB 42C473EC 781C7F4C B4F2D608


      V is
                           31794496 598053E1 0DA80269 31349040


      output_block is
                           407918E1 DE591203 5D647E0E DD62AE0B


      temp is
        912734C5 1650B758 E174DF45 FE78D27C 607F2F46 44BA4BDE
        E94EA700 CFA1A761 407918E1 DE591203 5D647E0E DD62AE0B


    temp XOR provided_data is
                           912734C5 1650B758 E174DF45 FE78D27C
        607F2F46 44BA4BDE E94EA700 CFA1A761 407918E1 DE591203


    Key is
        912734C5 1650B758 E174DF45 FE78D27C 607F2F46 44BA4BDE


    V is
                           E94EA700 CFA1A761 407918E1 DE591203


rnd_val is
                                               4C36423F DDD11096
        DB6A62DA B872B607 F51ACB6E AA1A8FAD BA9A955E 08C2C136


------------------------------------------------------------

Second call to Generate

************************************************************

CTR_DRBG_Generate
```

```
  requested_number_of_bits = 256

    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


---------------------------

  Update

    provided_data is
                          60606060 60606060 60606060 60606060
        60606060 60606060 60606060 60606060 20202020 20202020


    ------------

      While loop

      Key is
        912734C5 1650B758 E174DF45 FE78D27C 607F2F46 44BA4BDE


      V is
                          E94EA700 CFA1A761 407918E1 DE591204


      output_block is
                          27CF86C6 8CC59F31 B56D6AEF C5E39991
```

```
  temp is
                      27CF86C6 8CC59F31 B56D6AEF C5E39991


------------

  While loop

  Key is
    912734C5 1650B758 E174DF45 FE78D27C 607F2F46 44BA4BDE


  V is
                      E94EA700 CFA1A761 407918E1 DE591205


  output_block is
                      5464349A 2D386DD7 8C680950 896580CB


  temp is
                                        27CF86C6 8CC59F31
    B56D6AEF C5E39991 5464349A 2D386DD7 8C680950 896580CB


------------

  While loop

  Key is
    912734C5 1650B758 E174DF45 FE78D27C 607F2F46 44BA4BDE


  V is
                      E94EA700 CFA1A761 407918E1 DE591206


  output_block is
                      90002416 13E390C0 BF953D14 A880A2C4


  temp is
    27CF86C6 8CC59F31 B56D6AEF C5E39991 5464349A 2D386DD7
    8C680950 896580CB 90002416 13E390C0 BF953D14 A880A2C4
```

```
    temp XOR provided_data is
                          47AFE6A6 ECA5FF51 D50D0A8F A583F9F1
        340454FA 4D580DB7 EC086930 E905E0AB B0200436 33C3B0E0


    Key is
        47AFE6A6 ECA5FF51 D50D0A8F A583F9F1 340454FA 4D580DB7


    V is
                          EC086930 E905E0AB B0200436 33C3B0E0


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
        47AFE6A6 ECA5FF51 D50D0A8F A583F9F1 340454FA 4D580DB7


      V is
                          EC086930 E905E0AB B0200436 33C3B0E3


      output_block is
                          EAC7E6F8 4AC4F0FF 1740CEF4 EE88EF73
```

```
  temp is
                      EAC7E6F8 4AC4F0FF 1740CEF4 EE88EF73


------------

  While loop

  Key is
    47AFE6A6 ECA5FF51 D50D0A8F A583F9F1 340454FA 4D580DB7


  V is
                      EC086930 E905E0AB B0200436 33C3B0E4


  output_block is
                      C16D1FBC 4061AEE2 4702F9A7 81EB43A2


  temp is
                                          EAC7E6F8 4AC4F0FF
    1740CEF4 EE88EF73 C16D1FBC 4061AEE2 4702F9A7 81EB43A2


------------

  While loop

  Key is
    47AFE6A6 ECA5FF51 D50D0A8F A583F9F1 340454FA 4D580DB7


  V is
                      EC086930 E905E0AB B0200436 33C3B0E5


  output_block is
                      274483A2 FC3B21EB B267557C 42C6AB80


  temp is
    EAC7E6F8 4AC4F0FF 1740CEF4 EE88EF73 C16D1FBC 4061AEE2
    4702F9A7 81EB43A2 274483A2 FC3B21EB B267557C 42C6AB80
```

```
    temp XOR provided_data is
                          EAC7E6F8 4AC4F0FF 1740CEF4 EE88EF73
        C16D1FBC 4061AEE2 4702F9A7 81EB43A2 274483A2 FC3B21EB


    Key is
        EAC7E6F8 4AC4F0FF 1740CEF4 EE88EF73 C16D1FBC 4061AEE2


    V is
                          4702F9A7 81EB43A2 274483A2 FC3B21EB


rnd_val is
                                             D859C7BF 0D15D50D
        81A65FEA B7D34605 1123E19F 64141105 43EA6D6F EE50EDEB


################################################################

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    PersonalizationString = <empty>

    AdditionalInput = <empty>
```

```
###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Update

    provided_data is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    ------------

      While loop

      Key is
                                              00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001


      output_block is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


      temp is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


    ------------
```

```
  While loop

  Key is
                                              00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000002


  output_block is
                      CEA7403D 4D606B6E 074EC5D3 BAF39D18


  temp is
                                              530F8AFB C74536B9
    A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18


------------

  While loop

  Key is
                                              00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000003


  output_block is
                      726003CA 37A62A74 D1A2F58E 7506358E


  temp is
    530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
    074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


temp XOR provided_data is
    530E88F8 C34030BE A16ABEFA C8C67D84 DEB6522E 59757D79
    1F57DFC8 A6EE8307 524121E9 13830C53 F98BDFA5 592B1BA1
```

```
    Key is
                                            530E88F8 C34030BE
        A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


    V is
                          524121E9 13830C53 F98BDFA5 592B1BA1


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                                            530E88F8 C34030BE
        A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


      V is
                          524121E9 13830C53 F98BDFA5 592B1BA4


      output_block is
```

```
                    056A8C26 6F9EF97E D08541DB D2E1FFA1

  temp is
                    056A8C26 6F9EF97E D08541DB D2E1FFA1

------------

  While loop

  Key is
                                        530E88F8 C34030BE
    A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307

  V is
                    524121E9 13830C53 F98BDFA5 592B1BA5

  output_block is
                    9810F539 2D076276 EF41277C 3AB6E94A

  temp is
                                        056A8C26 6F9EF97E
    D08541DB D2E1FFA1 9810F539 2D076276 EF41277C 3AB6E94A

------------

  While loop

  Key is
                                        530E88F8 C34030BE
    A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307

  V is
                    524121E9 13830C53 F98BDFA5 592B1BA6

  output_block is
                    4E3B7DCC 104A05BB 089D338B F55C72CA
```

```
      temp is
        056A8C26 6F9EF97E D08541DB D2E1FFA1 9810F539 2D076276
        EF41277C 3AB6E94A 4E3B7DCC 104A05BB 089D338B F55C72CA


    temp XOR provided_data is
        056A8C26 6F9EF97E D08541DB D2E1FFA1 9810F539 2D076276
        EF41277C 3AB6E94A 4E3B7DCC 104A05BB 089D338B F55C72CA


    Key is
                                            056A8C26 6F9EF97E
        D08541DB D2E1FFA1 9810F539 2D076276 EF41277C 3AB6E94A


    V is
                           4E3B7DCC 104A05BB 089D338B F55C72CA


rnd_val is
                                            06155023 4D158C5E
        C95595FE 04EF7A25 767F2E24 CC2BC479 D09D86DC 9ABCFDE7


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

--------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------
```

```
  While loop

  Key is
                                          056A8C26 6F9EF97E
    D08541DB D2E1FFA1 9810F539 2D076276 EF41277C 3AB6E94A


  V is
                      4E3B7DCC 104A05BB 089D338B F55C72CD


  output_block is
                      18FB8B4B 5DAC63E5 B479E085 C28B4073


  temp is
                      18FB8B4B 5DAC63E5 B479E085 C28B4073


------------

  While loop

  Key is
                                          056A8C26 6F9EF97E
    D08541DB D2E1FFA1 9810F539 2D076276 EF41277C 3AB6E94A


  V is
                      4E3B7DCC 104A05BB 089D338B F55C72CE


  output_block is
                      A6D7A24A 4E880BCE 3CFE4D7F B9DFABE1


  temp is
                                          18FB8B4B 5DAC63E5
    B479E085 C28B4073 A6D7A24A 4E880BCE 3CFE4D7F B9DFABE1


------------

  While loop
```

```
      Key is
                                              056A8C26 6F9EF97E
        D08541DB D2E1FFA1 9810F539 2D076276 EF41277C 3AB6E94A


      V is
                           4E3B7DCC 104A05BB 089D338B F55C72CF


      output_block is
                           AFDD5272 2A0D37B5 17F7B959 2D4E755D


      temp is
        18FB8B4B 5DAC63E5 B479E085 C28B4073 A6D7A24A 4E880BCE
        3CFE4D7F B9DFABE1 AFDD5272 2A0D37B5 17F7B959 2D4E755D


    temp XOR provided_data is
        18FB8B4B 5DAC63E5 B479E085 C28B4073 A6D7A24A 4E880BCE
        3CFE4D7F B9DFABE1 AFDD5272 2A0D37B5 17F7B959 2D4E755D


    Key is
                                              18FB8B4B 5DAC63E5
        B479E085 C28B4073 A6D7A24A 4E880BCE 3CFE4D7F B9DFABE1


    V is
                           AFDD5272 2A0D37B5 17F7B959 2D4E755D


rnd_val is
                                              1A9FBCBC 8DA36DFF
        2ABE2032 96170FDB 97C3297F 67FCB679 AC719C9F D00253B0


################################################################

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
```

```
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    PersonalizationString = <empty>

    AdditionalInput1 =
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


    AdditionalInput2 =
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


################################################################

****************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Update

    provided_data is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
```

```
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


------------

  While loop

  Key is
                                              00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                       00000000 00000000 00000000 00000001


  output_block is
                       530F8AFB C74536B9 A963B4F1 C4CB738B


  temp is
                       530F8AFB C74536B9 A963B4F1 C4CB738B


------------

  While loop

  Key is
                                              00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                       00000000 00000000 00000000 00000002


  output_block is
                       CEA7403D 4D606B6E 074EC5D3 BAF39D18


  temp is
                                              530F8AFB C74536B9
    A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18
```

```
    ------------

      While loop

      Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000003


      output_block is
                           726003CA 37A62A74 D1A2F58E 7506358E


      temp is
        530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
        074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


    temp XOR provided_data is
        530E88F8 C34030BE A16ABEFA C8C67D84 DEB6522E 59757D79
        1F57DFC8 A6EE8307 524121E9 13830C53 F98BDFA5 592B1BA1


    Key is
                                                530E88F8 C34030BE
        A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


    V is
                           524121E9 13830C53 F98BDFA5 592B1BA1


------------------------------------------------------------

First call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256
```

```
    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


  additional_input <> NULL, process appropriately
--------------------------

  Update

    provided_data is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


    ------------

      While loop

      Key is
                                              530E88F8 C34030BE
        A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


      V is
                          524121E9 13830C53 F98BDFA5 592B1BA2


      output_block is
                          06155023 4D158C5E C95595FE 04EF7A25


      temp is
                          06155023 4D158C5E C95595FE 04EF7A25


    ------------

      While loop

      Key is
                                              530E88F8 C34030BE
        A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


      V is
```

```
                      524121E9 13830C53 F98BDFA5 592B1BA3


  output_block is
                      767F2E24 CC2BC479 D09D86DC 9ABCFDE7


  temp is
                                        06155023 4D158C5E
    C95595FE 04EF7A25 767F2E24 CC2BC479 D09D86DC 9ABCFDE7


------------

  While loop

  Key is
                                        530E88F8 C34030BE
    A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


  V is
                      524121E9 13830C53 F98BDFA5 592B1BA4


  output_block is
                      056A8C26 6F9EF97E D08541DB D2E1FFA1


  temp is
    06155023 4D158C5E C95595FE 04EF7A25 767F2E24 CC2BC479
    D09D86DC 9ABCFDE7 056A8C26 6F9EF97E D08541DB D2E1FFA1


temp XOR provided_data is
    66743240 2970EA39 A13CFF95 6882144A 060E5C57 B85EB20E
    A8E4FCA7 E6C18398 85EB0EA5 EB1B7FF9 580CCB50 5E6C712E


Key is
                                        66743240 2970EA39
    A13CFF95 6882144A 060E5C57 B85EB20E A8E4FCA7 E6C18398


V is
                      85EB0EA5 EB1B7FF9 580CCB50 5E6C712E
```

```
---------------------------

  Update

    provided_data is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


    ------------

      While loop

      Key is
                                              66743240 2970EA39
        A13CFF95 6882144A 060E5C57 B85EB20E A8E4FCA7 E6C18398


      V is
                           85EB0EA5 EB1B7FF9 580CCB50 5E6C7131


      output_block is
                           346800DF CE6D40F5 0FCB89CD EE82941B


      temp is
                           346800DF CE6D40F5 0FCB89CD EE82941B


    ------------

      While loop

      Key is
                                              66743240 2970EA39
        A13CFF95 6882144A 060E5C57 B85EB20E A8E4FCA7 E6C18398


      V is
                           85EB0EA5 EB1B7FF9 580CCB50 5E6C7132


      output_block is
```

```
                        7E6C7BA8 4CFACC6A 0D721810 81DD5C32


      temp is
                                              346800DF CE6D40F5
        0FCB89CD EE82941B 7E6C7BA8 4CFACC6A 0D721810 81DD5C32


    ------------

      While loop

      Key is
                                              66743240 2970EA39
        A13CFF95 6882144A 060E5C57 B85EB20E A8E4FCA7 E6C18398


      V is
                        85EB0EA5 EB1B7FF9 580CCB50 5E6C7133


      output_block is
                        877534D9 08545CFD 9CAEAB8B 7A239397


      temp is
        346800DF CE6D40F5 0FCB89CD EE82941B 7E6C7BA8 4CFACC6A
        0D721810 81DD5C32 877534D9 08545CFD 9CAEAB8B 7A239397


    temp XOR provided_data is
        540962BC AA082692 67A2E3A6 82EFFA74 0E1D09DB 388FBA1D
        750B626B FDA0224D 07F4B65A 8CD1DA7A 14272100 F6AE1D18


    Key is
                                              540962BC AA082692
        67A2E3A6 82EFFA74 0E1D09DB 388FBA1D 750B626B FDA0224D


    V is
                        07F4B65A 8CD1DA7A 14272100 F6AE1D18


rnd_val is
                                              93A8EF3A C44E4A3D
```

```
        587DF216 EB6FE3B7 75EE3E94 4CAAC70F 35B56004 AE24B7B8


------------------------------------------------------------

Second call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    ------------

      While loop

      Key is
                                             540962BC AA082692
        67A2E3A6 82EFFA74 0E1D09DB 388FBA1D 750B626B FDA0224D


      V is
                           07F4B65A 8CD1DA7A 14272100 F6AE1D19


      output_block is
                           BCF91363 DA114FBB 6251B840 B0132E6C


      temp is
```

```
                    BCF91363 DA114FBB 6251B840 B0132E6C


------------

  While loop

  Key is
                                        540962BC AA082692
    67A2E3A6 82EFFA74 0E1D09DB 388FBA1D 750B626B FDA0224D


  V is
                    07F4B65A 8CD1DA7A 14272100 F6AE1D1A


  output_block is
                    F4B50026 055E61C5 B89CB4C2 3D8C1F6A


  temp is
                                        BCF91363 DA114FBB
    6251B840 B0132E6C F4B50026 055E61C5 B89CB4C2 3D8C1F6A


------------

  While loop

  Key is
                                        540962BC AA082692
    67A2E3A6 82EFFA74 0E1D09DB 388FBA1D 750B626B FDA0224D


  V is
                    07F4B65A 8CD1DA7A 14272100 F6AE1D1B


  output_block is
                    F50B710D 4167CE53 0C1463B0 A361FBB0


  temp is
    BCF91363 DA114FBB 6251B840 B0132E6C F4B50026 055E61C5
    B89CB4C2 3D8C1F6A F50B710D 4167CE53 0C1463B0 A361FBB0
```

```
    temp XOR provided_data is
        1C58B1C0 7EB4E91C CAF812EB 1CBE80C3 4404B295 B1EBD772
        00250E79 8131A1D5 35CAB3CE 85A20894 C4DDA97B 6FAC357F


    Key is
                                            1C58B1C0 7EB4E91C
        CAF812EB 1CBE80C3 4404B295 B1EBD772 00250E79 8131A1D5


    V is
                         35CAB3CE 85A20894 C4DDA97B 6FAC357F


---------------------------

  Update

    provided_data is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    ------------

      While loop

      Key is
                                            1C58B1C0 7EB4E91C
        CAF812EB 1CBE80C3 4404B295 B1EBD772 00250E79 8131A1D5


      V is
                         35CAB3CE 85A20894 C4DDA97B 6FAC3582


      output_block is
                         EECEE3A0 69F7653D 4A96AE43 7172EE2C


      temp is
                         EECEE3A0 69F7653D 4A96AE43 7172EE2C


    ------------
```

```
  While loop

  Key is
                                          1C58B1C0 7EB4E91C
    CAF812EB 1CBE80C3 4404B295 B1EBD772 00250E79 8131A1D5


  V is
                      35CAB3CE 85A20894 C4DDA97B 6FAC3583


  output_block is
                      848A92C9 E1E71461 E48D403E E6893AB0


  temp is
                                          EECEE3A0 69F7653D
    4A96AE43 7172EE2C 848A92C9 E1E71461 E48D403E E6893AB0


------------

  While loop

  Key is
                                          1C58B1C0 7EB4E91C
    CAF812EB 1CBE80C3 4404B295 B1EBD772 00250E79 8131A1D5


  V is
                      35CAB3CE 85A20894 C4DDA97B 6FAC3584


  output_block is
                      2393599C 9F15A18C A4F18BCE E25FDBD3


  temp is
    EECEE3A0 69F7653D 4A96AE43 7172EE2C 848A92C9 E1E71461
    E48D403E E6893AB0 2393599C 9F15A18C A4F18BCE E25FDBD3


temp XOR provided_data is
    4E6F4103 CD52C39A E23F04E8 DDDF4083 343B207A 5552A2D6
    5C34FA85 5A34840F E3529B5F 5BD0674B 6C384105 2E92151C
```

```
    Key is
                                            4E6F4103 CD52C39A
        E23F04E8 DDDF4083 343B207A 5552A2D6 5C34FA85 5A34840F


    V is
                         E3529B5F 5BD0674B 6C384105 2E92151C


rnd_val is
                                            8911B73C 1EC1626F
        37F221B1 2929BD5D 20B67373 768048E8 A1E0737E DF0F22D6


###############################################################

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    PersonalizationString =
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    AdditionalInput = <empty>

###############################################################
```

```
***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Update

    provided_data is
        40404040 40404040 40404040 40404040 40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


    ------------

      While loop

      Key is
                                              00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001


      output_block is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


      temp is
                           530F8AFB C74536B9 A963B4F1 C4CB738B
```

```
------------

  While loop

  Key is
                                              00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000002


  output_block is
                      CEA7403D 4D606B6E 074EC5D3 BAF39D18


  temp is
                                              530F8AFB C74536B9
    A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18


------------

  While loop

  Key is
                                              00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000003


  output_block is
                      726003CA 37A62A74 D1A2F58E 7506358E


  temp is
    530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
    074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


temp XOR provided_data is
```

```
        134FCABB 870576F9 E923F4B1 848B33CB 8EE7007D 0D202B2E
        470E8593 FAB3DD58 3220438A 77E66A34 91E2B5CE 354675CE


    Key is
                                           134FCABB 870576F9
        E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


    V is
                         3220438A 77E66A34 91E2B5CE 354675CE


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                                           134FCABB 870576F9
        E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


      V is
                         3220438A 77E66A34 91E2B5CE 354675D1
```

```
  output_block is
                      79B18865 9E08DC83 10050D9A 2EB958DF

  temp is
                      79B18865 9E08DC83 10050D9A 2EB958DF

------------

  While loop

  Key is
                                        134FCABB 870576F9
    E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58

  V is
                      3220438A 77E66A34 91E2B5CE 354675D2

  output_block is
                      87730C9A E9461189 C5EF7300 DE0F752C

  temp is
                                        79B18865 9E08DC83
    10050D9A 2EB958DF 87730C9A E9461189 C5EF7300 DE0F752C

------------

  While loop

  Key is
                                        134FCABB 870576F9
    E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58

  V is
                      3220438A 77E66A34 91E2B5CE 354675D3

  output_block is
                      33AC1C7E FB7384A0 A4A267F4 9CC5DA4E
```

```
      temp is
        79B18865 9E08DC83 10050D9A 2EB958DF 87730C9A E9461189
        C5EF7300 DE0F752C 33AC1C7E FB7384A0 A4A267F4 9CC5DA4E


    temp XOR provided_data is
        79B18865 9E08DC83 10050D9A 2EB958DF 87730C9A E9461189
        C5EF7300 DE0F752C 33AC1C7E FB7384A0 A4A267F4 9CC5DA4E


    Key is
                                            79B18865 9E08DC83
        10050D9A 2EB958DF 87730C9A E9461189 C5EF7300 DE0F752C


    V is
                          33AC1C7E FB7384A0 A4A267F4 9CC5DA4E


rnd_val is
                                            5DE6AA50 022F01DF
        045B3FDA 58A2AD77 9132F66F B04CE0C2 B0FA0721 F686D3E4


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
```

```
------------

  While loop

  Key is
                                          79B18865 9E08DC83
    10050D9A 2EB958DF 87730C9A E9461189 C5EF7300 DE0F752C


  V is
                      33AC1C7E FB7384A0 A4A267F4 9CC5DA51


  output_block is
                      CA8AFAEE 6CAFC480 16508AD9 1B8F9012


  temp is
                      CA8AFAEE 6CAFC480 16508AD9 1B8F9012


------------

  While loop

  Key is
                                          79B18865 9E08DC83
    10050D9A 2EB958DF 87730C9A E9461189 C5EF7300 DE0F752C


  V is
                      33AC1C7E FB7384A0 A4A267F4 9CC5DA52


  output_block is
                      DFCAEBD4 7953986D E33FDCCB 3CD614DD


  temp is
                                          CA8AFAEE 6CAFC480
    16508AD9 1B8F9012 DFCAEBD4 7953986D E33FDCCB 3CD614DD


------------
```

```
      While loop

      Key is
                                              79B18865 9E08DC83
        10050D9A 2EB958DF 87730C9A E9461189 C5EF7300 DE0F752C


      V is
                           33AC1C7E FB7384A0 A4A267F4 9CC5DA53


      output_block is
                           443B3D78 CCF212E4 9EFD4003 A3C33A05


      temp is
        CA8AFAEE 6CAFC480 16508AD9 1B8F9012 DFCAEBD4 7953986D
        E33FDCCB 3CD614DD 443B3D78 CCF212E4 9EFD4003 A3C33A05


    temp XOR provided_data is
        CA8AFAEE 6CAFC480 16508AD9 1B8F9012 DFCAEBD4 7953986D
        E33FDCCB 3CD614DD 443B3D78 CCF212E4 9EFD4003 A3C33A05


    Key is
                                              CA8AFAEE 6CAFC480
        16508AD9 1B8F9012 DFCAEBD4 7953986D E33FDCCB 3CD614DD


    V is
                           443B3D78 CCF212E4 9EFD4003 A3C33A05


rnd_val is
                                              1DD89F20 7997AE24
        C8EB7550 21A90AA1 3CA67FFC 6881D577 1A9745F8 0C7FD207


################################################################

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "NOT ENABLED"
```

```
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    PersonalizationString =
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    AdditionalInput1 =
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


    AdditionalInput2 =
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


##############################################################

**************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F
```

```
    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Update

    provided_data is
        40404040 40404040 40404040 40404040 40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


    ------------

      While loop

      Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001


      output_block is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


      temp is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


    ------------

      While loop

      Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000002


      output_block is
```

```
                        CEA7403D 4D606B6E 074EC5D3 BAF39D18


      temp is
                                               530F8AFB C74536B9
        A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18


    ------------

      While loop

      Key is
                                               00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                        00000000 00000000 00000000 00000003


      output_block is
                        726003CA 37A62A74 D1A2F58E 7506358E


      temp is
        530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
        074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


    temp XOR provided_data is
        134FCABB 870576F9 E923F4B1 848B33CB 8EE7007D 0D202B2E
        470E8593 FAB3DD58 3220438A 77E66A34 91E2B5CE 354675CE


    Key is
                                               134FCABB 870576F9
        E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


    V is
                        3220438A 77E66A34 91E2B5CE 354675CE


------------------------------------------------------------
```

```
First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


    ------------

      While loop

      Key is
                                            134FCABB 870576F9
        E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


      V is
                          3220438A 77E66A34 91E2B5CE 354675CF


      output_block is
                          5DE6AA50 022F01DF 045B3FDA 58A2AD77


      temp is
                          5DE6AA50 022F01DF 045B3FDA 58A2AD77


    ------------
```

```
  While loop

  Key is
                                          134FCABB 870576F9
    E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


  V is
                     3220438A 77E66A34 91E2B5CE 354675D0


  output_block is
                     9132F66F B04CE0C2 B0FA0721 F686D3E4


  temp is
                                          5DE6AA50 022F01DF
    045B3FDA 58A2AD77 9132F66F B04CE0C2 B0FA0721 F686D3E4


------------

  While loop

  Key is
                                          134FCABB 870576F9
    E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


  V is
                     3220438A 77E66A34 91E2B5CE 354675D1


  output_block is
                     79B18865 9E08DC83 10050D9A 2EB958DF


  temp is
    5DE6AA50 022F01DF 045B3FDA 58A2AD77 9132F66F B04CE0C2
    B0FA0721 F686D3E4 79B18865 9E08DC83 10050D9A 2EB958DF


temp XOR provided_data is
    3D87C833 664A67B8 6C3255B1 34CFC318 E143841C C43996B5
    C8837D5A 8AFBAD9B F9300AE6 1A8D5A04 988C8711 A234D650
```

```
    Key is
                                              3D87C833 664A67B8
        6C3255B1 34CFC318 E143841C C43996B5 C8837D5A 8AFBAD9B


    V is
                         F9300AE6 1A8D5A04 988C8711 A234D650


---------------------------

  Update

    provided_data is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


    ------------

      While loop

      Key is
                                              3D87C833 664A67B8
        6C3255B1 34CFC318 E143841C C43996B5 C8837D5A 8AFBAD9B


      V is
                         F9300AE6 1A8D5A04 988C8711 A234D653


      output_block is
                         FE4B16FC 3F12CD7C 9D681FEF BE37D72E


      temp is
                         FE4B16FC 3F12CD7C 9D681FEF BE37D72E


    ------------

      While loop

      Key is
                                              3D87C833 664A67B8
```

```
    6C3255B1 34CFC318 E143841C C43996B5 C8837D5A 8AFBAD9B


  V is
                      F9300AE6 1A8D5A04 988C8711 A234D654


  output_block is
                      0793697D B707C0D0 D194BDB6 7A7C821D


  temp is
                                        FE4B16FC 3F12CD7C
    9D681FEF BE37D72E 0793697D B707C0D0 D194BDB6 7A7C821D


------------

  While loop

  Key is
                                        3D87C833 664A67B8
    6C3255B1 34CFC318 E143841C C43996B5 C8837D5A 8AFBAD9B


  V is
                      F9300AE6 1A8D5A04 988C8711 A234D655


  output_block is
                      522AC4DF 59F07E9E 79359831 6150EFB3


  temp is
    FE4B16FC 3F12CD7C 9D681FEF BE37D72E 0793697D B707C0D0
    D194BDB6 7A7C821D 522AC4DF 59F07E9E 79359831 6150EFB3


temp XOR provided_data is
    9E2A749F 5B77AB1B F5017584 D25AB941 77E21B0E C372B6A7
    A9EDC7CD 0601FC62 D2AB465C DD75F819 F1BC12BA EDDD613C


Key is
                                        9E2A749F 5B77AB1B
    F5017584 D25AB941 77E21B0E C372B6A7 A9EDC7CD 0601FC62
```

```
    V is
                          D2AB465C DD75F819 F1BC12BA EDDD613C


rnd_val is
                                              35CE8218 C03B7592
        FAF29D19 72273983 6CEEF066 6E058ABF 8B837AB5 E5E743D9


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    ------------

      While loop

      Key is
                                              9E2A749F 5B77AB1B
        F5017584 D25AB941 77E21B0E C372B6A7 A9EDC7CD 0601FC62


      V is
```

```
                      D2AB465C DD75F819 F1BC12BA EDDD613D

  output_block is
                      3E56FF9B 2E3BC503 12CDDC61 47A1511F

  temp is
                      3E56FF9B 2E3BC503 12CDDC61 47A1511F

------------

  While loop

  Key is
                                          9E2A749F 5B77AB1B
    F5017584 D25AB941 77E21B0E C372B6A7 A9EDC7CD 0601FC62

  V is
                      D2AB465C DD75F819 F1BC12BA EDDD613E

  output_block is
                      FE3CCEA1 E661A3C3 9F75BF33 E6A50D11

  temp is
                                          3E56FF9B 2E3BC503
    12CDDC61 47A1511F FE3CCEA1 E661A3C3 9F75BF33 E6A50D11

------------

  While loop

  Key is
                                          9E2A749F 5B77AB1B
    F5017584 D25AB941 77E21B0E C372B6A7 A9EDC7CD 0601FC62

  V is
                      D2AB465C DD75F819 F1BC12BA EDDD613F
```

```
      output_block is
                           BAFDFC5F E40E86DE BA48BFAE 8A16B1F5


      temp is
        3E56FF9B 2E3BC503 12CDDC61 47A1511F FE3CCEA1 E661A3C3
        9F75BF33 E6A50D11 BAFDFC5F E40E86DE BA48BFAE 8A16B1F5


    temp XOR provided_data is
        9EF75D38 8A9E63A4 BA6476CA EB0CFFB0 4E8D7C12 52D41574
        27CC0588 5A18B3AE 7A3C3E9C 20CB4019 72817565 46DB7F3A


    Key is
                                             9EF75D38 8A9E63A4
        BA6476CA EB0CFFB0 4E8D7C12 52D41574 27CC0588 5A18B3AE


    V is
                           7A3C3E9C 20CB4019 72817565 46DB7F3A


---------------------------

  Update

    provided_data is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    ------------

      While loop

      Key is
                                             9EF75D38 8A9E63A4
        BA6476CA EB0CFFB0 4E8D7C12 52D41574 27CC0588 5A18B3AE


      V is
                           7A3C3E9C 20CB4019 72817565 46DB7F3D


      output_block is
```

```
                    0D5AC3AD 225F868B 78ED4FD6 821E5C5E

  temp is
                    0D5AC3AD 225F868B 78ED4FD6 821E5C5E

------------

  While loop

  Key is
                                       9EF75D38 8A9E63A4
    BA6476CA EB0CFFB0 4E8D7C12 52D41574 27CC0588 5A18B3AE

  V is
                    7A3C3E9C 20CB4019 72817565 46DB7F3E

  output_block is
                    61B988FC E1614A2E 85BC9BEA 4767F7F7

  temp is
                                       0D5AC3AD 225F868B
    78ED4FD6 821E5C5E 61B988FC E1614A2E 85BC9BEA 4767F7F7

------------

  While loop

  Key is
                                       9EF75D38 8A9E63A4
    BA6476CA EB0CFFB0 4E8D7C12 52D41574 27CC0588 5A18B3AE

  V is
                    7A3C3E9C 20CB4019 72817565 46DB7F3F

  output_block is
                    29C2F084 866A22CF 1E447F3D 7A46C68B
```

```
      temp is
        0D5AC3AD 225F868B 78ED4FD6 821E5C5E 61B988FC E1614A2E
        85BC9BEA 4767F7F7 29C2F084 866A22CF 1E447F3D 7A46C68B


    temp XOR provided_data is
        ADFB610E 86FA202C D044E57D 2EB3F2F1 D1083A4F 55D4FC99
        3D052151 FBDA4948 E9033247 42AFE408 D68DB5F6 B68B0844


    Key is
                                            ADFB610E 86FA202C
        D044E57D 2EB3F2F1 D1083A4F 55D4FC99 3D052151 FBDA4948


    V is
                           E9033247 42AFE408 D68DB5F6 B68B0844


rnd_val is
                                            836CA0F7 75468B8A
        ABCD3129 FE2A2227 B2251DCC 22A0BFA0 175EAB7C A29892BA


################################################################

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF
```

```
    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Update

    provided_data is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    ------------

      While loop

      Key is
                                              00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001


      output_block is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


      temp is
```

```
                    530F8AFB C74536B9 A963B4F1 C4CB738B


------------

  While loop

  Key is
                                          00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                    00000000 00000000 00000000 00000002


  output_block is
                    CEA7403D 4D606B6E 074EC5D3 BAF39D18


  temp is
                                          530F8AFB C74536B9
    A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18


------------

  While loop

  Key is
                                          00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                    00000000 00000000 00000000 00000003


  output_block is
                    726003CA 37A62A74 D1A2F58E 7506358E


  temp is
    530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
    074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E
```

```
    temp XOR provided_data is
        530E88F8 C34030BE A16ABEFA C8C67D84 DEB6522E 59757D79
        1F57DFC8 A6EE8307 524121E9 13830C53 F98BDFA5 592B1BA1


    Key is
                                            530E88F8 C34030BE
        A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


    V is
                          524121E9 13830C53 F98BDFA5 592B1BA1


------------------------------------------------------------

First call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    additional_input is  <empty>

--------------------------

  Update

    provided_data is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
```

```
------------

  While loop

  Key is
                                          530E88F8 C34030BE
    A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


  V is
                      524121E9 13830C53 F98BDFA5 592B1BA2


  output_block is
                      06155023 4D158C5E C95595FE 04EF7A25


  temp is
                      06155023 4D158C5E C95595FE 04EF7A25


------------

  While loop

  Key is
                                          530E88F8 C34030BE
    A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


  V is
                      524121E9 13830C53 F98BDFA5 592B1BA3


  output_block is
                      767F2E24 CC2BC479 D09D86DC 9ABCFDE7


  temp is
                                          06155023 4D158C5E
    C95595FE 04EF7A25 767F2E24 CC2BC479 D09D86DC 9ABCFDE7


------------
```

```
      While loop

      Key is
                                              530E88F8 C34030BE
        A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


      V is
                           524121E9 13830C53 F98BDFA5 592B1BA4


      output_block is
                           056A8C26 6F9EF97E D08541DB D2E1FFA1


      temp is
        06155023 4D158C5E C95595FE 04EF7A25 767F2E24 CC2BC479
        D09D86DC 9ABCFDE7 056A8C26 6F9EF97E D08541DB D2E1FFA1


    temp XOR provided_data is
        8694D2A0 C9900AD9 41DC1F75 8862F4AA E6EEBCB7 58BE52EE
        48041C47 06216378 A5CB2E85 CB3B5FD9 782CEB70 7E4C510E


    Key is
                                              8694D2A0 C9900AD9
        41DC1F75 8862F4AA E6EEBCB7 58BE52EE 48041C47 06216378


    V is
                           A5CB2E85 CB3B5FD9 782CEB70 7E4C510E


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update
```

```
provided_data is
    00000000 00000000 00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


------------

  While loop

  Key is
                                          8694D2A0 C9900AD9
    41DC1F75 8862F4AA E6EEBCB7 58BE52EE 48041C47 06216378


  V is
                     A5CB2E85 CB3B5FD9 782CEB70 7E4C5111


  output_block is
                     D38F59F3 0937A627 4AFFFC17 6FF04E6C


  temp is
                     D38F59F3 0937A627 4AFFFC17 6FF04E6C


------------

  While loop

  Key is
                                          8694D2A0 C9900AD9
    41DC1F75 8862F4AA E6EEBCB7 58BE52EE 48041C47 06216378


  V is
                     A5CB2E85 CB3B5FD9 782CEB70 7E4C5112


  output_block is
                     6BCA6A95 33E7A5DB 8B946C2D 24271896


  temp is
                                          D38F59F3 0937A627
```

```
        4AFFFC17 6FF04E6C 6BCA6A95 33E7A5DB 8B946C2D 24271896


    ------------

      While loop

      Key is
                                              8694D2A0 C9900AD9
        41DC1F75 8862F4AA E6EEBCB7 58BE52EE 48041C47 06216378


      V is
                           A5CB2E85 CB3B5FD9 782CEB70 7E4C5113


      output_block is
                           ED06041B 417EBE9F 071443C9 47A03552


      temp is
        D38F59F3 0937A627 4AFFFC17 6FF04E6C 6BCA6A95 33E7A5DB
        8B946C2D 24271896 ED06041B 417EBE9F 071443C9 47A03552


    temp XOR provided_data is
        D38F59F3 0937A627 4AFFFC17 6FF04E6C 6BCA6A95 33E7A5DB
        8B946C2D 24271896 ED06041B 417EBE9F 071443C9 47A03552


    Key is
                                              D38F59F3 0937A627
        4AFFFC17 6FF04E6C 6BCA6A95 33E7A5DB 8B946C2D 24271896


    V is
                           ED06041B 417EBE9F 071443C9 47A03552


rnd_val is
                                              893EB3AE 65F69FE3
        1D7EFC8E E1583348 C1723F25 9F66875A 213CD971 2706FBA1


----------------------------------------------------------------
```

```
Second call to Generate

****************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
****************************************************************

CTR_DRBG_Reseed

    entropy_input is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    additional_input is  <empty>

---------------------------

  Update

    provided_data is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    ------------

      While loop

      Key is
                                              D38F59F3 0937A627
        4AFFFC17 6FF04E6C 6BCA6A95 33E7A5DB 8B946C2D 24271896


      V is
                           ED06041B 417EBE9F 071443C9 47A03553


      output_block is
                           9C7214B1 7A62F3FF 04208CE6 37FDE278
```

```
  temp is
                      9C7214B1 7A62F3FF 04208CE6 37FDE278


------------

  While loop

  Key is
                                           D38F59F3 0937A627
    4AFFFC17 6FF04E6C 6BCA6A95 33E7A5DB 8B946C2D 24271896


  V is
                      ED06041B 417EBE9F 071443C9 47A03554


  output_block is
                      D15FE4BB 48ED41E1 7CD0BCB9 C3EC3734


  temp is
                                           9C7214B1 7A62F3FF
    04208CE6 37FDE278 D15FE4BB 48ED41E1 7CD0BCB9 C3EC3734


------------

  While loop

  Key is
                                           D38F59F3 0937A627
    4AFFFC17 6FF04E6C 6BCA6A95 33E7A5DB 8B946C2D 24271896


  V is
                      ED06041B 417EBE9F 071443C9 47A03555


  output_block is
                      85E9A763 6B4BD924 6743708C B189CA43


  temp is
```

```
        9C7214B1 7A62F3FF 04208CE6 37FDE278 D15FE4BB 48ED41E1
        7CD0BCB9 C3EC3734 85E9A763 6B4BD924 6743708C B189CA43


    temp XOR provided_data is
        5CB3D672 BEA73538 CCE9462D FB302CB7 018E3668 9C389736
        A4096662 1F31E9EB 65084580 8FAE3FC3 8FAA9A67 5D6424AC


    Key is
                                            5CB3D672 BEA73538
        CCE9462D FB302CB7 018E3668 9C389736 A4096662 1F31E9EB


    V is
                          65084580 8FAE3FC3 8FAA9A67 5D6424AC


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                                            5CB3D672 BEA73538
        CCE9462D FB302CB7 018E3668 9C389736 A4096662 1F31E9EB


      V is
                          65084580 8FAE3FC3 8FAA9A67 5D6424AF
```

```
  output_block is
                      71A61373 72EB2FBE 90990C00 1B36E133

  temp is
                      71A61373 72EB2FBE 90990C00 1B36E133

------------

  While loop

  Key is
                                          5CB3D672 BEA73538
    CCE9462D FB302CB7 018E3668 9C389736 A4096662 1F31E9EB

  V is
                      65084580 8FAE3FC3 8FAA9A67 5D6424B0

  output_block is
                      8CAECEDB 87EE5AC1 02796183 02CAEFDF

  temp is
                                          71A61373 72EB2FBE
    90990C00 1B36E133 8CAECEDB 87EE5AC1 02796183 02CAEFDF

------------

  While loop

  Key is
                                          5CB3D672 BEA73538
    CCE9462D FB302CB7 018E3668 9C389736 A4096662 1F31E9EB

  V is
                      65084580 8FAE3FC3 8FAA9A67 5D6424B1

  output_block is
```

```
                          F58B83F4 A66CDE4D 30E913DC DF0F9501


      temp is
        71A61373 72EB2FBE 90990C00 1B36E133 8CAECEDB 87EE5AC1
        02796183 02CAEFDF F58B83F4 A66CDE4D 30E913DC DF0F9501


    temp XOR provided_data is
        71A61373 72EB2FBE 90990C00 1B36E133 8CAECEDB 87EE5AC1
        02796183 02CAEFDF F58B83F4 A66CDE4D 30E913DC DF0F9501


    Key is
                                           71A61373 72EB2FBE
        90990C00 1B36E133 8CAECEDB 87EE5AC1 02796183 02CAEFDF


    V is
                          F58B83F4 A66CDE4D 30E913DC DF0F9501


rnd_val is
                                           67219E23 0FEF83C0
        DF3B2020 1C8F9B5D DFF62224 D9CEF23A 6C96474C 2D1A51CD


################################################################

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
```

```
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    PersonalizationString = <empty>

    AdditionalInput1 =
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


    AdditionalInput2 =
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Update

    provided_data is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    ------------

      While loop

      Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
```

```
  V is
                      00000000 00000000 00000000 00000001

  output_block is
                      530F8AFB C74536B9 A963B4F1 C4CB738B

  temp is
                      530F8AFB C74536B9 A963B4F1 C4CB738B

------------

  While loop

  Key is
                                            00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000002

  output_block is
                      CEA7403D 4D606B6E 074EC5D3 BAF39D18

  temp is
                                            530F8AFB C74536B9
    A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18

------------

  While loop

  Key is
                                            00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000

  V is
```

```
                        00000000 00000000 00000000 00000003


      output_block is
                        726003CA 37A62A74 D1A2F58E 7506358E


      temp is
        530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
        074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


    temp XOR provided_data is
        530E88F8 C34030BE A16ABEFA C8C67D84 DEB6522E 59757D79
        1F57DFC8 A6EE8307 524121E9 13830C53 F98BDFA5 592B1BA1


    Key is
                                            530E88F8 C34030BE
        A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


    V is
                        524121E9 13830C53 F98BDFA5 592B1BA1


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


Generate FAILED: Reseed is required
*************************************************************

CTR_DRBG_Reseed
```

```
    entropy_input is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


----------------------------

  Update

    provided_data is
        E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0
        E0E0E0E0 E0E0E0E0 20202020 20202020 20202020 20202020


    ------------

      While loop

      Key is
                                              530E88F8 C34030BE
        A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


      V is
                           524121E9 13830C53 F98BDFA5 592B1BA2


      output_block is
                           06155023 4D158C5E C95595FE 04EF7A25


      temp is
                           06155023 4D158C5E C95595FE 04EF7A25


    ------------

      While loop

      Key is
                                              530E88F8 C34030BE
```

```
    A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


  V is
                      524121E9 13830C53 F98BDFA5 592B1BA3


  output_block is
                      767F2E24 CC2BC479 D09D86DC 9ABCFDE7


  temp is
                                        06155023 4D158C5E
    C95595FE 04EF7A25 767F2E24 CC2BC479 D09D86DC 9ABCFDE7


------------

  While loop

  Key is
                                        530E88F8 C34030BE
    A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


  V is
                      524121E9 13830C53 F98BDFA5 592B1BA4


  output_block is
                      056A8C26 6F9EF97E D08541DB D2E1FFA1


  temp is
    06155023 4D158C5E C95595FE 04EF7A25 767F2E24 CC2BC479
    D09D86DC 9ABCFDE7 056A8C26 6F9EF97E D08541DB D2E1FFA1


temp XOR provided_data is
    E6F5B0C3 ADF56CBE 29B5751E E40F9AC5 969FCEC4 2CCB2499
    307D663C 7A5C1D07 254AAC06 4FBED95E F0A561FB F2C1DF81


Key is
                                        E6F5B0C3 ADF56CBE
    29B5751E E40F9AC5 969FCEC4 2CCB2499 307D663C 7A5C1D07
```

```
    V is
                          254AAC06 4FBED95E F0A561FB F2C1DF81

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                                             E6F5B0C3 ADF56CBE
        29B5751E E40F9AC5 969FCEC4 2CCB2499 307D663C 7A5C1D07


      V is
                          254AAC06 4FBED95E F0A561FB F2C1DF84


      output_block is
                          DD63AE35 48ABB73F BF204A84 128DB2DB


      temp is
                          DD63AE35 48ABB73F BF204A84 128DB2DB


    ------------
```

```
  While loop

  Key is
                                          E6F5B0C3 ADF56CBE
    29B5751E E40F9AC5 969FCEC4 2CCB2499 307D663C 7A5C1D07


  V is
                      254AAC06 4FBED95E F0A561FB F2C1DF85


  output_block is
                      6562237F 51697F0D 33E4E071 64FCF487


  temp is
                                          DD63AE35 48ABB73F
    BF204A84 128DB2DB 6562237F 51697F0D 33E4E071 64FCF487


------------

  While loop

  Key is
                                          E6F5B0C3 ADF56CBE
    29B5751E E40F9AC5 969FCEC4 2CCB2499 307D663C 7A5C1D07


  V is
                      254AAC06 4FBED95E F0A561FB F2C1DF86


  output_block is
                      17E289C6 FFECF684 27E216B5 FE2907EC


  temp is
    DD63AE35 48ABB73F BF204A84 128DB2DB 6562237F 51697F0D
    33E4E071 64FCF487 17E289C6 FFECF684 27E216B5 FE2907EC


temp XOR provided_data is
    DD63AE35 48ABB73F BF204A84 128DB2DB 6562237F 51697F0D
    33E4E071 64FCF487 17E289C6 FFECF684 27E216B5 FE2907EC
```

```
    Key is
                                            DD63AE35 48ABB73F
        BF204A84 128DB2DB 6562237F 51697F0D 33E4E071 64FCF487


    V is
                          17E289C6 FFECF684 27E216B5 FE2907EC


rnd_val is
                                            499B4951 9CB0C1A7
        13CA0E5B 82DF4D11 6C370752 3D483563 BEBE9407 8C2A5E01


------------------------------------------------------------

Second call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


--------------------------
```

```
Update

  provided_data is
      60606060 60606060 60606060 60606060 60606060 60606060
      60606060 60606060 20202020 20202020 20202020 20202020


  ------------

    While loop

    Key is
                                              DD63AE35 48ABB73F
      BF204A84 128DB2DB 6562237F 51697F0D 33E4E071 64FCF487


    V is
                         17E289C6 FFECF684 27E216B5 FE2907ED


    output_block is
                         63262AB5 C764586B F1B3B575 1A872086


    temp is
                         63262AB5 C764586B F1B3B575 1A872086


  ------------

    While loop

    Key is
                                              DD63AE35 48ABB73F
      BF204A84 128DB2DB 6562237F 51697F0D 33E4E071 64FCF487


    V is
                         17E289C6 FFECF684 27E216B5 FE2907EE


    output_block is
                         80A7C59D 38A25C34 9BEBA5A2 4AB4223D
```

```
      temp is
                                                63262AB5 C764586B
        F1B3B575 1A872086 80A7C59D 38A25C34 9BEBA5A2 4AB4223D


    ------------

      While loop

      Key is
                                                DD63AE35 48ABB73F
        BF204A84 128DB2DB 6562237F 51697F0D 33E4E071 64FCF487


      V is
                           17E289C6 FFECF684 27E216B5 FE2907EF


      output_block is
                           6FB7EC4C 720DE4FB C66C81B2 719FDD90


      temp is
        63262AB5 C764586B F1B3B575 1A872086 80A7C59D 38A25C34
        9BEBA5A2 4AB4223D 6FB7EC4C 720DE4FB C66C81B2 719FDD90


    temp XOR provided_data is
        03464AD5 A704380B 91D3D515 7AE740E6 E0C7A5FD 58C23C54
        FB8BC5C2 2AD4425D 4F97CC6C 522DC4DB E64CA192 51BFFDB0


    Key is
                                                03464AD5 A704380B
        91D3D515 7AE740E6 E0C7A5FD 58C23C54 FB8BC5C2 2AD4425D


    V is
                           4F97CC6C 522DC4DB E64CA192 51BFFDB0

**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256
```

```
    additional_input is  <empty>

---------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                                                03464AD5 A704380B
        91D3D515 7AE740E6 E0C7A5FD 58C23C54 FB8BC5C2 2AD4425D


      V is
                           4F97CC6C 522DC4DB E64CA192 51BFFDB3


      output_block is
                           6F2CD028 10A911FF 62691817 C3A59DDD


      temp is
                           6F2CD028 10A911FF 62691817 C3A59DDD


    ------------

      While loop

      Key is
                                                03464AD5 A704380B
        91D3D515 7AE740E6 E0C7A5FD 58C23C54 FB8BC5C2 2AD4425D


      V is
                           4F97CC6C 522DC4DB E64CA192 51BFFDB4
```

```
      output_block is
                          4EB1F43E 186B49EF B7C3024E A407151A

      temp is
                                               6F2CD028 10A911FF
        62691817 C3A59DDD 4EB1F43E 186B49EF B7C3024E A407151A

    ------------

      While loop

      Key is
                                               03464AD5 A704380B
        91D3D515 7AE740E6 E0C7A5FD 58C23C54 FB8BC5C2 2AD4425D

      V is
                          4F97CC6C 522DC4DB E64CA192 51BFFDB5

      output_block is
                          8D075C41 42648381 376D27A8 8EE2760A

      temp is
        6F2CD028 10A911FF 62691817 C3A59DDD 4EB1F43E 186B49EF
        B7C3024E A407151A 8D075C41 42648381 376D27A8 8EE2760A

    temp XOR provided_data is
        6F2CD028 10A911FF 62691817 C3A59DDD 4EB1F43E 186B49EF
        B7C3024E A407151A 8D075C41 42648381 376D27A8 8EE2760A

    Key is
                                               6F2CD028 10A911FF
        62691817 C3A59DDD 4EB1F43E 186B49EF B7C3024E A407151A

    V is
                          8D075C41 42648381 376D27A8 8EE2760A

rnd_val is
```

```
                                                353B67AA E68C0CC6
        3C5567B4 86F2B27C 121469A2 757951E0 9429E33F 0758F3AD


###############################################################

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    PersonalizationString =
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    AdditionalInput = <empty>

###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
```

```
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Update

    provided_data is
        40404040 40404040 40404040 40404040 40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


    ------------

      While loop

      Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001


      output_block is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


      temp is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


    ------------

      While loop

      Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000002
```

```
  output_block is
                      CEA7403D 4D606B6E 074EC5D3 BAF39D18


  temp is
                                          530F8AFB C74536B9
    A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18


------------

  While loop

  Key is
                                          00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000003


  output_block is
                      726003CA 37A62A74 D1A2F58E 7506358E


  temp is
    530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
    074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


temp XOR provided_data is
    134FCABB 870576F9 E923F4B1 848B33CB 8EE7007D 0D202B2E
    470E8593 FAB3DD58 3220438A 77E66A34 91E2B5CE 354675CE


Key is
                                          134FCABB 870576F9
    E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


V is
                      3220438A 77E66A34 91E2B5CE 354675CE
```

```
---------------------------------------------------------------

First call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    additional_input is  <empty>

---------------------------

  Update

    provided_data is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    ------------

      While loop

      Key is
                                            134FCABB 870576F9
        E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


      V is
                          3220438A 77E66A34 91E2B5CE 354675CF
```

```
  output_block is
                      5DE6AA50 022F01DF 045B3FDA 58A2AD77

  temp is
                      5DE6AA50 022F01DF 045B3FDA 58A2AD77

------------

  While loop

  Key is
                                          134FCABB 870576F9
    E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58

  V is
                      3220438A 77E66A34 91E2B5CE 354675D0

  output_block is
                      9132F66F B04CE0C2 B0FA0721 F686D3E4

  temp is
                                          5DE6AA50 022F01DF
    045B3FDA 58A2AD77 9132F66F B04CE0C2 B0FA0721 F686D3E4

------------

  While loop

  Key is
                                          134FCABB 870576F9
    E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58

  V is
                      3220438A 77E66A34 91E2B5CE 354675D1

  output_block is
                      79B18865 9E08DC83 10050D9A 2EB958DF
```

```
      temp is
        5DE6AA50 022F01DF 045B3FDA 58A2AD77 9132F66F B04CE0C2
        B0FA0721 F686D3E4 79B18865 9E08DC83 10050D9A 2EB958DF


    temp XOR provided_data is
        DD6728D3 86AA8758 8CD2B551 D42F23F8 01A364FC 24D97655
        28639DBA 6A1B4D7B D9102AC6 3AAD7A24 B8ACA731 8214F670


    Key is
                                            DD6728D3 86AA8758
        8CD2B551 D42F23F8 01A364FC 24D97655 28639DBA 6A1B4D7B


    V is
                          D9102AC6 3AAD7A24 B8ACA731 8214F670


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                                            DD6728D3 86AA8758
        8CD2B551 D42F23F8 01A364FC 24D97655 28639DBA 6A1B4D7B
```

```
  V is
                      D9102AC6 3AAD7A24 B8ACA731 8214F673

  output_block is
                      11B6D033 090305B8 189EC43F 14921586

  temp is
                      11B6D033 090305B8 189EC43F 14921586

------------

  While loop

  Key is
                                          DD6728D3 86AA8758
    8CD2B551 D42F23F8 01A364FC 24D97655 28639DBA 6A1B4D7B

  V is
                      D9102AC6 3AAD7A24 B8ACA731 8214F674

  output_block is
                      B2430E0C 27B8117A 155C0F24 4FAFF785

  temp is
                                          11B6D033 090305B8
    189EC43F 14921586 B2430E0C 27B8117A 155C0F24 4FAFF785

------------

  While loop

  Key is
                                          DD6728D3 86AA8758
    8CD2B551 D42F23F8 01A364FC 24D97655 28639DBA 6A1B4D7B

  V is
                      D9102AC6 3AAD7A24 B8ACA731 8214F675
```

```
      output_block is
                           659E02E3 3674432B E02B26C7 CFC5F21E


      temp is
        11B6D033 090305B8 189EC43F 14921586 B2430E0C 27B8117A
        155C0F24 4FAFF785 659E02E3 3674432B E02B26C7 CFC5F21E


    temp XOR provided_data is
        11B6D033 090305B8 189EC43F 14921586 B2430E0C 27B8117A
        155C0F24 4FAFF785 659E02E3 3674432B E02B26C7 CFC5F21E


    Key is
                                              11B6D033 090305B8
        189EC43F 14921586 B2430E0C 27B8117A 155C0F24 4FAFF785


    V is
                           659E02E3 3674432B E02B26C7 CFC5F21E


rnd_val is
                                              1CD51D0A A03AA992
        782B53B5 96297930 DD0541DC 3B05C9AD 35998E53 DB960664


------------------------------------------------------------

Second call to Generate

**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
**************************************************************

CTR_DRBG_Reseed
```

```
    entropy_input is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    additional_input is  <empty>

---------------------------

  Update

    provided_data is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    ------------

      While loop

      Key is
                                              11B6D033 090305B8
        189EC43F 14921586 B2430E0C 27B8117A 155C0F24 4FAFF785


      V is
                           659E02E3 3674432B E02B26C7 CFC5F21F


      output_block is
                           08D669B0 3A7A8061 B04F770F E270384C


      temp is
                           08D669B0 3A7A8061 B04F770F E270384C


    ------------

      While loop

      Key is
                                              11B6D033 090305B8
        189EC43F 14921586 B2430E0C 27B8117A 155C0F24 4FAFF785
```

```
  V is
                      659E02E3 3674432B E02B26C7 CFC5F220


  output_block is
                      DD6A1359 4038AEC7 272E7C58 EA864D02


  temp is
                                           08D669B0 3A7A8061
    B04F770F E270384C DD6A1359 4038AEC7 272E7C58 EA864D02


------------

  While loop

  Key is
                                           11B6D033 090305B8
    189EC43F 14921586 B2430E0C 27B8117A 155C0F24 4FAFF785


  V is
                      659E02E3 3674432B E02B26C7 CFC5F221


  output_block is
                      D08EB2D1 33BF2A6E 1B19F017 F38518D3


  temp is
    08D669B0 3A7A8061 B04F770F E270384C DD6A1359 4038AEC7
    272E7C58 EA864D02 D08EB2D1 33BF2A6E 1B19F017 F38518D3


temp XOR provided_data is
    C817AB73 FEBF46A6 7886BDC4 2EBDF683 0DBBC18A 94ED7810
    FFF7A683 365B93DD 306F5032 D75ACC89 F3F01AFC 1F68F63C


Key is
                                           C817AB73 FEBF46A6
    7886BDC4 2EBDF683 0DBBC18A 94ED7810 FFF7A683 365B93DD
```

```
    V is
                          306F5032 D75ACC89 F3F01AFC 1F68F63C

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                                              C817AB73 FEBF46A6
        7886BDC4 2EBDF683 0DBBC18A 94ED7810 FFF7A683 365B93DD


      V is
                          306F5032 D75ACC89 F3F01AFC 1F68F63F


      output_block is
                          3E94A310 16B2A5FE 650AA422 DB996CD9


      temp is
                          3E94A310 16B2A5FE 650AA422 DB996CD9


    ------------

      While loop
```

```
  Key is
                                        C817AB73 FEBF46A6
    7886BDC4 2EBDF683 0DBBC18A 94ED7810 FFF7A683 365B93DD


  V is
                      306F5032 D75ACC89 F3F01AFC 1F68F640


  output_block is
                      1E261052 E88E88C5 D7A9FC48 35597270


  temp is
                                        3E94A310 16B2A5FE
    650AA422 DB996CD9 1E261052 E88E88C5 D7A9FC48 35597270


------------

  While loop

  Key is
                                        C817AB73 FEBF46A6
    7886BDC4 2EBDF683 0DBBC18A 94ED7810 FFF7A683 365B93DD


  V is
                      306F5032 D75ACC89 F3F01AFC 1F68F641


  output_block is
                      BC908518 2245456E 639DA7BA BDD8723E


  temp is
    3E94A310 16B2A5FE 650AA422 DB996CD9 1E261052 E88E88C5
    D7A9FC48 35597270 BC908518 2245456E 639DA7BA BDD8723E


temp XOR provided_data is
    3E94A310 16B2A5FE 650AA422 DB996CD9 1E261052 E88E88C5
    D7A9FC48 35597270 BC908518 2245456E 639DA7BA BDD8723E


Key is
```

                                                3E94A310 16B2A5FE
        650AA422 DB996CD9 1E261052 E88E88C5 D7A9FC48 35597270

    V is
                            BC908518 2245456E 639DA7BA BDD8723E

rnd_val is
                                                3A4E58FC 06DD9AAB
        B85480E7 896AF882 0B43F969 FDC38628 EBA7F06C D9A063D8

##

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F

    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF

    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF

    PersonalizationString =
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F

    AdditionalInput1 =
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F

    AdditionalInput2 =

```
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Update

    provided_data is
        40404040 40404040 40404040 40404040 40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


    ------------

      While loop

      Key is
                                              00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001


      output_block is
                           530F8AFB C74536B9 A963B4F1 C4CB738B
```

```
  temp is
                      530F8AFB C74536B9 A963B4F1 C4CB738B


------------

  While loop

  Key is
                                              00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000002


  output_block is
                      CEA7403D 4D606B6E 074EC5D3 BAF39D18


  temp is
                                              530F8AFB C74536B9
    A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18


------------

  While loop

  Key is
                                              00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000003


  output_block is
                      726003CA 37A62A74 D1A2F58E 7506358E


  temp is
```

```
        530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
        074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


    temp XOR provided_data is
        134FCABB 870576F9 E923F4B1 848B33CB 8EE7007D 0D202B2E
        470E8593 FAB3DD58 3220438A 77E66A34 91E2B5CE 354675CE


    Key is
                                           134FCABB 870576F9
        E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


    V is
                           3220438A 77E66A34 91E2B5CE 354675CE


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


Generate FAILED: Reseed is required
*************************************************************

CTR_DRBG_Reseed

    entropy_input is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F
```

```
---------------------------

  Update

    provided_data is
        E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0
        E0E0E0E0 E0E0E0E0 20202020 20202020 20202020 20202020


    ------------

      While loop

      Key is
                                              134FCABB 870576F9
        E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


      V is
                           3220438A 77E66A34 91E2B5CE 354675CF


      output_block is
                           5DE6AA50 022F01DF 045B3FDA 58A2AD77


      temp is
                           5DE6AA50 022F01DF 045B3FDA 58A2AD77


    ------------

      While loop

      Key is
                                              134FCABB 870576F9
        E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


      V is
                           3220438A 77E66A34 91E2B5CE 354675D0


      output_block is
```

```
                        9132F66F B04CE0C2 B0FA0721 F686D3E4


      temp is
                                              5DE6AA50 022F01DF
        045B3FDA 58A2AD77 9132F66F B04CE0C2 B0FA0721 F686D3E4


    ------------

      While loop

      Key is
                                              134FCABB 870576F9
        E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


      V is
                        3220438A 77E66A34 91E2B5CE 354675D1


      output_block is
                        79B18865 9E08DC83 10050D9A 2EB958DF


      temp is
        5DE6AA50 022F01DF 045B3FDA 58A2AD77 9132F66F B04CE0C2
        B0FA0721 F686D3E4 79B18865 9E08DC83 10050D9A 2EB958DF


    temp XOR provided_data is
        BD064AB0 E2CFE13F E4BBDF3A B8424D97 71D2168F 50AC0022
        501AE7C1 16663304 5991A845 BE28FCA3 30252DBA 0E9978FF


    Key is
                                              BD064AB0 E2CFE13F
        E4BBDF3A B8424D97 71D2168F 50AC0022 501AE7C1 16663304


    V is
                        5991A845 BE28FCA3 30252DBA 0E9978FF

**************************************************************
```

```
CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                                              BD064AB0 E2CFE13F
        E4BBDF3A B8424D97 71D2168F 50AC0022 501AE7C1 16663304


      V is
                           5991A845 BE28FCA3 30252DBA 0E997902


      output_block is
                           0D3F8C6B 2BE6683F 042281B8 78AA03F3


      temp is
                           0D3F8C6B 2BE6683F 042281B8 78AA03F3


    ------------

      While loop

      Key is
                                              BD064AB0 E2CFE13F
        E4BBDF3A B8424D97 71D2168F 50AC0022 501AE7C1 16663304


      V is
```

```
                      5991A845 BE28FCA3 30252DBA 0E997903


  output_block is
                      0778915B 5E4D27D4 D637F72A 8B3AD309


  temp is
                                        0D3F8C6B 2BE6683F
    042281B8 78AA03F3 0778915B 5E4D27D4 D637F72A 8B3AD309


------------

  While loop

  Key is
                                        BD064AB0 E2CFE13F
    E4BBDF3A B8424D97 71D2168F 50AC0022 501AE7C1 16663304


  V is
                      5991A845 BE28FCA3 30252DBA 0E997904


  output_block is
                      0B6551E1 680E4908 FEAF5E04 F71DABD4


  temp is
    0D3F8C6B 2BE6683F 042281B8 78AA03F3 0778915B 5E4D27D4
    D637F72A 8B3AD309 0B6551E1 680E4908 FEAF5E04 F71DABD4


temp XOR provided_data is
    0D3F8C6B 2BE6683F 042281B8 78AA03F3 0778915B 5E4D27D4
    D637F72A 8B3AD309 0B6551E1 680E4908 FEAF5E04 F71DABD4


Key is
                                        0D3F8C6B 2BE6683F
    042281B8 78AA03F3 0778915B 5E4D27D4 D637F72A 8B3AD309


V is
                      0B6551E1 680E4908 FEAF5E04 F71DABD4
```

```
rnd_val is
                                                DBAFEF48 988EF939
        5298F5E3 4CF7A6A4 FBD2256C 52A8C8C7 80B848BB B90EA521


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


Generate FAILED: Reseed is required
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


---------------------------

  Update

    provided_data is
        60606060 60606060 60606060 60606060 60606060 60606060
        60606060 60606060 20202020 20202020 20202020 20202020
```

```
------------

  While loop

  Key is
                                          0D3F8C6B 2BE6683F
    042281B8 78AA03F3 0778915B 5E4D27D4 D637F72A 8B3AD309


  V is
                     0B6551E1 680E4908 FEAF5E04 F71DABD5


  output_block is
                     13E83086 24D57354 0A188423 C5CBFFBA


  temp is
                     13E83086 24D57354 0A188423 C5CBFFBA


------------

  While loop

  Key is
                                          0D3F8C6B 2BE6683F
    042281B8 78AA03F3 0778915B 5E4D27D4 D637F72A 8B3AD309


  V is
                     0B6551E1 680E4908 FEAF5E04 F71DABD6


  output_block is
                     901788F6 86854925 9ACC8A66 A8681F0C


  temp is
                                          13E83086 24D57354
    0A188423 C5CBFFBA 901788F6 86854925 9ACC8A66 A8681F0C


------------

  While loop
```

```
      Key is
                                            0D3F8C6B 2BE6683F
        042281B8 78AA03F3 0778915B 5E4D27D4 D637F72A 8B3AD309


      V is
                          0B6551E1 680E4908 FEAF5E04 F71DABD7


      output_block is
                          8DC5475B B6CC802F E14CD960 C78DCBF6


      temp is
        13E83086 24D57354 0A188423 C5CBFFBA 901788F6 86854925
        9ACC8A66 A8681F0C 8DC5475B B6CC802F E14CD960 C78DCBF6


    temp XOR provided_data is
        738850E6 44B51334 6A78E443 A5AB9FDA F077E896 E6E52945
        FAACEA06 C8087F6C ADE5677B 96ECA00F C16CF940 E7ADEBD6


    Key is
                                            738850E6 44B51334
        6A78E443 A5AB9FDA F077E896 E6E52945 FAACEA06 C8087F6C


    V is
                          ADE5677B 96ECA00F C16CF940 E7ADEBD6


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
```

```
    00000000 00000000 00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


------------

  While loop

  Key is
                                          738850E6 44B51334
    6A78E443 A5AB9FDA F077E896 E6E52945 FAACEA06 C8087F6C


  V is
                      ADE5677B 96ECA00F C16CF940 E7ADEBD9


  output_block is
                      AA2DB253 D141A408 B1CF00B2 05C7FB66


  temp is
                      AA2DB253 D141A408 B1CF00B2 05C7FB66


------------

  While loop

  Key is
                                          738850E6 44B51334
    6A78E443 A5AB9FDA F077E896 E6E52945 FAACEA06 C8087F6C


  V is
                      ADE5677B 96ECA00F C16CF940 E7ADEBDA


  output_block is
                      E7AEF3D0 0C992E32 B2BB091A 1A6D90AA


  temp is
                                          AA2DB253 D141A408
    B1CF00B2 05C7FB66 E7AEF3D0 0C992E32 B2BB091A 1A6D90AA
```

```
    ------------

      While loop

      Key is
                                              738850E6 44B51334
        6A78E443 A5AB9FDA F077E896 E6E52945 FAACEA06 C8087F6C


      V is
                           ADE5677B 96ECA00F C16CF940 E7ADEBDB


      output_block is
                           B58E18F1 C55434A6 30E81E94 74855E7C


      temp is
        AA2DB253 D141A408 B1CF00B2 05C7FB66 E7AEF3D0 0C992E32
        B2BB091A 1A6D90AA B58E18F1 C55434A6 30E81E94 74855E7C


    temp XOR provided_data is
        AA2DB253 D141A408 B1CF00B2 05C7FB66 E7AEF3D0 0C992E32
        B2BB091A 1A6D90AA B58E18F1 C55434A6 30E81E94 74855E7C


    Key is
                                              AA2DB253 D141A408
        B1CF00B2 05C7FB66 E7AEF3D0 0C992E32 B2BB091A 1A6D90AA


    V is
                           B58E18F1 C55434A6 30E81E94 74855E7C


rnd_val is
                                              50A6509D 314E1C24
        26ADD435 2D1B3CF4 6C9896F5 7E4148A9 4DBCA894 63F22239
```

```
################################################################

CTR_DRBG

    Requested Security Strength = 112

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    EntropyInput1 (for Reseed1) =
                                                        80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    Nonce =
                                                202122 23242526


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    nonce is
                                                202122 23242526


    personal_str is  <empty>
```

```
    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                                    00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C202122 23242526


    number_of_bits_to_return = 232

    S is
        00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C202122 23242526 80000000


    ------------

      BCC

      IV is
                                               00000000 00000000


      IV || S is
                                               00000000 00000000
        00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C202122 23242526 80000000


    temp is
                                               4A2145C3 52BD4642


    ------------

      BCC

      IV is
                                               00000001 00000000


      IV || S is
```

```
                                          00000001 00000000
    00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C202122 23242526 80000000


temp is
                     4A2145C3 52BD4642 EEB5E70D CAE11D42


------------

  BCC

  IV is
                                          00000002 00000000


  IV || S is
                                          00000002 00000000
    00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C202122 23242526 80000000


temp is
    4A2145C3 52BD4642 EEB5E70D CAE11D42 82FD02F7 B62641C4


------------

  BCC

  IV is
                                          00000003 00000000


  IV || S is
                                          00000003 00000000
    00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C202122 23242526 80000000


temp is
                                          4A2145C3 52BD4642
    EEB5E70D CAE11D42 82FD02F7 B62641C4 BAE575D6 E7411566
```

```
    ------------

    Key is
              4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6


    X is
                                            2641C4BA E575D6E7


Block #1
Blockin   2641C4BA E575D6E7
Blockout  B4300B8B 7D547B40

    ------------

      BlockEncrypt

      Key is
              4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6


      X is
                                            2641C4BA E575D6E7


      X = BlockEncrypt(Key, X) is
                                            B4300B8B 7D547B40


      temp is
                                            B4300B8B 7D547B40


Block #1
Blockin   B4300B8B 7D547B40
Blockout  599CFD0E B13B1607

    ------------

      BlockEncrypt

      Key is
              4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6
```

```
      X is
                                          B4300B8B 7D547B40


      X = BlockEncrypt(Key, X) is
                                          599CFD0E B13B1607


      temp is
                          B4300B8B 7D547B40 599CFD0E B13B1607


Block #1
Blockin   599CFD0E B13B1607
Blockout  2398EF59 1553A5A3

    ------------

      BlockEncrypt

      Key is
              4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6


      X is
                                          599CFD0E B13B1607


      X = BlockEncrypt(Key, X) is
                                          2398EF59 1553A5A3


      temp is
        B4300B8B 7D547B40 599CFD0E B13B1607 2398EF59 1553A5A3


Block #1
Blockin   2398EF59 1553A5A3
Blockout  A10292FE FE535642

    ------------

      BlockEncrypt

      Key is
              4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6
```

```
      X is
                                              2398EF59 1553A5A3

      X = BlockEncrypt(Key, X) is
                                              A10292FE FE535642

      temp is
                                              B4300B8B 7D547B40
        599CFD0E B13B1607 2398EF59 1553A5A3 A10292FE FE535642

      requested_bits is
                                                    B4 300B8B7D
        547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE

    seed_material is
                                                    B4 300B8B7D
        547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE

---------------------------

  Update

    provided_data is
                                                    B4 300B8B7D
        547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE

    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000

      V is
                                              00000000 00000001
```

```
Block #1
Blockin   00000000 00000001
Blockout  166B40B4 4ABA4BD6

      output_block is
                                              166B40B4 4ABA4BD6


      temp is
                                              166B40B4 4ABA4BD6


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000002


Block #1
Blockin   00000000 00000002
Blockout  06E7EA22 CE92708F

      output_block is
                                              06E7EA22 CE92708F


      temp is
                           166B40B4 4ABA4BD6 06E7EA22 CE92708F


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000003
```

```
Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                              4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000004


Block #1
Blockin   00000000 00000004
Blockout  D2FD8867 D50D2DFE

      output_block is
                                              D2FD8867 D50D2DFE


      temp is
                                              166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                    A2 5B4B3F37
        EE30965F 7B172C7F A966886D 297F90B7 A9B33F73 FF1A992B


    Key is
              A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7
```

```
    V is
                                                A9B33F73 FF1A992B

------------------------------------------------------------

First call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   A9B33F73 FF1A992C
Blockout  ABC88224 514D0316

Block #1
Blockin   A9B33F73 FF1A992D
Blockout  EA3D48AE E3C9A2B4

---------------------------

  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7


      V is
                                                A9B33F73 FF1A992E
```

```
Block #1
Blockin   A9B33F73 FF1A992E
Blockout  27CE2546 E5F9CE73

      output_block is
                                              27CE2546 E5F9CE73


      temp is
                                              27CE2546 E5F9CE73


    ------------

      While loop

      Key is
              A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7


      V is
                                              A9B33F73 FF1A992F


Block #1
Blockin   A9B33F73 FF1A992F
Blockout  AC843CE9 A9F8B369

      output_block is
                                              AC843CE9 A9F8B369


      temp is
                           27CE2546 E5F9CE73 AC843CE9 A9F8B369


    ------------

      While loop

      Key is
              A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7


      V is
```

A9B33F73 FF1A9930

Block #1
Blockin   A9B33F73 FF1A9930
Blockout D6053CD6 D4543E9B

output_block is
D6053CD6 D4543E9B

temp is
27CE2546 E5F9CE73 AC843CE9 A9F8B369 D6053CD6 D4543E9B

While loop

Key is
A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7

V is
A9B33F73 FF1A9931

Block #1
Blockin   A9B33F73 FF1A9931
Blockout CF882969 5162BE82

output_block is
CF882969 5162BE82

temp is
27CE2546 E5F9CE73
AC843CE9 A9F8B369 D6053CD6 D4543E9B CF882969 5162BE82

temp XOR provided_data is
27 CE2546E5
F9CE73AC 843CE9A9 F8B369D6 053CD6D4 543E9BCF 88296951

Key is

```
              27 CE2546E5 F9CE73AC 843CE9A9 F8B369D6 053CD6D4

    V is
                                            543E9BCF 88296951

rnd_val is
                          ABC88224 514D0316 EA3D48AE E3C9A2B4

---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   543E9BCF 88296952
Blockout  D3D3F372 E43E7ABD

Block #1
Blockin   543E9BCF 88296953
Blockout  C4FA2937 43EED076

---------------------------

  Update

    provided_data is
                                                      00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              27 CE2546E5 F9CE73AC 843CE9A9 F8B369D6 053CD6D4
```

```
      V is
                                                543E9BCF 88296954


Block #1
Blockin   543E9BCF 88296954
Blockout  4966D8DE 011D2169

      output_block is
                                                4966D8DE 011D2169


      temp is
                                                4966D8DE 011D2169


    ------------

      While loop

      Key is
              27 CE2546E5 F9CE73AC 843CE9A9 F8B369D6 053CD6D4


      V is
                                                543E9BCF 88296955


Block #1
Blockin   543E9BCF 88296955
Blockout  D0EA8DCA 25F59A82

      output_block is
                                                D0EA8DCA 25F59A82


      temp is
                           4966D8DE 011D2169 D0EA8DCA 25F59A82


    ------------

      While loop
```

```
      Key is
              27 CE2546E5 F9CE73AC 843CE9A9 F8B369D6 053CD6D4


      V is
                                              543E9BCF 88296956


Block #1
Blockin   543E9BCF 88296956
Blockout  9C246045 E5453E30

      output_block is
                                              9C246045 E5453E30


      temp is
        4966D8DE 011D2169 D0EA8DCA 25F59A82 9C246045 E5453E30


    ------------

      While loop

      Key is
              27 CE2546E5 F9CE73AC 843CE9A9 F8B369D6 053CD6D4


      V is
                                              543E9BCF 88296957


Block #1
Blockin   543E9BCF 88296957
Blockout  6D98529D 4CF1B0A6

      output_block is
                                              6D98529D 4CF1B0A6


      temp is
                                              4966D8DE 011D2169
        D0EA8DCA 25F59A82 9C246045 E5453E30 6D98529D 4CF1B0A6


    temp XOR provided_data is
```

                                                    49 66D8DE01
        1D2169D0 EA8DCA25 F59A829C 246045E5 453E306D 98529D4C

    Key is
              49 66D8DE01 1D2169D0 EA8DCA25 F59A829C 246045E5

    V is
                                            453E306D 98529D4C

rnd_val is
                          D3D3F372 E43E7ABD C4FA2937 43EED076

###

CTR_DRBG

    Requested Security Strength = 112

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                    00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C

    EntropyInput1 (for Reseed1) =
                                                    80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C

    EntropyInput2 (for Reseed2) =
                                                    C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC

    Nonce =
                                                202122 23242526

    PersonalizationString = <empty>

    AdditionalInput1 =
                                                    60 61626364

```
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


    AdditionalInput2 =
                                                        A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


################################################################

****************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    nonce is
                                                202122 23242526


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                                     00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C202122 23242526


    number_of_bits_to_return = 232

    S is
        00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C202122 23242526 80000000


    ------------

      BCC
```

```
  IV is
                                        00000000 00000000


  IV || S is
                                        00000000 00000000
    00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C202122 23242526 80000000


temp is
                                        4A2145C3 52BD4642


------------

  BCC

  IV is
                                        00000001 00000000


  IV || S is
                                        00000001 00000000
    00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C202122 23242526 80000000


temp is
                     4A2145C3 52BD4642 EEB5E70D CAE11D42


------------

  BCC

  IV is
                                        00000002 00000000


  IV || S is
                                        00000002 00000000
    00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C202122 23242526 80000000
```

```
    temp is
        4A2145C3 52BD4642 EEB5E70D CAE11D42 82FD02F7 B62641C4


    ------------

      BCC

      IV is
                                              00000003 00000000


      IV || S is
                                              00000003 00000000
        00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C202122 23242526 80000000


    temp is
                                              4A2145C3 52BD4642
        EEB5E70D CAE11D42 82FD02F7 B62641C4 BAE575D6 E7411566


    ------------

    Key is
              4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6


    X is
                                              2641C4BA E575D6E7


Block #1
Blockin   2641C4BA E575D6E7
Blockout  B4300B8B 7D547B40

    ------------

      BlockEncrypt

      Key is
              4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6
```

```
      X is
                                          2641C4BA E575D6E7

      X = BlockEncrypt(Key, X) is
                                          B4300B8B 7D547B40

      temp is
                                          B4300B8B 7D547B40


Block #1
Blockin   B4300B8B 7D547B40
Blockout  599CFD0E B13B1607

    ------------

      BlockEncrypt

      Key is
              4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

      X is
                                          B4300B8B 7D547B40

      X = BlockEncrypt(Key, X) is
                                          599CFD0E B13B1607

      temp is
                          B4300B8B 7D547B40 599CFD0E B13B1607


Block #1
Blockin   599CFD0E B13B1607
Blockout  2398EF59 1553A5A3

    ------------

      BlockEncrypt

      Key is
              4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6
```

```
      X is
                                              599CFD0E B13B1607


      X = BlockEncrypt(Key, X) is
                                              2398EF59 1553A5A3


      temp is
        B4300B8B 7D547B40 599CFD0E B13B1607 2398EF59 1553A5A3


Block #1
Blockin   2398EF59 1553A5A3
Blockout  A10292FE FE535642

    ------------

      BlockEncrypt

      Key is
              4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6


      X is
                                              2398EF59 1553A5A3


      X = BlockEncrypt(Key, X) is
                                              A10292FE FE535642


      temp is
                                              B4300B8B 7D547B40
        599CFD0E B13B1607 2398EF59 1553A5A3 A10292FE FE535642


      requested_bits is
                                                    B4 300B8B7D
        547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE


    seed_material is
                                                    B4 300B8B7D
```

```
        547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE


---------------------------

  Update

    provided_data is
                                                        B4 300B8B7D
        547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                           00000000 00000001


Block #1
Blockin   00000000 00000001
Blockout  166B40B4 4ABA4BD6

      output_block is
                                           166B40B4 4ABA4BD6


      temp is
                                           166B40B4 4ABA4BD6


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                           00000000 00000002
```

```
Block #1
Blockin   00000000 00000002
Blockout  06E7EA22 CE92708F

      output_block is
                                            06E7EA22 CE92708F


      temp is
                          166B40B4 4ABA4BD6 06E7EA22 CE92708F


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                            00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                            4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000
```

```
      V is
                                                00000000 00000004


Block #1
Blockin   00000000 00000004
Blockout  D2FD8867 D50D2DFE

      output_block is
                                                D2FD8867 D50D2DFE


      temp is
                                                166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                      A2 5B4B3F37
        EE30965F 7B172C7F A966886D 297F90B7 A9B33F73 FF1A992B


    Key is
              A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7


    V is
                                                A9B33F73 FF1A992B


------------------------------------------------------------

First call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                      60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


  additional_input <> NULL, process appropriately
```

```
---------------------------

  Block_Cipher_df

    input_str is
                                                        60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


    number_of_bits_to_return = 232

    S is
                           0000001D 0000001D 60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C800000


    ------------

      BCC

      IV is
                                               00000000 00000000


      IV || S is
        00000000 00000000 0000001D 0000001D 60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C800000


    temp is
                                               A9DAAC27 BD128BB4


    ------------

      BCC

      IV is
                                               00000001 00000000


      IV || S is
        00000001 00000000 0000001D 0000001D 60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C800000
```

```
temp is
                    A9DAAC27 BD128BB4 08EB0C8C 15DB001C


------------

  BCC

  IV is
                                        00000002 00000000


  IV || S is
    00000002 00000000 0000001D 0000001D 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C800000


temp is
    A9DAAC27 BD128BB4 08EB0C8C 15DB001C 68175B62 9929DBB3


------------

  BCC

  IV is
                                        00000003 00000000


  IV || S is
    00000003 00000000 0000001D 0000001D 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C800000


temp is
                                        A9DAAC27 BD128BB4
    08EB0C8C 15DB001C 68175B62 9929DBB3 EBF330CD 6977A3C0


------------

Key is
          A9 DAAC27BD 128BB408 EB0C8C15 DB001C68 175B6299


X is
```

```
                                        29DBB3EB F330CD69


Block #1
Blockin   29DBB3EB F330CD69
Blockout  68099422 99837788

    ------------

      BlockEncrypt

      Key is
              A9 DAAC27BD 128BB408 EB0C8C15 DB001C68 175B6299


      X is
                                        29DBB3EB F330CD69


      X = BlockEncrypt(Key, X) is
                                        68099422 99837788


      temp is
                                        68099422 99837788


Block #1
Blockin   68099422 99837788
Blockout  1665F614 303AD2C0

    ------------

      BlockEncrypt

      Key is
              A9 DAAC27BD 128BB408 EB0C8C15 DB001C68 175B6299


      X is
                                        68099422 99837788


      X = BlockEncrypt(Key, X) is
                                        1665F614 303AD2C0
```

```
      temp is
                          68099422 99837788 1665F614 303AD2C0


Block #1
Blockin   1665F614 303AD2C0
Blockout  3EEA906C 48996C3C

    ------------

      BlockEncrypt

      Key is
              A9 DAAC27BD 128BB408 EB0C8C15 DB001C68 175B6299


      X is
                                            1665F614 303AD2C0


      X = BlockEncrypt(Key, X) is
                                            3EEA906C 48996C3C


      temp is
        68099422 99837788 1665F614 303AD2C0 3EEA906C 48996C3C


Block #1
Blockin   3EEA906C 48996C3C
Blockout  22131B5A 94AF9E8C

    ------------

      BlockEncrypt

      Key is
              A9 DAAC27BD 128BB408 EB0C8C15 DB001C68 175B6299


      X is
                                            3EEA906C 48996C3C


      X = BlockEncrypt(Key, X) is
```

```
                                                  22131B5A 94AF9E8C


      temp is
                                                  68099422 99837788
        1665F614 303AD2C0 3EEA906C 48996C3C 22131B5A 94AF9E8C


      requested_bits is
                                                        68 09942299
        83778816 65F61430 3AD2C03E EA906C48 996C3C22 131B5A94


---------------------------

  Update

    provided_data is
                                                        68 09942299
        83778816 65F61430 3AD2C03E EA906C48 996C3C22 131B5A94


    ------------

      While loop

      Key is
              A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7


      V is
                                                  A9B33F73 FF1A992C


Block #1
Blockin   A9B33F73 FF1A992C
Blockout  ABC88224 514D0316

      output_block is
                                                  ABC88224 514D0316


      temp is
                                                  ABC88224 514D0316
```

```
    ------------

      While loop

      Key is
              A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7


      V is
                                            A9B33F73 FF1A992D


Block #1
Blockin   A9B33F73 FF1A992D
Blockout  EA3D48AE E3C9A2B4

      output_block is
                                            EA3D48AE E3C9A2B4


      temp is
                           ABC88224 514D0316 EA3D48AE E3C9A2B4


    ------------

      While loop

      Key is
              A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7


      V is
                                            A9B33F73 FF1A992E


Block #1
Blockin   A9B33F73 FF1A992E
Blockout  27CE2546 E5F9CE73

      output_block is
                                            27CE2546 E5F9CE73


      temp is
        ABC88224 514D0316 EA3D48AE E3C9A2B4 27CE2546 E5F9CE73
```

```
    ------------

      While loop

      Key is
              A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7


      V is
                                              A9B33F73 FF1A992F


Block #1
Blockin   A9B33F73 FF1A992F
Blockout  AC843CE9 A9F8B369

      output_block is
                                              AC843CE9 A9F8B369


      temp is
                                              ABC88224 514D0316
        EA3D48AE E3C9A2B4 27CE2546 E5F9CE73 AC843CE9 A9F8B369


    temp XOR provided_data is
                                                    C3 C11606C8
        CE749EFC 58BEBAD3 F3707419 24B52AAD 60A24F8E 9727B33D


    Key is
              C3 C11606C8 CE749EFC 58BEBAD3 F3707419 24B52AAD


    V is
                                              60A24F8E 9727B33D


Block #1
Blockin   60A24F8E 9727B33E
Blockout  D4564EE0 72ACA5BD

Block #1
Blockin   60A24F8E 9727B33F
```

```
Blockout  279536E1 4F94CB12

---------------------------

  Update

    provided_data is
                                                        68 09942299
        83778816 65F61430 3AD2C03E EA906C48 996C3C22 131B5A94


    ------------

      While loop

      Key is
              C3 C11606C8 CE749EFC 58BEBAD3 F3707419 24B52AAD


      V is
                                            60A24F8E 9727B340


Block #1
Blockin   60A24F8E 9727B340
Blockout  22066DF2 B2647580

      output_block is
                                            22066DF2 B2647580


      temp is
                                            22066DF2 B2647580


    ------------

      While loop

      Key is
              C3 C11606C8 CE749EFC 58BEBAD3 F3707419 24B52AAD


      V is
                                            60A24F8E 9727B341
```

```
Block #1
Blockin   60A24F8E 9727B341
Blockout  8F2219FC 67C1EF3F

      output_block is
                                            8F2219FC 67C1EF3F


      temp is
                          22066DF2 B2647580 8F2219FC 67C1EF3F


    ------------

      While loop

      Key is
              C3 C11606C8 CE749EFC 58BEBAD3 F3707419 24B52AAD


      V is
                                            60A24F8E 9727B342


Block #1
Blockin   60A24F8E 9727B342
Blockout  A78B1FEF 0CC07F38

      output_block is
                                            A78B1FEF 0CC07F38


      temp is
        22066DF2 B2647580 8F2219FC 67C1EF3F A78B1FEF 0CC07F38


    ------------

      While loop

      Key is
              C3 C11606C8 CE749EFC 58BEBAD3 F3707419 24B52AAD


      V is
```

```
                                          60A24F8E 9727B343


Block #1
Blockin   60A24F8E 9727B343
Blockout  EBF91126 56BE9085

      output_block is
                                          EBF91126 56BE9085


      temp is
                                          22066DF2 B2647580
        8F2219FC 67C1EF3F A78B1FEF 0CC07F38 EBF91126 56BE9085


    temp XOR provided_data is
                                                    4A 0FF9D02B
        E7020899 47EFE857 FB3DFF99 618F8344 591304C9 EA0A7CC2


    Key is
              4A 0FF9D02B E7020899 47EFE857 FB3DFF99 618F8344


    V is
                                          591304C9 EA0A7CC2


rnd_val is
                         D4564EE0 72ACA5BD 279536E1 4F94CB12


------------------------------------------------------------

Second call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                    A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC
```

```
  additional_input <> NULL, process appropriately
---------------------------

  Block_Cipher_df

    input_str is
                                                        A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


    number_of_bits_to_return = 232

    S is
                          0000001D 0000001D A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BC800000


    ------------

      BCC

      IV is
                                               00000000 00000000


      IV || S is
        00000000 00000000 0000001D 0000001D A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BC800000


    temp is
                                               89213498 76E519BE


    ------------

      BCC

      IV is
                                               00000001 00000000


      IV || S is
        00000001 00000000 0000001D 0000001D A0A1A2A3 A4A5A6A7
```

```
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BC800000


temp is
                     89213498 76E519BE FC10164B 5A8722CE


------------

  BCC

  IV is
                                          00000002 00000000


  IV || S is
    00000002 00000000 0000001D 0000001D A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BC800000


temp is
    89213498 76E519BE FC10164B 5A8722CE 5C92E9C1 6F213C22


------------

  BCC

  IV is
                                          00000003 00000000


  IV || S is
    00000003 00000000 0000001D 0000001D A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BC800000


temp is
                                          89213498 76E519BE
    FC10164B 5A8722CE 5C92E9C1 6F213C22 9B946180 1B6BAA48


------------

Key is
          89 21349876 E519BEFC 10164B5A 8722CE5C 92E9C16F
```

```
    X is
                                            213C229B 9461801B


Block #1
Blockin   213C229B 9461801B
Blockout  07669398 0A486518

    ------------

      BlockEncrypt

      Key is
              89 21349876 E519BEFC 10164B5A 8722CE5C 92E9C16F


      X is
                                            213C229B 9461801B


      X = BlockEncrypt(Key, X) is
                                            07669398 0A486518


      temp is
                                            07669398 0A486518


Block #1
Blockin   07669398 0A486518
Blockout  DC19FECA F56EF259

    ------------

      BlockEncrypt

      Key is
              89 21349876 E519BEFC 10164B5A 8722CE5C 92E9C16F


      X is
                                            07669398 0A486518
```

```
      X = BlockEncrypt(Key, X) is
                                              DC19FECA F56EF259


      temp is
                           07669398 0A486518 DC19FECA F56EF259


Block #1
Blockin   DC19FECA F56EF259
Blockout  0FF65EF1 FE9A7410

    ------------

      BlockEncrypt

      Key is
              89 21349876 E519BEFC 10164B5A 8722CE5C 92E9C16F


      X is
                                              DC19FECA F56EF259


      X = BlockEncrypt(Key, X) is
                                              0FF65EF1 FE9A7410


      temp is
        07669398 0A486518 DC19FECA F56EF259 0FF65EF1 FE9A7410


Block #1
Blockin   0FF65EF1 FE9A7410
Blockout  8C1FC048 1C36F198

    ------------

      BlockEncrypt

      Key is
              89 21349876 E519BEFC 10164B5A 8722CE5C 92E9C16F


      X is
                                              0FF65EF1 FE9A7410
```

```
      X = BlockEncrypt(Key, X) is
                                              8C1FC048 1C36F198


      temp is
                                              07669398 0A486518
        DC19FECA F56EF259 0FF65EF1 FE9A7410 8C1FC048 1C36F198


      requested_bits is
                                                    07 6693980A
        486518DC 19FECAF5 6EF2590F F65EF1FE 9A74108C 1FC0481C


----------------------------

  Update

    provided_data is
                                                    07 6693980A
        486518DC 19FECAF5 6EF2590F F65EF1FE 9A74108C 1FC0481C


    ------------

      While loop

      Key is
              4A 0FF9D02B E7020899 47EFE857 FB3DFF99 618F8344


      V is
                                              591304C9 EA0A7CC3


Block #1
Blockin   591304C9 EA0A7CC3
Blockout  9635E4B7 B32E5C48

      output_block is
                                              9635E4B7 B32E5C48


      temp is
```

```
                                                9635E4B7 B32E5C48


    ------------

      While loop

      Key is
              4A 0FF9D02B E7020899 47EFE857 FB3DFF99 618F8344


      V is
                                                591304C9 EA0A7CC4


Block #1
Blockin   591304C9 EA0A7CC4
Blockout  282A17EC C27079E4

      output_block is
                                                282A17EC C27079E4


      temp is
                            9635E4B7 B32E5C48 282A17EC C27079E4


    ------------

      While loop

      Key is
              4A 0FF9D02B E7020899 47EFE857 FB3DFF99 618F8344


      V is
                                                591304C9 EA0A7CC5


Block #1
Blockin   591304C9 EA0A7CC5
Blockout  88315A82 0680A9C8

      output_block is
                                                88315A82 0680A9C8
```

```
      temp is
        9635E4B7 B32E5C48 282A17EC C27079E4 88315A82 0680A9C8


    ------------

      While loop

      Key is
              4A 0FF9D02B E7020899 47EFE857 FB3DFF99 618F8344


      V is
                                            591304C9 EA0A7CC6


Block #1
Blockin   591304C9 EA0A7CC6
Blockout  A12A7C65 AE8DFB7F

      output_block is
                                            A12A7C65 AE8DFB7F


      temp is
                                            9635E4B7 B32E5C48
        282A17EC C27079E4 88315A82 0680A9C8 A12A7C65 AE8DFB7F


    temp XOR provided_data is
                                                  91 53772FB9
        663950F4 33E92637 1E8BBD87 C70473F8 1ADDD82D 35BC2DB2


    Key is
              91 53772FB9 663950F4 33E92637 1E8BBD87 C70473F8


    V is
                                            1ADDD82D 35BC2DB2


Block #1
Blockin   1ADDD82D 35BC2DB3
Blockout  1CCD9AFE F15A9679
```

```
Block #1
Blockin   1ADDD82D 35BC2DB4
Blockout  BA75E352 25585DEA

---------------------------

  Update

    provided_data is
                                                        07 6693980A
        486518DC 19FECAF5 6EF2590F F65EF1FE 9A74108C 1FC0481C


    ------------

      While loop

      Key is
              91 53772FB9 663950F4 33E92637 1E8BBD87 C70473F8


      V is
                                              1ADDD82D 35BC2DB5


Block #1
Blockin   1ADDD82D 35BC2DB5
Blockout  36CF2571 806190D4

      output_block is
                                              36CF2571 806190D4


      temp is
                                              36CF2571 806190D4


    ------------

      While loop

      Key is
              91 53772FB9 663950F4 33E92637 1E8BBD87 C70473F8
```

```
      V is
                                              1ADDD82D 35BC2DB6


Block #1
Blockin   1ADDD82D 35BC2DB6
Blockout  BD6179FA AB46D4B0

      output_block is
                                              BD6179FA AB46D4B0


      temp is
                           36CF2571 806190D4 BD6179FA AB46D4B0


    ------------

      While loop

      Key is
              91 53772FB9 663950F4 33E92637 1E8BBD87 C70473F8


      V is
                                              1ADDD82D 35BC2DB7


Block #1
Blockin   1ADDD82D 35BC2DB7
Blockout  A5452BC5 EFC172BE

      output_block is
                                              A5452BC5 EFC172BE


      temp is
        36CF2571 806190D4 BD6179FA AB46D4B0 A5452BC5 EFC172BE


    ------------

      While loop

      Key is
              91 53772FB9 663950F4 33E92637 1E8BBD87 C70473F8
```

```
      V is
                                              1ADDD82D 35BC2DB8


Block #1
Blockin   1ADDD82D 35BC2DB8
Blockout  BAF89D04 7DEF27ED

      output_block is
                                              BAF89D04 7DEF27ED


      temp is
                                              36CF2571 806190D4
        BD6179FA AB46D4B0 A5452BC5 EFC172BE BAF89D04 7DEF27ED


    temp XOR provided_data is
                                                       31 A9B6E98A
        29F5CC61 7887305E 2826E9AA B3753411 5B06AE36 E75D4C61


    Key is
              31 A9B6E98A 29F5CC61 7887305E 2826E9AA B3753411


    V is
                                              5B06AE36 E75D4C61


rnd_val is
                          1CCD9AFE F15A9679 BA75E352 25585DEA


################################################################

CTR_DRBG

    Requested Security Strength = 112

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                       00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C
```

```
    EntropyInput1 (for Reseed1) =
                                                        80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    Nonce =
                                                  202122 23242526


    PersonalizationString =
                                                        40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    AdditionalInput = <empty>

###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    nonce is
                                                  202122 23242526


    personal_str is
                                                        40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    prediction_resistance_flag = "No PredictionResistance"

---------------------------
```

```
Block_Cipher_df

  input_str is
                     00 01020304 05060708 090A0B0C 0D0E0F10
      11121314 15161718 191A1B1C 20212223 24252640 41424344
      45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


  number_of_bits_to_return = 232

  S is
                                           00000041 0000001D
      00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
      18191A1B 1C202122 23242526 40414243 44454647 48494A4B
      4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000


  ------------

    BCC

    IV is
                                           00000000 00000000


    IV || S is
                         00000000 00000000 00000041 0000001D
      00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
      18191A1B 1C202122 23242526 40414243 44454647 48494A4B
      4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000


  temp is
                                           BF5C8905 7D02B0A6


  ------------

    BCC

    IV is
                                           00000001 00000000


    IV || S is
```

```
                     00000001 00000000 00000041 0000001D
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C202122 23242526 40414243 44454647 48494A4B
    4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000


temp is
                     BF5C8905 7D02B0A6 77FE7647 E9554668


------------

  BCC

  IV is
                                         00000002 00000000


  IV || S is
                     00000002 00000000 00000041 0000001D
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C202122 23242526 40414243 44454647 48494A4B
    4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000


temp is
    BF5C8905 7D02B0A6 77FE7647 E9554668 AE4D8DE0 DB992E46


------------

  BCC

  IV is
                                         00000003 00000000


  IV || S is
                     00000003 00000000 00000041 0000001D
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C202122 23242526 40414243 44454647 48494A4B
    4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000


temp is
                                         BF5C8905 7D02B0A6
```

77FE7647 E9554668 AE4D8DE0 DB992E46 83E1389F 33A1E91F

Key is
BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is
992E4683 E1389F33

Block #1
Blockin 992E4683 E1389F33
Blockout 70F9F85E 350177E5

BlockEncrypt

Key is
BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is
992E4683 E1389F33

X = BlockEncrypt(Key, X) is
70F9F85E 350177E5

temp is
70F9F85E 350177E5

Block #1
Blockin 70F9F85E 350177E5
Blockout B228D49C 6374BBB6

BlockEncrypt

Key is

```
              BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

      X is
                                           70F9F85E 350177E5

      X = BlockEncrypt(Key, X) is
                                           B228D49C 6374BBB6

      temp is
                           70F9F85E 350177E5 B228D49C 6374BBB6


Block #1
Blockin   B228D49C 6374BBB6
Blockout  EA3DCFFA 463099CA

    ------------

      BlockEncrypt

      Key is
              BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

      X is
                                           B228D49C 6374BBB6

      X = BlockEncrypt(Key, X) is
                                           EA3DCFFA 463099CA

      temp is
        70F9F85E 350177E5 B228D49C 6374BBB6 EA3DCFFA 463099CA


Block #1
Blockin   EA3DCFFA 463099CA
Blockout  F0781291 15A9A8E8

    ------------

      BlockEncrypt
```

```
      Key is
              BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

      X is
                                             EA3DCFFA 463099CA

      X = BlockEncrypt(Key, X) is
                                             F0781291 15A9A8E8

      temp is
                                             70F9F85E 350177E5
        B228D49C 6374BBB6 EA3DCFFA 463099CA F0781291 15A9A8E8

      requested_bits is
                                                   70 F9F85E35
        0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115

    seed_material is
                                                   70 F9F85E35
        0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115

----------------------------

  Update

    provided_data is
                                                   70 F9F85E35
        0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115

    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000

      V is
```

```
                                          00000000 00000001


Block #1
Blockin   00000000 00000001
Blockout  166B40B4 4ABA4BD6

      output_block is
                                          166B40B4 4ABA4BD6


      temp is
                                          166B40B4 4ABA4BD6


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                          00000000 00000002


Block #1
Blockin   00000000 00000002
Blockout  06E7EA22 CE92708F

      output_block is
                                          06E7EA22 CE92708F


      temp is
                          166B40B4 4ABA4BD6 06E7EA22 CE92708F


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000
```

```
      V is
                                              00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                              4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000004


Block #1
Blockin   00000000 00000004
Blockout  D2FD8867 D50D2DFE

      output_block is
                                              D2FD8867 D50D2DFE


      temp is
                                              166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                    66 92B8EA7F
        BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4 CA8F5622 859AF6C0
```

```
    Key is
              66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4


    V is
                                             CA8F5622 859AF6C0


------------------------------------------------------------

First call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   CA8F5622 859AF6C1
Blockout  760BED7D 92B083B1

Block #1
Blockin   CA8F5622 859AF6C2
Blockout  0AF31CF0 656081EB

---------------------------

  Update

    provided_data is
                                                    00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4
```

```
      V is
                                              CA8F5622 859AF6C3


Block #1
Blockin   CA8F5622 859AF6C3
Blockout  51D241F0 2DA51012

      output_block is
                                              51D241F0 2DA51012


      temp is
                                              51D241F0 2DA51012


    ------------

      While loop

      Key is
              66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4


      V is
                                              CA8F5622 859AF6C4


Block #1
Blockin   CA8F5622 859AF6C4
Blockout  AAF72BA5 971324B4

      output_block is
                                              AAF72BA5 971324B4


      temp is
                           51D241F0 2DA51012 AAF72BA5 971324B4


    ------------

      While loop

      Key is
              66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4
```

```
      V is
                                              CA8F5622 859AF6C5


Block #1
Blockin   CA8F5622 859AF6C5
Blockout  DE98EFE1 F7E66820

      output_block is
                                              DE98EFE1 F7E66820


      temp is
        51D241F0 2DA51012 AAF72BA5 971324B4 DE98EFE1 F7E66820


    ------------

      While loop

      Key is
              66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4


      V is
                                              CA8F5622 859AF6C6


Block #1
Blockin   CA8F5622 859AF6C6
Blockout  77D41DF0 D0B555E0

      output_block is
                                              77D41DF0 D0B555E0


      temp is
                                              51D241F0 2DA51012
        AAF72BA5 971324B4 DE98EFE1 F7E66820 77D41DF0 D0B555E0


    temp XOR provided_data is
                                                    51 D241F02D
        A51012AA F72BA597 1324B4DE 98EFE1F7 E6682077 D41DF0D0
```

```
    Key is
              51 D241F02D A51012AA F72BA597 1324B4DE 98EFE1F7

    V is
                                           E6682077 D41DF0D0

rnd_val is
                          760BED7D 92B083B1 0AF31CF0 656081EB

---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   E6682077 D41DF0D1
Blockout  FD1AC414 82384D82

Block #1
Blockin   E6682077 D41DF0D2
Blockout  3CF3FD6F 0E6C88B3

---------------------------

  Update

    provided_data is
                                                    00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop
```

```
      Key is
              51 D241F02D A51012AA F72BA597 1324B4DE 98EFE1F7


      V is
                                            E6682077 D41DF0D3


Block #1
Blockin   E6682077 D41DF0D3
Blockout  B928604D 47360185

      output_block is
                                            B928604D 47360185


      temp is
                                            B928604D 47360185


    ------------

      While loop

      Key is
              51 D241F02D A51012AA F72BA597 1324B4DE 98EFE1F7


      V is
                                            E6682077 D41DF0D4


Block #1
Blockin   E6682077 D41DF0D4
Blockout  4667FB5F 7ECEF1E0

      output_block is
                                            4667FB5F 7ECEF1E0


      temp is
                          B928604D 47360185 4667FB5F 7ECEF1E0


    ------------
```

```
      While loop

      Key is
              51 D241F02D A51012AA F72BA597 1324B4DE 98EFE1F7


      V is
                                            E6682077 D41DF0D5


Block #1
Blockin   E6682077 D41DF0D5
Blockout  090D3F82 5ADB078F

      output_block is
                                            090D3F82 5ADB078F


      temp is
        B928604D 47360185 4667FB5F 7ECEF1E0 090D3F82 5ADB078F


    ------------

      While loop

      Key is
              51 D241F02D A51012AA F72BA597 1324B4DE 98EFE1F7


      V is
                                            E6682077 D41DF0D6


Block #1
Blockin   E6682077 D41DF0D6
Blockout  6CB64FC1 4C6821E0

      output_block is
                                            6CB64FC1 4C6821E0


      temp is
                                            B928604D 47360185
        4667FB5F 7ECEF1E0 090D3F82 5ADB078F 6CB64FC1 4C6821E0
```

temp XOR provided_data is
                                                    B9 28604D47
    36018546 67FB5F7E CEF1E009 0D3F825A DB078F6C B64FC14C

Key is
          B9 28604D47 36018546 67FB5F7E CEF1E009 0D3F825A

V is
                                           DB078F6C B64FC14C

rnd_val is
                        FD1AC414 82384D82 3CF3FD6F 0E6C88B3

##

CTR_DRBG

Requested Security Strength = 112

prediction_resistance_flag = "NOT ENABLED"
EntropyInput =
                                                    00 01020304
    05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C

EntropyInput1 (for Reseed1) =
                                                    80 81828384
    85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C

EntropyInput2 (for Reseed2) =
                                                    C0 C1C2C3C4
    C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC

Nonce =
                                               202122 23242526

PersonalizationString =

```
                                                        40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    AdditionalInput1 =
                                                        60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


    AdditionalInput2 =
                                                        A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


################################################################

****************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    nonce is
                                                 202122 23242526


    personal_str is
                                                        40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                        00 01020304 05060708 090A0B0C 0D0E0F10
        11121314 15161718 191A1B1C 20212223 24252640 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C
```

```
number_of_bits_to_return = 232

S is
                                          00000041 0000001D
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C202122 23242526 40414243 44454647 48494A4B
    4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000


------------

  BCC

  IV is
                                          00000000 00000000


  IV || S is
                       00000000 00000000 00000041 0000001D
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C202122 23242526 40414243 44454647 48494A4B
    4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000


temp is
                                          BF5C8905 7D02B0A6


------------

  BCC

  IV is
                                          00000001 00000000


  IV || S is
                       00000001 00000000 00000041 0000001D
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C202122 23242526 40414243 44454647 48494A4B
    4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000


temp is
                       BF5C8905 7D02B0A6 77FE7647 E9554668
```

```
------------

  BCC

  IV is
                                          00000002 00000000


  IV || S is
                       00000002 00000000 00000041 0000001D
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C202122 23242526 40414243 44454647 48494A4B
    4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000


temp is
    BF5C8905 7D02B0A6 77FE7647 E9554668 AE4D8DE0 DB992E46


------------

  BCC

  IV is
                                          00000003 00000000


  IV || S is
                       00000003 00000000 00000041 0000001D
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C202122 23242526 40414243 44454647 48494A4B
    4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000


temp is
                                          BF5C8905 7D02B0A6
    77FE7647 E9554668 AE4D8DE0 DB992E46 83E1389F 33A1E91F


------------

Key is
          BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB
```

```
    X is
                                            992E4683 E1389F33


Block #1
Blockin   992E4683 E1389F33
Blockout  70F9F85E 350177E5

    ------------

      BlockEncrypt

      Key is
              BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB


      X is
                                            992E4683 E1389F33


      X = BlockEncrypt(Key, X) is
                                            70F9F85E 350177E5


      temp is
                                            70F9F85E 350177E5


Block #1
Blockin   70F9F85E 350177E5
Blockout  B228D49C 6374BBB6

    ------------

      BlockEncrypt

      Key is
              BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB


      X is
                                            70F9F85E 350177E5


      X = BlockEncrypt(Key, X) is
                                            B228D49C 6374BBB6
```

```
      temp is
                           70F9F85E 350177E5 B228D49C 6374BBB6


Block #1
Blockin   B228D49C 6374BBB6
Blockout  EA3DCFFA 463099CA

    ------------

      BlockEncrypt

      Key is
              BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB


      X is
                                           B228D49C 6374BBB6


      X = BlockEncrypt(Key, X) is
                                           EA3DCFFA 463099CA


      temp is
        70F9F85E 350177E5 B228D49C 6374BBB6 EA3DCFFA 463099CA


Block #1
Blockin   EA3DCFFA 463099CA
Blockout  F0781291 15A9A8E8

    ------------

      BlockEncrypt

      Key is
              BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB


      X is
                                           EA3DCFFA 463099CA
```

```
      X = BlockEncrypt(Key, X) is
                                              F0781291 15A9A8E8


      temp is
                                              70F9F85E 350177E5
        B228D49C 6374BBB6 EA3DCFFA 463099CA F0781291 15A9A8E8


      requested_bits is
                                                    70 F9F85E35
        0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115


    seed_material is
                                                    70 F9F85E35
        0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115


---------------------------

  Update

    provided_data is
                                                    70 F9F85E35
        0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000001


Block #1
Blockin   00000000 00000001
Blockout  166B40B4 4ABA4BD6

      output_block is
                                              166B40B4 4ABA4BD6
```

```
      temp is
                                              166B40B4 4ABA4BD6


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000002


Block #1
Blockin   00000000 00000002
Blockout  06E7EA22 CE92708F

      output_block is
                                              06E7EA22 CE92708F


      temp is
                           166B40B4 4ABA4BD6 06E7EA22 CE92708F


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C
```

```
      output_block is
                                              4EB190C9 A2FA169C

      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C

    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000

      V is
                                              00000000 00000004

Block #1
Blockin   00000000 00000004
Blockout  D2FD8867 D50D2DFE

      output_block is
                                              D2FD8867 D50D2DFE

      temp is
                                              166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE

    temp XOR provided_data is
                                                    66 92B8EA7F
        BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4 CA8F5622 859AF6C0

    Key is
              66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

    V is
                                              CA8F5622 859AF6C0
```

```
---------------------------------------------------------------

First call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                        60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


  additional_input <> NULL, process appropriately
----------------------------

  Block_Cipher_df

    input_str is
                                                        60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


    number_of_bits_to_return = 232

    S is
                           0000001D 0000001D 60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C800000


    ------------

      BCC

      IV is
                                               00000000 00000000


      IV || S is
        00000000 00000000 0000001D 0000001D 60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C800000


    temp is
```

A9DAAC27 BD128BB4

BCC

IV is
00000001 00000000

IV || S is
00000001 00000000 0000001D 0000001D 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C800000

temp is
A9DAAC27 BD128BB4 08EB0C8C 15DB001C

BCC

IV is
00000002 00000000

IV || S is
00000002 00000000 0000001D 0000001D 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C800000

temp is
A9DAAC27 BD128BB4 08EB0C8C 15DB001C 68175B62 9929DBB3

BCC

IV is
00000003 00000000

IV || S is

```
        00000003 00000000 0000001D 0000001D 60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C800000


    temp is
                                               A9DAAC27 BD128BB4
        08EB0C8C 15DB001C 68175B62 9929DBB3 EBF330CD 6977A3C0


    ------------

    Key is
              A9 DAAC27BD 128BB408 EB0C8C15 DB001C68 175B6299


    X is
                                               29DBB3EB F330CD69


Block #1
Blockin   29DBB3EB F330CD69
Blockout  68099422 99837788

    ------------

      BlockEncrypt

      Key is
              A9 DAAC27BD 128BB408 EB0C8C15 DB001C68 175B6299


      X is
                                               29DBB3EB F330CD69


      X = BlockEncrypt(Key, X) is
                                               68099422 99837788


      temp is
                                               68099422 99837788


Block #1
Blockin   68099422 99837788
Blockout  1665F614 303AD2C0
```

```
    ------------

      BlockEncrypt

      Key is
              A9 DAAC27BD 128BB408 EB0C8C15 DB001C68 175B6299


      X is
                                            68099422 99837788


      X = BlockEncrypt(Key, X) is
                                            1665F614 303AD2C0


      temp is
                           68099422 99837788 1665F614 303AD2C0


Block #1
Blockin   1665F614 303AD2C0
Blockout  3EEA906C 48996C3C

    ------------

      BlockEncrypt

      Key is
              A9 DAAC27BD 128BB408 EB0C8C15 DB001C68 175B6299


      X is
                                            1665F614 303AD2C0


      X = BlockEncrypt(Key, X) is
                                            3EEA906C 48996C3C


      temp is
        68099422 99837788 1665F614 303AD2C0 3EEA906C 48996C3C


Block #1
```

```
Blockin   3EEA906C 48996C3C
Blockout  22131B5A 94AF9E8C

    ------------

      BlockEncrypt

      Key is
              A9 DAAC27BD 128BB408 EB0C8C15 DB001C68 175B6299


      X is
                                              3EEA906C 48996C3C


      X = BlockEncrypt(Key, X) is
                                              22131B5A 94AF9E8C


      temp is
                                              68099422 99837788
        1665F614 303AD2C0 3EEA906C 48996C3C 22131B5A 94AF9E8C


      requested_bits is
                                                    68 09942299
        83778816 65F61430 3AD2C03E EA906C48 996C3C22 131B5A94


---------------------------

  Update

    provided_data is
                                                    68 09942299
        83778816 65F61430 3AD2C03E EA906C48 996C3C22 131B5A94


    ------------

      While loop

      Key is
              66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4
```

```
      V is
                                              CA8F5622 859AF6C1


Block #1
Blockin   CA8F5622 859AF6C1
Blockout  760BED7D 92B083B1

      output_block is
                                              760BED7D 92B083B1


      temp is
                                              760BED7D 92B083B1


    ------------

      While loop

      Key is
              66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4


      V is
                                              CA8F5622 859AF6C2


Block #1
Blockin   CA8F5622 859AF6C2
Blockout  0AF31CF0 656081EB

      output_block is
                                              0AF31CF0 656081EB


      temp is
                           760BED7D 92B083B1 0AF31CF0 656081EB


    ------------

      While loop

      Key is
              66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4
```

```
      V is
                                              CA8F5622 859AF6C3


Block #1
Blockin   CA8F5622 859AF6C3
Blockout  51D241F0 2DA51012

      output_block is
                                              51D241F0 2DA51012


      temp is
        760BED7D 92B083B1 0AF31CF0 656081EB 51D241F0 2DA51012


    ------------

      While loop

      Key is
              66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4


      V is
                                              CA8F5622 859AF6C4


Block #1
Blockin   CA8F5622 859AF6C4
Blockout  AAF72BA5 971324B4

      output_block is
                                              AAF72BA5 971324B4


      temp is
                                              760BED7D 92B083B1
        0AF31CF0 656081EB 51D241F0 2DA51012 AAF72BA5 971324B4


    temp XOR provided_data is
                                                    1E 02795F0B
        33F4391C 96EAE455 5A532B6F 38D19C65 3C7C2E88 E430FF03
```

```
    Key is
              1E 02795F0B 33F4391C 96EAE455 5A532B6F 38D19C65


    V is
                                            3C7C2E88 E430FF03


Block #1
Blockin   3C7C2E88 E430FF04
Blockout  7A4C1D7A DC8A67FD

Block #1
Blockin   3C7C2E88 E430FF05
Blockout  B50100ED 23583A2C

---------------------------

  Update

    provided_data is
                                                      68 09942299
        83778816 65F61430 3AD2C03E EA906C48 996C3C22 131B5A94


    ------------

      While loop

      Key is
              1E 02795F0B 33F4391C 96EAE455 5A532B6F 38D19C65


      V is
                                            3C7C2E88 E430FF06


Block #1
Blockin   3C7C2E88 E430FF06
Blockout  E389E6D3 774C1B77

      output_block is
                                            E389E6D3 774C1B77
```

```
      temp is
                                              E389E6D3 774C1B77


    ------------

      While loop

      Key is
              1E 02795F0B 33F4391C 96EAE455 5A532B6F 38D19C65


      V is
                                              3C7C2E88 E430FF07


Block #1
Blockin   3C7C2E88 E430FF07
Blockout  95098FD6 517B8586

      output_block is
                                              95098FD6 517B8586


      temp is
                           E389E6D3 774C1B77 95098FD6 517B8586


    ------------

      While loop

      Key is
              1E 02795F0B 33F4391C 96EAE455 5A532B6F 38D19C65


      V is
                                              3C7C2E88 E430FF08


Block #1
Blockin   3C7C2E88 E430FF08
Blockout  39FA9717 298A170E

      output_block is
```

```
                                              39FA9717 298A170E


      temp is
        E389E6D3 774C1B77 95098FD6 517B8586 39FA9717 298A170E


    ------------

      While loop

      Key is
              1E 02795F0B 33F4391C 96EAE455 5A532B6F 38D19C65


      V is
                                              3C7C2E88 E430FF09


Block #1
Blockin   3C7C2E88 E430FF09
Blockout  C4D08986 886423EA

      output_block is
                                              C4D08986 886423EA


      temp is
                                              E389E6D3 774C1B77
        95098FD6 517B8586 39FA9717 298A170E C4D08986 886423EA


    temp XOR provided_data is
                                                    8B 8072F1EE
        CF6CFF83 6C79C261 41574607 10077B61 137B32E6 C392DC1C


    Key is
              8B 8072F1EE CF6CFF83 6C79C261 41574607 10077B61


    V is
                                              137B32E6 C392DC1C


rnd_val is
```

```
                          7A4C1D7A DC8A67FD B50100ED 23583A2C


-------------------------------------------------------------

Second call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                    A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


  additional_input <> NULL, process appropriately
---------------------------

  Block_Cipher_df

    input_str is
                                                    A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


    number_of_bits_to_return = 232

    S is
                          0000001D 0000001D A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BC800000


    ------------

      BCC

      IV is
                                               00000000 00000000


      IV || S is
        00000000 00000000 0000001D 0000001D A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BC800000
```

```
temp is
                                        89213498 76E519BE


------------

  BCC

  IV is
                                        00000001 00000000


  IV || S is
    00000001 00000000 0000001D 0000001D A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BC800000


temp is
                     89213498 76E519BE FC10164B 5A8722CE


------------

  BCC

  IV is
                                        00000002 00000000


  IV || S is
    00000002 00000000 0000001D 0000001D A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BC800000


temp is
    89213498 76E519BE FC10164B 5A8722CE 5C92E9C1 6F213C22


------------

  BCC

  IV is
                                        00000003 00000000
```

```
      IV || S is
        00000003 00000000 0000001D 0000001D A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BC800000


    temp is
                                              89213498 76E519BE
        FC10164B 5A8722CE 5C92E9C1 6F213C22 9B946180 1B6BAA48


    ------------

    Key is
              89 21349876 E519BEFC 10164B5A 8722CE5C 92E9C16F


    X is
                                              213C229B 9461801B


Block #1
Blockin   213C229B 9461801B
Blockout  07669398 0A486518

    ------------

      BlockEncrypt

      Key is
              89 21349876 E519BEFC 10164B5A 8722CE5C 92E9C16F


      X is
                                              213C229B 9461801B


      X = BlockEncrypt(Key, X) is
                                              07669398 0A486518


      temp is
                                              07669398 0A486518
```

```
Block #1
Blockin   07669398 0A486518
Blockout  DC19FECA F56EF259

    ------------

      BlockEncrypt

      Key is
              89 21349876 E519BEFC 10164B5A 8722CE5C 92E9C16F


      X is
                                            07669398 0A486518


      X = BlockEncrypt(Key, X) is
                                            DC19FECA F56EF259


      temp is
                           07669398 0A486518 DC19FECA F56EF259


Block #1
Blockin   DC19FECA F56EF259
Blockout  0FF65EF1 FE9A7410

    ------------

      BlockEncrypt

      Key is
              89 21349876 E519BEFC 10164B5A 8722CE5C 92E9C16F


      X is
                                            DC19FECA F56EF259


      X = BlockEncrypt(Key, X) is
                                            0FF65EF1 FE9A7410


      temp is
        07669398 0A486518 DC19FECA F56EF259 0FF65EF1 FE9A7410
```

```
Block #1
Blockin   0FF65EF1 FE9A7410
Blockout  8C1FC048 1C36F198

    ------------

      BlockEncrypt

      Key is
              89 21349876 E519BEFC 10164B5A 8722CE5C 92E9C16F


      X is
                                              0FF65EF1 FE9A7410


      X = BlockEncrypt(Key, X) is
                                              8C1FC048 1C36F198


      temp is
                                              07669398 0A486518
        DC19FECA F56EF259 0FF65EF1 FE9A7410 8C1FC048 1C36F198


      requested_bits is
                                                    07 6693980A
        486518DC 19FECAF5 6EF2590F F65EF1FE 9A74108C 1FC0481C


---------------------------

  Update

    provided_data is
                                                    07 6693980A
        486518DC 19FECAF5 6EF2590F F65EF1FE 9A74108C 1FC0481C


    ------------

      While loop

      Key is
```

```
               8B 8072F1EE CF6CFF83 6C79C261 41574607 10077B61


      V is
                                              137B32E6 C392DC1D


Block #1
Blockin   137B32E6 C392DC1D
Blockout  71ACF298 A91A853C

      output_block is
                                              71ACF298 A91A853C


      temp is
                                              71ACF298 A91A853C


    ------------

      While loop

      Key is
               8B 8072F1EE CF6CFF83 6C79C261 41574607 10077B61


      V is
                                              137B32E6 C392DC1E


Block #1
Blockin   137B32E6 C392DC1E
Blockout  0B536A49 52A621E3

      output_block is
                                              0B536A49 52A621E3


      temp is
                           71ACF298 A91A853C 0B536A49 52A621E3


    ------------

      While loop
```

```
      Key is
              8B 8072F1EE CF6CFF83 6C79C261 41574607 10077B61


      V is
                                            137B32E6 C392DC1F


Block #1
Blockin   137B32E6 C392DC1F
Blockout  B73EC34D 076FA884

      output_block is
                                            B73EC34D 076FA884


      temp is
        71ACF298 A91A853C 0B536A49 52A621E3 B73EC34D 076FA884


    ------------

      While loop

      Key is
              8B 8072F1EE CF6CFF83 6C79C261 41574607 10077B61


      V is
                                            137B32E6 C392DC20


Block #1
Blockin   137B32E6 C392DC20
Blockout  8D840694 E86E372F

      output_block is
                                            8D840694 E86E372F


      temp is
                                            71ACF298 A91A853C
        0B536A49 52A621E3 B73EC34D 076FA884 8D840694 E86E372F
```

```
    temp XOR provided_data is
                                                        76 CA6100A3
        52E024D7 4A9483A7 C8D3BAB8 C89DBCF9 F5DC9401 9BC6DCF4


    Key is
              76 CA6100A3 52E024D7 4A9483A7 C8D3BAB8 C89DBCF9


    V is
                                              F5DC9401 9BC6DCF4


Block #1
Blockin   F5DC9401 9BC6DCF5
Blockout  43044D31 1C0E0754

Block #1
Blockin   F5DC9401 9BC6DCF6
Blockout  1CA5C8B0 916976B2

---------------------------

  Update

    provided_data is
                                                        07 6693980A
        486518DC 19FECAF5 6EF2590F F65EF1FE 9A74108C 1FC0481C


    ------------

      While loop

      Key is
              76 CA6100A3 52E024D7 4A9483A7 C8D3BAB8 C89DBCF9


      V is
                                              F5DC9401 9BC6DCF7


Block #1
Blockin   F5DC9401 9BC6DCF7
Blockout  CEF879E1 B6EF8D6F
```

```
      output_block is
                                              CEF879E1 B6EF8D6F


      temp is
                                              CEF879E1 B6EF8D6F


    ------------

      While loop

      Key is
              76 CA6100A3 52E024D7 4A9483A7 C8D3BAB8 C89DBCF9


      V is
                                              F5DC9401 9BC6DCF8


Block #1
Blockin   F5DC9401 9BC6DCF8
Blockout  59D0D09C E0588BF2

      output_block is
                                              59D0D09C E0588BF2


      temp is
                           CEF879E1 B6EF8D6F 59D0D09C E0588BF2


    ------------

      While loop

      Key is
              76 CA6100A3 52E024D7 4A9483A7 C8D3BAB8 C89DBCF9


      V is
                                              F5DC9401 9BC6DCF9


Block #1
Blockin   F5DC9401 9BC6DCF9
```

```
Blockout  913215D6 1DA82FF7

      output_block is
                                              913215D6 1DA82FF7


      temp is
        CEF879E1 B6EF8D6F 59D0D09C E0588BF2 913215D6 1DA82FF7


    ------------

      While loop

      Key is
              76 CA6100A3 52E024D7 4A9483A7 C8D3BAB8 C89DBCF9


      V is
                                              F5DC9401 9BC6DCFA


Block #1
Blockin   F5DC9401 9BC6DCFA
Blockout  4B2886B9 052DEFEB

      output_block is
                                              4B2886B9 052DEFEB


      temp is
                                              CEF879E1 B6EF8D6F
        59D0D09C E0588BF2 913215D6 1DA82FF7 4B2886B9 052DEFEB


    temp XOR provided_data is
                                                    C9 9EEA79BC
        A7E87785 C92E5615 3679AB9E C44B27E3 325BE7C7 3746F119


    Key is
              C9 9EEA79BC A7E87785 C92E5615 3679AB9E C44B27E3


    V is
                                              325BE7C7 3746F119
```

```
rnd_val is
                          43044D31 1C0E0754 1CA5C8B0 916976B2

################################################################

CTR_DRBG

    Requested Security Strength = 112

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                      00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    EntropyInput1 (for Reseed1) =
                                                      80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                      C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    Nonce =
                                                 202122 23242526


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                                                      00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C
```

```
    nonce is
                                                202122 23242526


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                                     00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C202122 23242526


    number_of_bits_to_return = 232

    S is
        00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C202122 23242526 80000000


    ------------

      BCC

      IV is
                                               00000000 00000000


      IV || S is
                                               00000000 00000000
        00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C202122 23242526 80000000


    temp is
                                               4A2145C3 52BD4642


    ------------

      BCC
```

```
  IV is
                                          00000001 00000000


  IV || S is
                                          00000001 00000000
    00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C202122 23242526 80000000


temp is
                     4A2145C3 52BD4642 EEB5E70D CAE11D42


------------

  BCC

  IV is
                                          00000002 00000000


  IV || S is
                                          00000002 00000000
    00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C202122 23242526 80000000


temp is
    4A2145C3 52BD4642 EEB5E70D CAE11D42 82FD02F7 B62641C4


------------

  BCC

  IV is
                                          00000003 00000000


  IV || S is
                                          00000003 00000000
    00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C202122 23242526 80000000
```

```
    temp is
                                            4A2145C3 52BD4642
        EEB5E70D CAE11D42 82FD02F7 B62641C4 BAE575D6 E7411566


    ------------

    Key is
              4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6


    X is
                                            2641C4BA E575D6E7


Block #1
Blockin   2641C4BA E575D6E7
Blockout  B4300B8B 7D547B40

    ------------

      BlockEncrypt

      Key is
              4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6


      X is
                                            2641C4BA E575D6E7


      X = BlockEncrypt(Key, X) is
                                            B4300B8B 7D547B40


      temp is
                                            B4300B8B 7D547B40


Block #1
Blockin   B4300B8B 7D547B40
Blockout  599CFD0E B13B1607

    ------------
```

```
      BlockEncrypt

      Key is
              4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6


      X is
                                              B4300B8B 7D547B40


      X = BlockEncrypt(Key, X) is
                                              599CFD0E B13B1607


      temp is
                            B4300B8B 7D547B40 599CFD0E B13B1607


Block #1
Blockin   599CFD0E B13B1607
Blockout  2398EF59 1553A5A3

    ------------

      BlockEncrypt

      Key is
              4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6


      X is
                                              599CFD0E B13B1607


      X = BlockEncrypt(Key, X) is
                                              2398EF59 1553A5A3


      temp is
        B4300B8B 7D547B40 599CFD0E B13B1607 2398EF59 1553A5A3


Block #1
Blockin   2398EF59 1553A5A3
Blockout  A10292FE FE535642
```

```
    ------------

      BlockEncrypt

      Key is
              4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6


      X is
                                            2398EF59 1553A5A3


      X = BlockEncrypt(Key, X) is
                                            A10292FE FE535642


      temp is
                                            B4300B8B 7D547B40
        599CFD0E B13B1607 2398EF59 1553A5A3 A10292FE FE535642


      requested_bits is
                                                    B4 300B8B7D
        547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE


    seed_material is
                                                    B4 300B8B7D
        547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE


---------------------------

  Update

    provided_data is
                                                    B4 300B8B7D
        547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000
```

```
      V is
                                                00000000 00000001


Block #1
Blockin   00000000 00000001
Blockout  166B40B4 4ABA4BD6

      output_block is
                                                166B40B4 4ABA4BD6


      temp is
                                                166B40B4 4ABA4BD6


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                                00000000 00000002


Block #1
Blockin   00000000 00000002
Blockout  06E7EA22 CE92708F

      output_block is
                                                06E7EA22 CE92708F


      temp is
                           166B40B4 4ABA4BD6 06E7EA22 CE92708F


    ------------

      While loop
```

```
      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                              4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000004


Block #1
Blockin   00000000 00000004
Blockout  D2FD8867 D50D2DFE

      output_block is
                                              D2FD8867 D50D2DFE


      temp is
                                              166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
```

```
                                                    A2 5B4B3F37
        EE30965F 7B172C7F A966886D 297F90B7 A9B33F73 FF1A992B


    Key is
              A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7


    V is
                                           A9B33F73 FF1A992B


------------------------------------------------------------

First call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                                    80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    additional_input is  <empty>

--------------------------

  Block_Cipher_df

    input_str is
                                                    80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    number_of_bits_to_return = 232
```

```
S is
                     0000001D 0000001D 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C800000


------------

  BCC

  IV is
                                        00000000 00000000


  IV || S is
    00000000 00000000 0000001D 0000001D 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C800000


temp is
                                        B435EC36 31249E3D


------------

  BCC

  IV is
                                        00000001 00000000


  IV || S is
    00000001 00000000 0000001D 0000001D 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C800000


temp is
                     B435EC36 31249E3D A735CE05 7E609075


------------

  BCC

  IV is
                                        00000002 00000000
```

```
      IV || S is
        00000002 00000000 0000001D 0000001D 80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C800000


    temp is
        B435EC36 31249E3D A735CE05 7E609075 CA6920F2 1DF7CB3D


    ------------

      BCC

      IV is
                                              00000003 00000000


      IV || S is
        00000003 00000000 0000001D 0000001D 80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C800000


    temp is
                                              B435EC36 31249E3D
        A735CE05 7E609075 CA6920F2 1DF7CB3D 6547CE54 BA8A17A5


    ------------

    Key is
              B4 35EC3631 249E3DA7 35CE057E 609075CA 6920F21D


    X is
                                              F7CB3D65 47CE54BA


Block #1
Blockin   F7CB3D65 47CE54BA
Blockout  7D3F6CAF 387E4C9A

    ------------

      BlockEncrypt
```

```
      Key is
              B4 35EC3631 249E3DA7 35CE057E 609075CA 6920F21D


      X is
                                           F7CB3D65 47CE54BA


      X = BlockEncrypt(Key, X) is
                                           7D3F6CAF 387E4C9A


      temp is
                                           7D3F6CAF 387E4C9A


Block #1
Blockin   7D3F6CAF 387E4C9A
Blockout  1A5787D4 81378C06

    ------------

      BlockEncrypt

      Key is
              B4 35EC3631 249E3DA7 35CE057E 609075CA 6920F21D


      X is
                                           7D3F6CAF 387E4C9A


      X = BlockEncrypt(Key, X) is
                                           1A5787D4 81378C06


      temp is
                           7D3F6CAF 387E4C9A 1A5787D4 81378C06


Block #1
Blockin   1A5787D4 81378C06
Blockout  C409511D DB736F2D

    ------------
```

```
      BlockEncrypt

      Key is
              B4 35EC3631 249E3DA7 35CE057E 609075CA 6920F21D


      X is
                                            1A5787D4 81378C06


      X = BlockEncrypt(Key, X) is
                                            C409511D DB736F2D


      temp is
        7D3F6CAF 387E4C9A 1A5787D4 81378C06 C409511D DB736F2D


Block #1
Blockin   C409511D DB736F2D
Blockout  D4CB361F 4C1392A0

    ------------

      BlockEncrypt

      Key is
              B4 35EC3631 249E3DA7 35CE057E 609075CA 6920F21D


      X is
                                            C409511D DB736F2D


      X = BlockEncrypt(Key, X) is
                                            D4CB361F 4C1392A0


      temp is
                                            7D3F6CAF 387E4C9A
        1A5787D4 81378C06 C409511D DB736F2D D4CB361F 4C1392A0


      requested_bits is
                                                  7D 3F6CAF38
```

```
        7E4C9A1A 5787D481 378C06C4 09511DDB 736F2DD4 CB361F4C


---------------------------

  Update

    provided_data is
                                                        7D 3F6CAF38
        7E4C9A1A 5787D481 378C06C4 09511DDB 736F2DD4 CB361F4C


    ------------

      While loop

      Key is
              A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7


      V is
                                            A9B33F73 FF1A992C


Block #1
Blockin   A9B33F73 FF1A992C
Blockout  ABC88224 514D0316

      output_block is
                                            ABC88224 514D0316


      temp is
                                            ABC88224 514D0316


    ------------

      While loop

      Key is
              A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7


      V is
                                            A9B33F73 FF1A992D
```

```
Block #1
Blockin   A9B33F73 FF1A992D
Blockout  EA3D48AE E3C9A2B4

      output_block is
                                              EA3D48AE E3C9A2B4


      temp is
                           ABC88224 514D0316 EA3D48AE E3C9A2B4


    ------------

      While loop

      Key is
              A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7


      V is
                                              A9B33F73 FF1A992E


Block #1
Blockin   A9B33F73 FF1A992E
Blockout  27CE2546 E5F9CE73

      output_block is
                                              27CE2546 E5F9CE73


      temp is
        ABC88224 514D0316 EA3D48AE E3C9A2B4 27CE2546 E5F9CE73


    ------------

      While loop

      Key is
              A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7
```

```
      V is
                                              A9B33F73 FF1A992F


Block #1
Blockin   A9B33F73 FF1A992F
Blockout  AC843CE9 A9F8B369

      output_block is
                                              AC843CE9 A9F8B369


      temp is
                                              ABC88224 514D0316
        EA3D48AE E3C9A2B4 27CE2546 E5F9CE73 AC843CE9 A9F8B369


    temp XOR provided_data is
                                                    D6 F7EE8B69
        334F8CF0 6ACF7A62 FE2EB2E3 C7745B3E 8AA15E78 4F0AF6E5


    Key is
              D6 F7EE8B69 334F8CF0 6ACF7A62 FE2EB2E3 C7745B3E


    V is
                                              8AA15E78 4F0AF6E5


************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   8AA15E78 4F0AF6E6
Blockout  8FB78ABC A75C9F28

Block #1
Blockin   8AA15E78 4F0AF6E7
Blockout  4E974E36 141866BC
```

```
---------------------------

  Update

    provided_data is
                                                          00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              D6 F7EE8B69 334F8CF0 6ACF7A62 FE2EB2E3 C7745B3E


      V is
                                            8AA15E78 4F0AF6E8


Block #1
Blockin   8AA15E78 4F0AF6E8
Blockout  8E30D7EE C6D9C99D

      output_block is
                                            8E30D7EE C6D9C99D


      temp is
                                            8E30D7EE C6D9C99D


    ------------

      While loop

      Key is
              D6 F7EE8B69 334F8CF0 6ACF7A62 FE2EB2E3 C7745B3E


      V is
                                            8AA15E78 4F0AF6E9


Block #1
```

```
Blockin   8AA15E78 4F0AF6E9
Blockout  83C99986 9BB24B13

      output_block is
                                              83C99986 9BB24B13


      temp is
                           8E30D7EE C6D9C99D 83C99986 9BB24B13


    ------------

      While loop

      Key is
              D6 F7EE8B69 334F8CF0 6ACF7A62 FE2EB2E3 C7745B3E


      V is
                                              8AA15E78 4F0AF6EA


Block #1
Blockin   8AA15E78 4F0AF6EA
Blockout  C2EC88E6 D3496FDA

      output_block is
                                              C2EC88E6 D3496FDA


      temp is
        8E30D7EE C6D9C99D 83C99986 9BB24B13 C2EC88E6 D3496FDA


    ------------

      While loop

      Key is
              D6 F7EE8B69 334F8CF0 6ACF7A62 FE2EB2E3 C7745B3E


      V is
                                              8AA15E78 4F0AF6EB
```

```
Block #1
Blockin   8AA15E78 4F0AF6EB
Blockout  6CFFF2EA DAFF7F6D

      output_block is
                                              6CFFF2EA DAFF7F6D


      temp is
                                              8E30D7EE C6D9C99D
        83C99986 9BB24B13 C2EC88E6 D3496FDA 6CFFF2EA DAFF7F6D


    temp XOR provided_data is
                                                    8E 30D7EEC6
        D9C99D83 C999869B B24B13C2 EC88E6D3 496FDA6C FFF2EADA


    Key is
              8E 30D7EEC6 D9C99D83 C999869B B24B13C2 EC88E6D3


    V is
                                              496FDA6C FFF2EADA


rnd_val is
                         8FB78ABC A75C9F28 4E974E36 141866BC


-------------------------------------------------------------

Second call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************
```

```
CTR_DRBG_Reseed

    entropy_input is
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    additional_input is  <empty>

---------------------------

  Block_Cipher_df

    input_str is
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    number_of_bits_to_return = 232

    S is
                          0000001D 0000001D C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DC800000


    ------------

      BCC

      IV is
                                               00000000 00000000


      IV || S is
        00000000 00000000 0000001D 0000001D C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DC800000


    temp is
                                               75D864A6 B6D27B8E


    ------------

      BCC
```

```
  IV is
                                          00000001 00000000


  IV || S is
    00000001 00000000 0000001D 0000001D C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DC800000


temp is
                     75D864A6 B6D27B8E F1B88BC4 D95D7412


------------

  BCC

  IV is
                                          00000002 00000000


  IV || S is
    00000002 00000000 0000001D 0000001D C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DC800000


temp is
    75D864A6 B6D27B8E F1B88BC4 D95D7412 DA1D4B49 3894DD64


------------

  BCC

  IV is
                                          00000003 00000000


  IV || S is
    00000003 00000000 0000001D 0000001D C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DC800000


temp is
                                          75D864A6 B6D27B8E
    F1B88BC4 D95D7412 DA1D4B49 3894DD64 1F27605F F6EAC071
```

```
    ------------

    Key is
              75 D864A6B6 D27B8EF1 B88BC4D9 5D7412DA 1D4B4938


    X is
                                            94DD641F 27605FF6


Block #1
Blockin   94DD641F 27605FF6
Blockout  1A1AD191 C4A0E7D1

    ------------

      BlockEncrypt

      Key is
              75 D864A6B6 D27B8EF1 B88BC4D9 5D7412DA 1D4B4938


      X is
                                            94DD641F 27605FF6


      X = BlockEncrypt(Key, X) is
                                            1A1AD191 C4A0E7D1


      temp is
                                            1A1AD191 C4A0E7D1


Block #1
Blockin   1A1AD191 C4A0E7D1
Blockout  EA461812 450132A6

    ------------

      BlockEncrypt

      Key is
              75 D864A6B6 D27B8EF1 B88BC4D9 5D7412DA 1D4B4938
```

```
      X is
                                          1A1AD191 C4A0E7D1

      X = BlockEncrypt(Key, X) is
                                          EA461812 450132A6

      temp is
                          1A1AD191 C4A0E7D1 EA461812 450132A6

Block #1
Blockin   EA461812 450132A6
Blockout  A84F5E05 D0A53DBD

    ------------

      BlockEncrypt

      Key is
              75 D864A6B6 D27B8EF1 B88BC4D9 5D7412DA 1D4B4938

      X is
                                          EA461812 450132A6

      X = BlockEncrypt(Key, X) is
                                          A84F5E05 D0A53DBD

      temp is
        1A1AD191 C4A0E7D1 EA461812 450132A6 A84F5E05 D0A53DBD

Block #1
Blockin   A84F5E05 D0A53DBD
Blockout  BCDC595B A4B22114

    ------------

      BlockEncrypt
```

```
      Key is
              75 D864A6B6 D27B8EF1 B88BC4D9 5D7412DA 1D4B4938


      X is
                                              A84F5E05 D0A53DBD


      X = BlockEncrypt(Key, X) is
                                              BCDC595B A4B22114


      temp is
                                              1A1AD191 C4A0E7D1
        EA461812 450132A6 A84F5E05 D0A53DBD BCDC595B A4B22114


      requested_bits is
                                                    1A 1AD191C4
        A0E7D1EA 46181245 0132A6A8 4F5E05D0 A53DBDBC DC595BA4


---------------------------

  Update

    provided_data is
                                                    1A 1AD191C4
        A0E7D1EA 46181245 0132A6A8 4F5E05D0 A53DBDBC DC595BA4


    ------------

      While loop

      Key is
              8E 30D7EEC6 D9C99D83 C999869B B24B13C2 EC88E6D3


      V is
                                              496FDA6C FFF2EADB


Block #1
Blockin   496FDA6C FFF2EADB
Blockout  8C96A647 4EEBF343
```

```
      output_block is
                                              8C96A647 4EEBF343

      temp is
                                              8C96A647 4EEBF343

    ------------

      While loop

      Key is
              8E 30D7EEC6 D9C99D83 C999869B B24B13C2 EC88E6D3

      V is
                                              496FDA6C FFF2EADC

Block #1
Blockin   496FDA6C FFF2EADC
Blockout  CB5C81A8 1AFEC815

      output_block is
                                              CB5C81A8 1AFEC815

      temp is
                           8C96A647 4EEBF343 CB5C81A8 1AFEC815

    ------------

      While loop

      Key is
              8E 30D7EEC6 D9C99D83 C999869B B24B13C2 EC88E6D3

      V is
                                              496FDA6C FFF2EADD

Block #1
```

```
Blockin   496FDA6C FFF2EADD
Blockout  22ECD7A2 B186E741

      output_block is
                                              22ECD7A2 B186E741


      temp is
        8C96A647 4EEBF343 CB5C81A8 1AFEC815 22ECD7A2 B186E741


    ------------

      While loop

      Key is
              8E 30D7EEC6 D9C99D83 C999869B B24B13C2 EC88E6D3


      V is
                                              496FDA6C FFF2EADE


Block #1
Blockin   496FDA6C FFF2EADE
Blockout  B92231DC 44D71E5B

      output_block is
                                              B92231DC 44D71E5B


      temp is
                                              8C96A647 4EEBF343
        CB5C81A8 1AFEC815 22ECD7A2 B186E741 B92231DC 44D71E5B


    temp XOR provided_data is
                                                    96 8C77D68A
        4B149221 1A99BA5F FFFAB38A A389A761 23DAFC05 FE6887E0


    Key is
              96 8C77D68A 4B149221 1A99BA5F FFFAB38A A389A761


    V is
```

```
                                                23DAFC05 FE6887E0

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   23DAFC05 FE6887E1
Blockout  9D9745FF 31C42A44

Block #1
Blockin   23DAFC05 FE6887E2
Blockout  88CBB771 B13B5D86

---------------------------

  Update

    provided_data is
                                                      00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              96 8C77D68A 4B149221 1A99BA5F FFFAB38A A389A761


      V is
                                                23DAFC05 FE6887E3


Block #1
Blockin   23DAFC05 FE6887E3
Blockout  7F7365D7 ED0AB324

      output_block is
                                                7F7365D7 ED0AB324
```

```
      temp is
                                              7F7365D7 ED0AB324


    ------------

      While loop

      Key is
              96 8C77D68A 4B149221 1A99BA5F FFFAB38A A389A761


      V is
                                              23DAFC05 FE6887E4


Block #1
Blockin   23DAFC05 FE6887E4
Blockout  DD1F46F2 8132DC76

      output_block is
                                              DD1F46F2 8132DC76


      temp is
                            7F7365D7 ED0AB324 DD1F46F2 8132DC76


    ------------

      While loop

      Key is
              96 8C77D68A 4B149221 1A99BA5F FFFAB38A A389A761


      V is
                                              23DAFC05 FE6887E5


Block #1
Blockin   23DAFC05 FE6887E5
Blockout  7A768AD8 F0F37B4D
```

```
      output_block is
                                              7A768AD8 F0F37B4D


      temp is
        7F7365D7 ED0AB324 DD1F46F2 8132DC76 7A768AD8 F0F37B4D


    ------------

      While loop

      Key is
              96 8C77D68A 4B149221 1A99BA5F FFFAB38A A389A761


      V is
                                              23DAFC05 FE6887E6


Block #1
Blockin   23DAFC05 FE6887E6
Blockout  DE770AB1 EF6B435C

      output_block is
                                              DE770AB1 EF6B435C


      temp is
                                              7F7365D7 ED0AB324
        DD1F46F2 8132DC76 7A768AD8 F0F37B4D DE770AB1 EF6B435C


    temp XOR provided_data is
                                                    7F 7365D7ED
        0AB324DD 1F46F281 32DC767A 768AD8F0 F37B4DDE 770AB1EF


    Key is
              7F 7365D7ED 0AB324DD 1F46F281 32DC767A 768AD8F0


    V is
                                              F37B4DDE 770AB1EF
```

```
rnd_val is
                          9D9745FF 31C42A44 88CBB771 B13B5D86


###############################################################

CTR_DRBG

    Requested Security Strength = 112

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                    00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    EntropyInput1 (for Reseed1) =
                                                    80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                    C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    Nonce =
                                                202122 23242526


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                    60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


    AdditionalInput2 =
                                                    A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


###############################################################

***************************************************************
```

```
CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    nonce is
                                                 202122 23242526


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                                      00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C202122 23242526


    number_of_bits_to_return = 232

    S is
        00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C202122 23242526 80000000


    ------------

      BCC

      IV is
                                               00000000 00000000


      IV || S is
                                               00000000 00000000
        00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C202122 23242526 80000000


    temp is
```

```
                                          4A2145C3 52BD4642


------------

  BCC

  IV is
                                          00000001 00000000


  IV || S is
                                          00000001 00000000
    00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C202122 23242526 80000000


temp is
                     4A2145C3 52BD4642 EEB5E70D CAE11D42


------------

  BCC

  IV is
                                          00000002 00000000


  IV || S is
                                          00000002 00000000
    00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C202122 23242526 80000000


temp is
    4A2145C3 52BD4642 EEB5E70D CAE11D42 82FD02F7 B62641C4


------------

  BCC

  IV is
                                          00000003 00000000
```

```
      IV || S is
                                                00000003 00000000
        00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C202122 23242526 80000000


    temp is
                                                4A2145C3 52BD4642
        EEB5E70D CAE11D42 82FD02F7 B62641C4 BAE575D6 E7411566


    ------------

    Key is
              4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6


    X is
                                                2641C4BA E575D6E7


Block #1
Blockin   2641C4BA E575D6E7
Blockout  B4300B8B 7D547B40

    ------------

      BlockEncrypt

      Key is
              4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6


      X is
                                                2641C4BA E575D6E7


      X = BlockEncrypt(Key, X) is
                                                B4300B8B 7D547B40


      temp is
                                                B4300B8B 7D547B40
```

```
Block #1
Blockin   B4300B8B 7D547B40
Blockout  599CFD0E B13B1607

    ------------

      BlockEncrypt

      Key is
              4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6


      X is
                                            B4300B8B 7D547B40


      X = BlockEncrypt(Key, X) is
                                            599CFD0E B13B1607


      temp is
                           B4300B8B 7D547B40 599CFD0E B13B1607


Block #1
Blockin   599CFD0E B13B1607
Blockout  2398EF59 1553A5A3

    ------------

      BlockEncrypt

      Key is
              4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6


      X is
                                            599CFD0E B13B1607


      X = BlockEncrypt(Key, X) is
                                            2398EF59 1553A5A3


      temp is
        B4300B8B 7D547B40 599CFD0E B13B1607 2398EF59 1553A5A3
```

```
Block #1
Blockin   2398EF59 1553A5A3
Blockout  A10292FE FE535642

    ------------

      BlockEncrypt

      Key is
              4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6


      X is
                                            2398EF59 1553A5A3


      X = BlockEncrypt(Key, X) is
                                            A10292FE FE535642


      temp is
                                            B4300B8B 7D547B40
        599CFD0E B13B1607 2398EF59 1553A5A3 A10292FE FE535642


      requested_bits is
                                                     B4 300B8B7D
        547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE


    seed_material is
                                                     B4 300B8B7D
        547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE


---------------------------

  Update

    provided_data is
                                                     B4 300B8B7D
        547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE
```

```
    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                             00000000 00000001


Block #1
Blockin   00000000 00000001
Blockout  166B40B4 4ABA4BD6

      output_block is
                                             166B40B4 4ABA4BD6


      temp is
                                             166B40B4 4ABA4BD6


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                             00000000 00000002


Block #1
Blockin   00000000 00000002
Blockout  06E7EA22 CE92708F

      output_block is
                                             06E7EA22 CE92708F


      temp is
                           166B40B4 4ABA4BD6 06E7EA22 CE92708F
```

```
    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                              4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000004


Block #1
Blockin   00000000 00000004
Blockout  D2FD8867 D50D2DFE

      output_block is
                                              D2FD8867 D50D2DFE
```

```
      temp is
                                                166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                    A2 5B4B3F37
        EE30965F 7B172C7F A966886D 297F90B7 A9B33F73 FF1A992B


    Key is
              A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7


    V is
                                                A9B33F73 FF1A992B


------------------------------------------------------------

First call to Generate

**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                    60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


Generate FAILED: Reseed is required
**************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                                    80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    additional_input is
                                                    60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C
```

```
---------------------------

  Block_Cipher_df

    input_str is
                                        8081 82838485 86878889
        8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


    number_of_bits_to_return = 232

    S is
        0000003A 0000001D 80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C606162 63646566 6768696A
        6B6C6D6E 6F707172 73747576 7778797A 7B7C8000 00000000


    ------------

      BCC

      IV is
                                            00000000 00000000


      IV || S is
                                            00000000 00000000
        0000003A 0000001D 80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C606162 63646566 6768696A
        6B6C6D6E 6F707172 73747576 7778797A 7B7C8000 00000000


    temp is
                                            58B3B0F6 8DD4432B


    ------------

      BCC

      IV is
                                            00000001 00000000
```

```
  IV || S is
                                              00000001 00000000
    0000003A 0000001D 80818283 84858687 88898A8B 8C8D8E8F
    90919293 94959697 98999A9B 9C606162 63646566 6768696A
    6B6C6D6E 6F707172 73747576 7778797A 7B7C8000 00000000


temp is
                     58B3B0F6 8DD4432B FE91AF80 FC822A3B


------------

  BCC

  IV is
                                              00000002 00000000


  IV || S is
                                              00000002 00000000
    0000003A 0000001D 80818283 84858687 88898A8B 8C8D8E8F
    90919293 94959697 98999A9B 9C606162 63646566 6768696A
    6B6C6D6E 6F707172 73747576 7778797A 7B7C8000 00000000


temp is
    58B3B0F6 8DD4432B FE91AF80 FC822A3B 16D6D0E6 185F1A8D


------------

  BCC

  IV is
                                              00000003 00000000


  IV || S is
                                              00000003 00000000
    0000003A 0000001D 80818283 84858687 88898A8B 8C8D8E8F
    90919293 94959697 98999A9B 9C606162 63646566 6768696A
    6B6C6D6E 6F707172 73747576 7778797A 7B7C8000 00000000
```

```
    temp is
                                                58B3B0F6 8DD4432B
        FE91AF80 FC822A3B 16D6D0E6 185F1A8D 6A2FC76E 4B22E671


    ------------

    Key is
              58 B3B0F68D D4432BFE 91AF80FC 822A3B16 D6D0E618


    X is
                                                5F1A8D6A 2FC76E4B


Block #1
Blockin   5F1A8D6A 2FC76E4B
Blockout  8C09C342 0E2573AD

    ------------

      BlockEncrypt

      Key is
              58 B3B0F68D D4432BFE 91AF80FC 822A3B16 D6D0E618


      X is
                                                5F1A8D6A 2FC76E4B


      X = BlockEncrypt(Key, X) is
                                                8C09C342 0E2573AD


      temp is
                                                8C09C342 0E2573AD


Block #1
Blockin   8C09C342 0E2573AD
Blockout  6112E91C 0CAD6C1C

    ------------

      BlockEncrypt
```

```
      Key is
              58 B3B0F68D D4432BFE 91AF80FC 822A3B16 D6D0E618


      X is
                                              8C09C342 0E2573AD


      X = BlockEncrypt(Key, X) is
                                              6112E91C 0CAD6C1C


      temp is
                           8C09C342 0E2573AD 6112E91C 0CAD6C1C


Block #1
Blockin   6112E91C 0CAD6C1C
Blockout  164907D9 2BF94019

    ------------

      BlockEncrypt

      Key is
              58 B3B0F68D D4432BFE 91AF80FC 822A3B16 D6D0E618


      X is
                                              6112E91C 0CAD6C1C


      X = BlockEncrypt(Key, X) is
                                              164907D9 2BF94019


      temp is
        8C09C342 0E2573AD 6112E91C 0CAD6C1C 164907D9 2BF94019


Block #1
Blockin   164907D9 2BF94019
Blockout  1E666F08 6A5CDA45

    ------------
```

```
      BlockEncrypt

      Key is
              58 B3B0F68D D4432BFE 91AF80FC 822A3B16 D6D0E618


      X is
                                              164907D9 2BF94019


      X = BlockEncrypt(Key, X) is
                                              1E666F08 6A5CDA45


      temp is
                                              8C09C342 0E2573AD
        6112E91C 0CAD6C1C 164907D9 2BF94019 1E666F08 6A5CDA45


      requested_bits is
                                                    8C 09C3420E
        2573AD61 12E91C0C AD6C1C16 4907D92B F940191E 666F086A


---------------------------

  Update

    provided_data is
                                                    8C 09C3420E
        2573AD61 12E91C0C AD6C1C16 4907D92B F940191E 666F086A


    ------------

      While loop

      Key is
              A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7


      V is
                                              A9B33F73 FF1A992C
```

```
Block #1
Blockin   A9B33F73 FF1A992C
Blockout  ABC88224 514D0316

      output_block is
                                              ABC88224 514D0316


      temp is
                                              ABC88224 514D0316


    ------------

      While loop

      Key is
              A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7


      V is
                                              A9B33F73 FF1A992D


Block #1
Blockin   A9B33F73 FF1A992D
Blockout  EA3D48AE E3C9A2B4

      output_block is
                                              EA3D48AE E3C9A2B4


      temp is
                           ABC88224 514D0316 EA3D48AE E3C9A2B4


    ------------

      While loop

      Key is
              A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7


      V is
                                              A9B33F73 FF1A992E
```

```
Block #1
Blockin   A9B33F73 FF1A992E
Blockout  27CE2546 E5F9CE73

      output_block is
                                              27CE2546 E5F9CE73


      temp is
        ABC88224 514D0316 EA3D48AE E3C9A2B4 27CE2546 E5F9CE73


    ------------

      While loop

      Key is
              A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7


      V is
                                              A9B33F73 FF1A992F


Block #1
Blockin   A9B33F73 FF1A992F
Blockout  AC843CE9 A9F8B369

      output_block is
                                              AC843CE9 A9F8B369


      temp is
                                              ABC88224 514D0316
        EA3D48AE E3C9A2B4 27CE2546 E5F9CE73 AC843CE9 A9F8B369


    temp XOR provided_data is
                                                    27 C141665F
        6870BB8B 2FA1B2EF 64CEA831 87229FCE 008E6AB2 E253E1C3


    Key is
              27 C141665F 6870BB8B 2FA1B2EF 64CEA831 87229FCE
```

```
    V is
                                                008E6AB2 E253E1C3

**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   008E6AB2 E253E1C4
Blockout  0E389920 A09B485A

Block #1
Blockin   008E6AB2 E253E1C5
Blockout  A4ABD0CA 7E60D89C

---------------------------

  Update

    provided_data is
                                                      00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              27 C141665F 6870BB8B 2FA1B2EF 64CEA831 87229FCE


      V is
                                                008E6AB2 E253E1C6


Block #1
Blockin   008E6AB2 E253E1C6
Blockout  E86795D8 9BEA95E8
```

```
      output_block is
                                              E86795D8 9BEA95E8


      temp is
                                              E86795D8 9BEA95E8


    ------------

      While loop

      Key is
              27 C141665F 6870BB8B 2FA1B2EF 64CEA831 87229FCE


      V is
                                              008E6AB2 E253E1C7


Block #1
Blockin   008E6AB2 E253E1C7
Blockout  D96797E7 9FBF96CF

      output_block is
                                              D96797E7 9FBF96CF


      temp is
                           E86795D8 9BEA95E8 D96797E7 9FBF96CF


    ------------

      While loop

      Key is
              27 C141665F 6870BB8B 2FA1B2EF 64CEA831 87229FCE


      V is
                                              008E6AB2 E253E1C8


Block #1
```

```
Blockin   008E6AB2 E253E1C8
Blockout  EF2F0302 1D6B4659

      output_block is
                                              EF2F0302 1D6B4659


      temp is
        E86795D8 9BEA95E8 D96797E7 9FBF96CF EF2F0302 1D6B4659


    ------------

      While loop

      Key is
              27 C141665F 6870BB8B 2FA1B2EF 64CEA831 87229FCE


      V is
                                              008E6AB2 E253E1C9


Block #1
Blockin   008E6AB2 E253E1C9
Blockout  CBE50DE0 C2F290F8

      output_block is
                                              CBE50DE0 C2F290F8


      temp is
                                              E86795D8 9BEA95E8
        D96797E7 9FBF96CF EF2F0302 1D6B4659 CBE50DE0 C2F290F8


    temp XOR provided_data is
                                                    E8 6795D89B
        EA95E8D9 6797E79F BF96CFEF 2F03021D 6B4659CB E50DE0C2


    Key is
              E8 6795D89B EA95E8D9 6797E79F BF96CFEF 2F03021D


    V is
```

```
                                                6B4659CB E50DE0C2

rnd_val is
                             0E389920 A09B485A A4ABD0CA 7E60D89C

---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                        A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


Generate FAILED: Reseed is required
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    additional_input is
                                                        A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


---------------------------

  Block_Cipher_df

    input_str is
                                       C0C1 C2C3C4C5 C6C7C8C9
        CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCA0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC
```

```
number_of_bits_to_return = 232

S is
    0000003A 0000001D C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
    D0D1D2D3 D4D5D6D7 D8D9DADB DCA0A1A2 A3A4A5A6 A7A8A9AA
    ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBC8000 00000000


------------

  BCC

  IV is
                                        00000000 00000000


  IV || S is
                                        00000000 00000000
    0000003A 0000001D C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
    D0D1D2D3 D4D5D6D7 D8D9DADB DCA0A1A2 A3A4A5A6 A7A8A9AA
    ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBC8000 00000000


temp is
                                        D9863A5A 51A096BD


------------

  BCC

  IV is
                                        00000001 00000000


  IV || S is
                                        00000001 00000000
    0000003A 0000001D C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
    D0D1D2D3 D4D5D6D7 D8D9DADB DCA0A1A2 A3A4A5A6 A7A8A9AA
    ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBC8000 00000000


temp is
                    D9863A5A 51A096BD F2424B3F 81E02A6A
```

```
------------

  BCC

  IV is
                                          00000002 00000000


  IV || S is
                                          00000002 00000000
    0000003A 0000001D C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
    D0D1D2D3 D4D5D6D7 D8D9DADB DCA0A1A2 A3A4A5A6 A7A8A9AA
    ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBC8000 00000000


temp is
    D9863A5A 51A096BD F2424B3F 81E02A6A 451263CA 7D8B9E2A


------------

  BCC

  IV is
                                          00000003 00000000


  IV || S is
                                          00000003 00000000
    0000003A 0000001D C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
    D0D1D2D3 D4D5D6D7 D8D9DADB DCA0A1A2 A3A4A5A6 A7A8A9AA
    ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBC8000 00000000


temp is
                                          D9863A5A 51A096BD
    F2424B3F 81E02A6A 451263CA 7D8B9E2A 7BDA3AEE 6EF73C33


------------

Key is
          D9 863A5A51 A096BDF2 424B3F81 E02A6A45 1263CA7D
```

```
    X is
                                            8B9E2A7B DA3AEE6E


Block #1
Blockin   8B9E2A7B DA3AEE6E
Blockout  B1161FE3 3849916E

    ------------

      BlockEncrypt

      Key is
              D9 863A5A51 A096BDF2 424B3F81 E02A6A45 1263CA7D


      X is
                                            8B9E2A7B DA3AEE6E


      X = BlockEncrypt(Key, X) is
                                            B1161FE3 3849916E


      temp is
                                            B1161FE3 3849916E


Block #1
Blockin   B1161FE3 3849916E
Blockout  F1F20C6E 141630BE

    ------------

      BlockEncrypt

      Key is
              D9 863A5A51 A096BDF2 424B3F81 E02A6A45 1263CA7D


      X is
                                            B1161FE3 3849916E


      X = BlockEncrypt(Key, X) is
                                            F1F20C6E 141630BE
```

```
      temp is
                           B1161FE3 3849916E F1F20C6E 141630BE


Block #1
Blockin   F1F20C6E 141630BE
Blockout  20E312AC 5E3EDC6E

    ------------

      BlockEncrypt

      Key is
              D9 863A5A51 A096BDF2 424B3F81 E02A6A45 1263CA7D


      X is
                                           F1F20C6E 141630BE


      X = BlockEncrypt(Key, X) is
                                           20E312AC 5E3EDC6E


      temp is
        B1161FE3 3849916E F1F20C6E 141630BE 20E312AC 5E3EDC6E


Block #1
Blockin   20E312AC 5E3EDC6E
Blockout  7E5A819E D1AC80D7

    ------------

      BlockEncrypt

      Key is
              D9 863A5A51 A096BDF2 424B3F81 E02A6A45 1263CA7D


      X is
                                           20E312AC 5E3EDC6E
```

```
      X = BlockEncrypt(Key, X) is
                                                7E5A819E D1AC80D7


      temp is
                                               B1161FE3 3849916E
        F1F20C6E 141630BE 20E312AC 5E3EDC6E 7E5A819E D1AC80D7


      requested_bits is
                                                     B1 161FE338
        49916EF1 F20C6E14 1630BE20 E312AC5E 3EDC6E7E 5A819ED1


---------------------------

  Update

    provided_data is
                                                     B1 161FE338
        49916EF1 F20C6E14 1630BE20 E312AC5E 3EDC6E7E 5A819ED1


    ------------

      While loop

      Key is
              E8 6795D89B EA95E8D9 6797E79F BF96CFEF 2F03021D


      V is
                                               6B4659CB E50DE0C3


Block #1
Blockin   6B4659CB E50DE0C3
Blockout  70DDFA87 A0397904

      output_block is
                                               70DDFA87 A0397904


      temp is
                                               70DDFA87 A0397904
```

```
    ------------

      While loop

      Key is
              E8 6795D89B EA95E8D9 6797E79F BF96CFEF 2F03021D


      V is
                                            6B4659CB E50DE0C4


Block #1
Blockin   6B4659CB E50DE0C4
Blockout  FE4FBE4C 6A424E69

      output_block is
                                            FE4FBE4C 6A424E69


      temp is
                           70DDFA87 A0397904 FE4FBE4C 6A424E69


    ------------

      While loop

      Key is
              E8 6795D89B EA95E8D9 6797E79F BF96CFEF 2F03021D


      V is
                                            6B4659CB E50DE0C5


Block #1
Blockin   6B4659CB E50DE0C5
Blockout  13554524 8F4F80F9

      output_block is
                                            13554524 8F4F80F9


      temp is
```

```
        70DDFA87 A0397904 FE4FBE4C 6A424E69 13554524 8F4F80F9


    ------------

      While loop

      Key is
              E8 6795D89B EA95E8D9 6797E79F BF96CFEF 2F03021D


      V is
                                            6B4659CB E50DE0C6


Block #1
Blockin   6B4659CB E50DE0C6
Blockout  B9E4F088 CD467B59

      output_block is
                                            B9E4F088 CD467B59


      temp is
                                            70DDFA87 A0397904
        FE4FBE4C 6A424E69 13554524 8F4F80F9 B9E4F088 CD467B59


    temp XOR provided_data is
                                                  C1 CBE56498
        70E86A0F BDB2227E 547ED733 B65788D1 715C97C7 BE71161C


    Key is
              C1 CBE56498 70E86A0F BDB2227E 547ED733 B65788D1


    V is
                                            715C97C7 BE71161C


*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128
```

```
    additional_input is  <empty>

Block #1
Blockin   715C97C7 BE71161D
Blockout  F4478EC6 659A0D35

Block #1
Blockin   715C97C7 BE71161E
Blockout  77625B0C 73A211DD

---------------------------

  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              C1 CBE56498 70E86A0F BDB2227E 547ED733 B65788D1


      V is
                                              715C97C7 BE71161F


Block #1
Blockin   715C97C7 BE71161F
Blockout  37A7C1A9 50C0FB8B

      output_block is
                                              37A7C1A9 50C0FB8B


      temp is
                                              37A7C1A9 50C0FB8B


    ------------
```

```
      While loop

      Key is
              C1 CBE56498 70E86A0F BDB2227E 547ED733 B65788D1


      V is
                                            715C97C7 BE711620


Block #1
Blockin   715C97C7 BE711620
Blockout  C21DABCB FDDA18B1

      output_block is
                                            C21DABCB FDDA18B1


      temp is
                           37A7C1A9 50C0FB8B C21DABCB FDDA18B1


    ------------

      While loop

      Key is
              C1 CBE56498 70E86A0F BDB2227E 547ED733 B65788D1


      V is
                                            715C97C7 BE711621


Block #1
Blockin   715C97C7 BE711621
Blockout  9BB6CC23 85CD194A

      output_block is
                                            9BB6CC23 85CD194A


      temp is
        37A7C1A9 50C0FB8B C21DABCB FDDA18B1 9BB6CC23 85CD194A
```

```
    ------------

      While loop

      Key is
              C1 CBE56498 70E86A0F BDB2227E 547ED733 B65788D1


      V is
                                            715C97C7 BE711622


Block #1
Blockin   715C97C7 BE711622
Blockout  C7CE7521 4803115B

      output_block is
                                            C7CE7521 4803115B


      temp is
                                            37A7C1A9 50C0FB8B
        C21DABCB FDDA18B1 9BB6CC23 85CD194A C7CE7521 4803115B


    temp XOR provided_data is
                                                  37 A7C1A950
        C0FB8BC2 1DABCBFD DA18B19B B6CC2385 CD194AC7 CE752148


    Key is
              37 A7C1A950 C0FB8BC2 1DABCBFD DA18B19B B6CC2385


    V is
                                            CD194AC7 CE752148


rnd_val is
                          F4478EC6 659A0D35 77625B0C 73A211DD


################################################################

CTR_DRBG
```

```
    Requested Security Strength = 112

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                    00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    EntropyInput1 (for Reseed1) =
                                                    80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                    C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    Nonce =
                                                202122 23242526


    PersonalizationString =
                                                    40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    AdditionalInput = <empty>

###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                                                    00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    nonce is
                                                202122 23242526


    personal_str is
                                                    40 41424344
```

```
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                        00 01020304 05060708 090A0B0C 0D0E0F10
        11121314 15161718 191A1B1C 20212223 24252640 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    number_of_bits_to_return = 232

    S is
                                               00000041 0000001D
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C202122 23242526 40414243 44454647 48494A4B
        4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000


    ------------

      BCC

      IV is
                                               00000000 00000000


      IV || S is
                           00000000 00000000 00000041 0000001D
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C202122 23242526 40414243 44454647 48494A4B
        4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000


    temp is
                                               BF5C8905 7D02B0A6


    ------------

      BCC
```

```
  IV is
                                        00000001 00000000


  IV || S is
                      00000001 00000000 00000041 0000001D
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C202122 23242526 40414243 44454647 48494A4B
    4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000


temp is
                      BF5C8905 7D02B0A6 77FE7647 E9554668


------------

  BCC

  IV is
                                        00000002 00000000


  IV || S is
                      00000002 00000000 00000041 0000001D
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C202122 23242526 40414243 44454647 48494A4B
    4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000


temp is
    BF5C8905 7D02B0A6 77FE7647 E9554668 AE4D8DE0 DB992E46


------------

  BCC

  IV is
                                        00000003 00000000


  IV || S is
                      00000003 00000000 00000041 0000001D
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
```

```
        18191A1B 1C202122 23242526 40414243 44454647 48494A4B
        4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000


    temp is
                                               BF5C8905 7D02B0A6
        77FE7647 E9554668 AE4D8DE0 DB992E46 83E1389F 33A1E91F


    ------------

    Key is
              BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB


    X is
                                               992E4683 E1389F33


Block #1
Blockin   992E4683 E1389F33
Blockout  70F9F85E 350177E5

    ------------

      BlockEncrypt

      Key is
              BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB


      X is
                                               992E4683 E1389F33


      X = BlockEncrypt(Key, X) is
                                               70F9F85E 350177E5


      temp is
                                               70F9F85E 350177E5


Block #1
Blockin   70F9F85E 350177E5
Blockout  B228D49C 6374BBB6
```

```
    ------------

      BlockEncrypt

      Key is
              BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB


      X is
                                            70F9F85E 350177E5


      X = BlockEncrypt(Key, X) is
                                            B228D49C 6374BBB6


      temp is
                           70F9F85E 350177E5 B228D49C 6374BBB6


Block #1
Blockin   B228D49C 6374BBB6
Blockout  EA3DCFFA 463099CA

    ------------

      BlockEncrypt

      Key is
              BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB


      X is
                                            B228D49C 6374BBB6


      X = BlockEncrypt(Key, X) is
                                            EA3DCFFA 463099CA


      temp is
        70F9F85E 350177E5 B228D49C 6374BBB6 EA3DCFFA 463099CA


Block #1
```

```
Blockin   EA3DCFFA 463099CA
Blockout  F0781291 15A9A8E8

    ------------

      BlockEncrypt

      Key is
              BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB


      X is
                                            EA3DCFFA 463099CA


      X = BlockEncrypt(Key, X) is
                                            F0781291 15A9A8E8


      temp is
                                            70F9F85E 350177E5
        B228D49C 6374BBB6 EA3DCFFA 463099CA F0781291 15A9A8E8


      requested_bits is
                                                  70 F9F85E35
        0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115


    seed_material is
                                                  70 F9F85E35
        0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115


---------------------------

  Update

    provided_data is
                                                  70 F9F85E35
        0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115


    ------------

      While loop
```

```
      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                             00000000 00000001


Block #1
Blockin   00000000 00000001
Blockout  166B40B4 4ABA4BD6

      output_block is
                                             166B40B4 4ABA4BD6


      temp is
                                             166B40B4 4ABA4BD6


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                             00000000 00000002


Block #1
Blockin   00000000 00000002
Blockout  06E7EA22 CE92708F

      output_block is
                                             06E7EA22 CE92708F


      temp is
                           166B40B4 4ABA4BD6 06E7EA22 CE92708F


    ------------
```

```
      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                              4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000004


Block #1
Blockin   00000000 00000004
Blockout  D2FD8867 D50D2DFE

      output_block is
                                              D2FD8867 D50D2DFE


      temp is
                                              166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE
```

```
    temp XOR provided_data is
                                                    66 92B8EA7F
        BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4 CA8F5622 859AF6C0


    Key is
              66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4


    V is
                                           CA8F5622 859AF6C0


------------------------------------------------------------

First call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                                    80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    additional_input is  <empty>

---------------------------

  Block_Cipher_df

    input_str is
                                                    80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C
```

```
number_of_bits_to_return = 232

S is
                      0000001D 0000001D 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C800000


------------

  BCC

  IV is
                                         00000000 00000000


  IV || S is
    00000000 00000000 0000001D 0000001D 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C800000


temp is
                                         B435EC36 31249E3D


------------

  BCC

  IV is
                                         00000001 00000000


  IV || S is
    00000001 00000000 0000001D 0000001D 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C800000


temp is
                      B435EC36 31249E3D A735CE05 7E609075


------------

  BCC
```

```
      IV is
                                              00000002 00000000


      IV || S is
        00000002 00000000 0000001D 0000001D 80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C800000


    temp is
        B435EC36 31249E3D A735CE05 7E609075 CA6920F2 1DF7CB3D


    ------------

      BCC

      IV is
                                              00000003 00000000


      IV || S is
        00000003 00000000 0000001D 0000001D 80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C800000


    temp is
                                              B435EC36 31249E3D
        A735CE05 7E609075 CA6920F2 1DF7CB3D 6547CE54 BA8A17A5


    ------------

    Key is
              B4 35EC3631 249E3DA7 35CE057E 609075CA 6920F21D


    X is
                                              F7CB3D65 47CE54BA


Block #1
Blockin   F7CB3D65 47CE54BA
Blockout  7D3F6CAF 387E4C9A
```

```
    ------------

      BlockEncrypt

      Key is
              B4 35EC3631 249E3DA7 35CE057E 609075CA 6920F21D


      X is
                                           F7CB3D65 47CE54BA


      X = BlockEncrypt(Key, X) is
                                           7D3F6CAF 387E4C9A


      temp is
                                           7D3F6CAF 387E4C9A


Block #1
Blockin   7D3F6CAF 387E4C9A
Blockout  1A5787D4 81378C06

    ------------

      BlockEncrypt

      Key is
              B4 35EC3631 249E3DA7 35CE057E 609075CA 6920F21D


      X is
                                           7D3F6CAF 387E4C9A


      X = BlockEncrypt(Key, X) is
                                           1A5787D4 81378C06


      temp is
                           7D3F6CAF 387E4C9A 1A5787D4 81378C06


Block #1
Blockin   1A5787D4 81378C06
```

```
Blockout  C409511D DB736F2D

    ------------

      BlockEncrypt

      Key is
              B4 35EC3631 249E3DA7 35CE057E 609075CA 6920F21D


      X is
                                            1A5787D4 81378C06


      X = BlockEncrypt(Key, X) is
                                            C409511D DB736F2D


      temp is
        7D3F6CAF 387E4C9A 1A5787D4 81378C06 C409511D DB736F2D


Block #1
Blockin   C409511D DB736F2D
Blockout  D4CB361F 4C1392A0

    ------------

      BlockEncrypt

      Key is
              B4 35EC3631 249E3DA7 35CE057E 609075CA 6920F21D


      X is
                                            C409511D DB736F2D


      X = BlockEncrypt(Key, X) is
                                            D4CB361F 4C1392A0


      temp is
                                            7D3F6CAF 387E4C9A
        1A5787D4 81378C06 C409511D DB736F2D D4CB361F 4C1392A0
```

```
      requested_bits is
                                                        7D 3F6CAF38
        7E4C9A1A 5787D481 378C06C4 09511DDB 736F2DD4 CB361F4C


---------------------------

  Update

    provided_data is
                                                        7D 3F6CAF38
        7E4C9A1A 5787D481 378C06C4 09511DDB 736F2DD4 CB361F4C


    ------------

      While loop

      Key is
              66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4


      V is
                                              CA8F5622 859AF6C1


Block #1
Blockin   CA8F5622 859AF6C1
Blockout  760BED7D 92B083B1

      output_block is
                                              760BED7D 92B083B1


      temp is
                                              760BED7D 92B083B1


    ------------

      While loop

      Key is
              66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4
```

```
      V is
                                              CA8F5622 859AF6C2


Block #1
Blockin   CA8F5622 859AF6C2
Blockout  0AF31CF0 656081EB

      output_block is
                                              0AF31CF0 656081EB


      temp is
                           760BED7D 92B083B1 0AF31CF0 656081EB


    ------------

      While loop

      Key is
              66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4


      V is
                                              CA8F5622 859AF6C3


Block #1
Blockin   CA8F5622 859AF6C3
Blockout  51D241F0 2DA51012

      output_block is
                                              51D241F0 2DA51012


      temp is
        760BED7D 92B083B1 0AF31CF0 656081EB 51D241F0 2DA51012


    ------------

      While loop

      Key is
```

```
              66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4


      V is
                                              CA8F5622 859AF6C4


Block #1
Blockin   CA8F5622 859AF6C4
Blockout  AAF72BA5 971324B4

      output_block is
                                              AAF72BA5 971324B4


      temp is
                                              760BED7D 92B083B1
        0AF31CF0 656081EB 51D241F0 2DA51012 AAF72BA5 971324B4


    temp XOR provided_data is
                                                    0B 3481D2AA
        CECF2B10 A49B24E4 570DED95 DB10EDF6 D67F3F7E 3C1DBADB


    Key is
              0B 3481D2AA CECF2B10 A49B24E4 570DED95 DB10EDF6


    V is
                                              D67F3F7E 3C1DBADB


************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   D67F3F7E 3C1DBADC
Blockout  64983055 D014550B

Block #1
```

```
Blockin   D67F3F7E 3C1DBADD
Blockout  39DE699E 43130B64

---------------------------

  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              0B 3481D2AA CECF2B10 A49B24E4 570DED95 DB10EDF6


      V is
                                            D67F3F7E 3C1DBADE


Block #1
Blockin   D67F3F7E 3C1DBADE
Blockout  9895D584 68F52888

      output_block is
                                            9895D584 68F52888


      temp is
                                            9895D584 68F52888


    ------------

      While loop

      Key is
              0B 3481D2AA CECF2B10 A49B24E4 570DED95 DB10EDF6


      V is
                                            D67F3F7E 3C1DBADF
```

```
Block #1
Blockin   D67F3F7E 3C1DBADF
Blockout  90E0C91A FE19D323

      output_block is
                                              90E0C91A FE19D323


      temp is
                           9895D584 68F52888 90E0C91A FE19D323


    ------------

      While loop

      Key is
              0B 3481D2AA CECF2B10 A49B24E4 570DED95 DB10EDF6


      V is
                                              D67F3F7E 3C1DBAE0


Block #1
Blockin   D67F3F7E 3C1DBAE0
Blockout  FD2B846F 724CC5D6

      output_block is
                                              FD2B846F 724CC5D6


      temp is
        9895D584 68F52888 90E0C91A FE19D323 FD2B846F 724CC5D6


    ------------

      While loop

      Key is
              0B 3481D2AA CECF2B10 A49B24E4 570DED95 DB10EDF6
```

```
      V is
                                              D67F3F7E 3C1DBAE1


Block #1
Blockin   D67F3F7E 3C1DBAE1
Blockout  5F04A5D3 31851A8D

      output_block is
                                              5F04A5D3 31851A8D


      temp is
                                              9895D584 68F52888
        90E0C91A FE19D323 FD2B846F 724CC5D6 5F04A5D3 31851A8D


    temp XOR provided_data is
                                                    98 95D58468
        F5288890 E0C91AFE 19D323FD 2B846F72 4CC5D65F 04A5D331


    Key is
              98 95D58468 F5288890 E0C91AFE 19D323FD 2B846F72


    V is
                                              4CC5D65F 04A5D331


rnd_val is
                          64983055 D014550B 39DE699E 43130B64


------------------------------------------------------------

Second call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>
```

```
Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    additional_input is  <empty>

---------------------------

  Block_Cipher_df

    input_str is
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    number_of_bits_to_return = 232

    S is
                          0000001D 0000001D C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DC800000


    ------------

      BCC

      IV is
                                               00000000 00000000


      IV || S is
        00000000 00000000 0000001D 0000001D C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DC800000


    temp is
                                               75D864A6 B6D27B8E


    ------------
```

```
  BCC

  IV is
                                          00000001 00000000


  IV || S is
    00000001 00000000 0000001D 0000001D C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DC800000


temp is
                     75D864A6 B6D27B8E F1B88BC4 D95D7412


------------

  BCC

  IV is
                                          00000002 00000000


  IV || S is
    00000002 00000000 0000001D 0000001D C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DC800000


temp is
    75D864A6 B6D27B8E F1B88BC4 D95D7412 DA1D4B49 3894DD64


------------

  BCC

  IV is
                                          00000003 00000000


  IV || S is
    00000003 00000000 0000001D 0000001D C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DC800000
```

```
    temp is
                                                75D864A6 B6D27B8E
        F1B88BC4 D95D7412 DA1D4B49 3894DD64 1F27605F F6EAC071


    ------------

    Key is
              75 D864A6B6 D27B8EF1 B88BC4D9 5D7412DA 1D4B4938


    X is
                                                94DD641F 27605FF6


Block #1
Blockin   94DD641F 27605FF6
Blockout  1A1AD191 C4A0E7D1

    ------------

      BlockEncrypt

      Key is
              75 D864A6B6 D27B8EF1 B88BC4D9 5D7412DA 1D4B4938


      X is
                                                94DD641F 27605FF6


      X = BlockEncrypt(Key, X) is
                                                1A1AD191 C4A0E7D1


      temp is
                                                1A1AD191 C4A0E7D1


Block #1
Blockin   1A1AD191 C4A0E7D1
Blockout  EA461812 450132A6

    ------------

      BlockEncrypt
```

```
      Key is
              75 D864A6B6 D27B8EF1 B88BC4D9 5D7412DA 1D4B4938


      X is
                                           1A1AD191 C4A0E7D1


      X = BlockEncrypt(Key, X) is
                                           EA461812 450132A6


      temp is
                           1A1AD191 C4A0E7D1 EA461812 450132A6


Block #1
Blockin   EA461812 450132A6
Blockout  A84F5E05 D0A53DBD

    ------------

      BlockEncrypt

      Key is
              75 D864A6B6 D27B8EF1 B88BC4D9 5D7412DA 1D4B4938


      X is
                                           EA461812 450132A6


      X = BlockEncrypt(Key, X) is
                                           A84F5E05 D0A53DBD


      temp is
        1A1AD191 C4A0E7D1 EA461812 450132A6 A84F5E05 D0A53DBD


Block #1
Blockin   A84F5E05 D0A53DBD
Blockout  BCDC595B A4B22114

    ------------
```

```
      BlockEncrypt

      Key is
              75 D864A6B6 D27B8EF1 B88BC4D9 5D7412DA 1D4B4938


      X is
                                             A84F5E05 D0A53DBD


      X = BlockEncrypt(Key, X) is
                                             BCDC595B A4B22114


      temp is
                                             1A1AD191 C4A0E7D1
        EA461812 450132A6 A84F5E05 D0A53DBD BCDC595B A4B22114


      requested_bits is
                                                   1A 1AD191C4
        A0E7D1EA 46181245 0132A6A8 4F5E05D0 A53DBDBC DC595BA4


---------------------------

  Update

    provided_data is
                                                   1A 1AD191C4
        A0E7D1EA 46181245 0132A6A8 4F5E05D0 A53DBDBC DC595BA4


    ------------

      While loop

      Key is
              98 95D58468 F5288890 E0C91AFE 19D323FD 2B846F72


      V is
                                             4CC5D65F 04A5D332
```

```
Block #1
Blockin   4CC5D65F 04A5D332
Blockout  F72FD288 19F8D378

      output_block is
                                              F72FD288 19F8D378


      temp is
                                              F72FD288 19F8D378


    ------------

      While loop

      Key is
              98 95D58468 F5288890 E0C91AFE 19D323FD 2B846F72


      V is
                                              4CC5D65F 04A5D333


Block #1
Blockin   4CC5D65F 04A5D333
Blockout  97C5D167 6B2377A3

      output_block is
                                              97C5D167 6B2377A3


      temp is
                           F72FD288 19F8D378 97C5D167 6B2377A3


    ------------

      While loop

      Key is
              98 95D58468 F5288890 E0C91AFE 19D323FD 2B846F72


      V is
                                              4CC5D65F 04A5D334
```

```
Block #1
Blockin   4CC5D65F 04A5D334
Blockout  10A2DCAC ED13843B

      output_block is
                                              10A2DCAC ED13843B


      temp is
        F72FD288 19F8D378 97C5D167 6B2377A3 10A2DCAC ED13843B


    ------------

      While loop

      Key is
              98 95D58468 F5288890 E0C91AFE 19D323FD 2B846F72


      V is
                                              4CC5D65F 04A5D335


Block #1
Blockin   4CC5D65F 04A5D335
Blockout  AF0C7BB0 5CAE9CA7

      output_block is
                                              AF0C7BB0 5CAE9CA7


      temp is
                                              F72FD288 19F8D378
        97C5D167 6B2377A3 10A2DCAC ED13843B AF0C7BB0 5CAE9CA7


    temp XOR provided_data is
                                                    ED 350319DD
        5834A97D 83C9752E 224505B8 ED82A93D B6B98613 D022EBF8


    Key is
              ED 350319DD 5834A97D 83C9752E 224505B8 ED82A93D
```

```
    V is
                                                B6B98613 D022EBF8

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   B6B98613 D022EBF9
Blockout  035FDDA8 582A2214

Block #1
Blockin   B6B98613 D022EBFA
Blockout  EC722C41 0A8D95D3

---------------------------

  Update

    provided_data is
                                                      00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              ED 350319DD 5834A97D 83C9752E 224505B8 ED82A93D


      V is
                                                B6B98613 D022EBFB


Block #1
Blockin   B6B98613 D022EBFB
Blockout  1AB79F3A 952A33CF
```

```
      output_block is
                                              1AB79F3A 952A33CF


      temp is
                                              1AB79F3A 952A33CF


    ------------

      While loop

      Key is
              ED 350319DD 5834A97D 83C9752E 224505B8 ED82A93D


      V is
                                              B6B98613 D022EBFC


Block #1
Blockin   B6B98613 D022EBFC
Blockout  35BEA654 602509AC

      output_block is
                                              35BEA654 602509AC


      temp is
                           1AB79F3A 952A33CF 35BEA654 602509AC


    ------------

      While loop

      Key is
              ED 350319DD 5834A97D 83C9752E 224505B8 ED82A93D


      V is
                                              B6B98613 D022EBFD


Block #1
```

```
Blockin   B6B98613 D022EBFD
Blockout  8D121E67 D0FED235

      output_block is
                                              8D121E67 D0FED235


      temp is
        1AB79F3A 952A33CF 35BEA654 602509AC 8D121E67 D0FED235


    ------------

      While loop

      Key is
              ED 350319DD 5834A97D 83C9752E 224505B8 ED82A93D


      V is
                                              B6B98613 D022EBFE


Block #1
Blockin   B6B98613 D022EBFE
Blockout  84BC5D0B 6C5410EA

      output_block is
                                              84BC5D0B 6C5410EA


      temp is
                                              1AB79F3A 952A33CF
        35BEA654 602509AC 8D121E67 D0FED235 84BC5D0B 6C5410EA


    temp XOR provided_data is
                                                    1A B79F3A95
        2A33CF35 BEA65460 2509AC8D 121E67D0 FED23584 BC5D0B6C


    Key is
              1A B79F3A95 2A33CF35 BEA65460 2509AC8D 121E67D0


    V is
```

FED23584 BC5D0B6C

rnd_val is
035FDDA8 582A2214 EC722C41 0A8D95D3

##

CTR_DRBG

Requested Security Strength = 112

prediction_resistance_flag = "ENABLED"
EntropyInput =
00 01020304
05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C

EntropyInput1 (for Reseed1) =
80 81828384
85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C

EntropyInput2 (for Reseed2) =
C0 C1C2C3C4
C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC

Nonce =
202122 23242526

PersonalizationString =
40 41424344
45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C

AdditionalInput1 =
60 61626364
65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C

AdditionalInput2 =
A0 A1A2A3A4
A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC

```
################################################################

****************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    nonce is
                                                  202122 23242526


    personal_str is
                                                        40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                        00 01020304 05060708 090A0B0C 0D0E0F10
        11121314 15161718 191A1B1C 20212223 24252640 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    number_of_bits_to_return = 232

    S is
                                                 00000041 0000001D
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C202122 23242526 40414243 44454647 48494A4B
        4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000


    ------------

      BCC
```

```
  IV is
                                        00000000 00000000


  IV || S is
                      00000000 00000000 00000041 0000001D
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C202122 23242526 40414243 44454647 48494A4B
    4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000


temp is
                                        BF5C8905 7D02B0A6


------------

  BCC

  IV is
                                        00000001 00000000


  IV || S is
                      00000001 00000000 00000041 0000001D
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C202122 23242526 40414243 44454647 48494A4B
    4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000


temp is
                      BF5C8905 7D02B0A6 77FE7647 E9554668


------------

  BCC

  IV is
                                        00000002 00000000


  IV || S is
                      00000002 00000000 00000041 0000001D
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
```

```
        18191A1B 1C202122 23242526 40414243 44454647 48494A4B
        4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000


    temp is
        BF5C8905 7D02B0A6 77FE7647 E9554668 AE4D8DE0 DB992E46


    ------------

      BCC

      IV is
                                              00000003 00000000


      IV || S is
                           00000003 00000000 00000041 0000001D
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C202122 23242526 40414243 44454647 48494A4B
        4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000


    temp is
                                              BF5C8905 7D02B0A6
        77FE7647 E9554668 AE4D8DE0 DB992E46 83E1389F 33A1E91F


    ------------

    Key is
              BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB


    X is
                                              992E4683 E1389F33


Block #1
Blockin   992E4683 E1389F33
Blockout  70F9F85E 350177E5

    ------------

      BlockEncrypt
```

```
      Key is
              BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB


      X is
                                           992E4683 E1389F33


      X = BlockEncrypt(Key, X) is
                                           70F9F85E 350177E5


      temp is
                                           70F9F85E 350177E5


Block #1
Blockin   70F9F85E 350177E5
Blockout  B228D49C 6374BBB6

    ------------

      BlockEncrypt

      Key is
              BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB


      X is
                                           70F9F85E 350177E5


      X = BlockEncrypt(Key, X) is
                                           B228D49C 6374BBB6


      temp is
                           70F9F85E 350177E5 B228D49C 6374BBB6


Block #1
Blockin   B228D49C 6374BBB6
Blockout  EA3DCFFA 463099CA

    ------------
```

```
      BlockEncrypt

      Key is
              BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB


      X is
                                            B228D49C 6374BBB6


      X = BlockEncrypt(Key, X) is
                                            EA3DCFFA 463099CA


      temp is
        70F9F85E 350177E5 B228D49C 6374BBB6 EA3DCFFA 463099CA


Block #1
Blockin   EA3DCFFA 463099CA
Blockout  F0781291 15A9A8E8

    ------------

      BlockEncrypt

      Key is
              BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB


      X is
                                            EA3DCFFA 463099CA


      X = BlockEncrypt(Key, X) is
                                            F0781291 15A9A8E8


      temp is
                                            70F9F85E 350177E5
        B228D49C 6374BBB6 EA3DCFFA 463099CA F0781291 15A9A8E8


      requested_bits is
                                                  70 F9F85E35
        0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115
```

```
    seed_material is
                                                        70 F9F85E35
        0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115


---------------------------

  Update

    provided_data is
                                                        70 F9F85E35
        0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                               00000000 00000001


Block #1
Blockin   00000000 00000001
Blockout  166B40B4 4ABA4BD6

      output_block is
                                               166B40B4 4ABA4BD6


      temp is
                                               166B40B4 4ABA4BD6


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000
```

```
      V is
                                              00000000 00000002


Block #1
Blockin   00000000 00000002
Blockout  06E7EA22 CE92708F

      output_block is
                                              06E7EA22 CE92708F


      temp is
                           166B40B4 4ABA4BD6 06E7EA22 CE92708F


    ------------

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                              4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


    ------------

      While loop
```

```
      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000004


Block #1
Blockin   00000000 00000004
Blockout  D2FD8867 D50D2DFE

      output_block is
                                              D2FD8867 D50D2DFE


      temp is
                                              166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                    66 92B8EA7F
        BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4 CA8F5622 859AF6C0


    Key is
              66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4


    V is
                                              CA8F5622 859AF6C0


---------------------------------------------------------------

First call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                    60 61626364
```

```
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                                    80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    additional_input is
                                                    60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


---------------------------

  Block_Cipher_df

    input_str is
                                         8081 82838485 86878889
        8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


    number_of_bits_to_return = 232

    S is
        0000003A 0000001D 80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C606162 63646566 6768696A
        6B6C6D6E 6F707172 73747576 7778797A 7B7C8000 00000000


    ------------

      BCC

      IV is
                                               00000000 00000000


      IV || S is
                                               00000000 00000000
```

```
    0000003A 0000001D 80818283 84858687 88898A8B 8C8D8E8F
    90919293 94959697 98999A9B 9C606162 63646566 6768696A
    6B6C6D6E 6F707172 73747576 7778797A 7B7C8000 00000000


temp is
                                        58B3B0F6 8DD4432B


------------

  BCC

  IV is
                                        00000001 00000000


  IV || S is
                                        00000001 00000000
    0000003A 0000001D 80818283 84858687 88898A8B 8C8D8E8F
    90919293 94959697 98999A9B 9C606162 63646566 6768696A
    6B6C6D6E 6F707172 73747576 7778797A 7B7C8000 00000000


temp is
                     58B3B0F6 8DD4432B FE91AF80 FC822A3B


------------

  BCC

  IV is
                                        00000002 00000000


  IV || S is
                                        00000002 00000000
    0000003A 0000001D 80818283 84858687 88898A8B 8C8D8E8F
    90919293 94959697 98999A9B 9C606162 63646566 6768696A
    6B6C6D6E 6F707172 73747576 7778797A 7B7C8000 00000000


temp is
    58B3B0F6 8DD4432B FE91AF80 FC822A3B 16D6D0E6 185F1A8D
```

```
    ------------

      BCC

      IV is
                                              00000003 00000000


      IV || S is
                                              00000003 00000000
        0000003A 0000001D 80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C606162 63646566 6768696A
        6B6C6D6E 6F707172 73747576 7778797A 7B7C8000 00000000


    temp is
                                              58B3B0F6 8DD4432B
        FE91AF80 FC822A3B 16D6D0E6 185F1A8D 6A2FC76E 4B22E671


    ------------

    Key is
              58 B3B0F68D D4432BFE 91AF80FC 822A3B16 D6D0E618


    X is
                                              5F1A8D6A 2FC76E4B


Block #1
Blockin   5F1A8D6A 2FC76E4B
Blockout  8C09C342 0E2573AD

    ------------

      BlockEncrypt

      Key is
              58 B3B0F68D D4432BFE 91AF80FC 822A3B16 D6D0E618


      X is
                                              5F1A8D6A 2FC76E4B
```

```
      X = BlockEncrypt(Key, X) is
                                              8C09C342 0E2573AD


      temp is
                                              8C09C342 0E2573AD


Block #1
Blockin   8C09C342 0E2573AD
Blockout  6112E91C 0CAD6C1C

    ------------

      BlockEncrypt

      Key is
              58 B3B0F68D D4432BFE 91AF80FC 822A3B16 D6D0E618


      X is
                                              8C09C342 0E2573AD


      X = BlockEncrypt(Key, X) is
                                              6112E91C 0CAD6C1C


      temp is
                           8C09C342 0E2573AD 6112E91C 0CAD6C1C


Block #1
Blockin   6112E91C 0CAD6C1C
Blockout  164907D9 2BF94019

    ------------

      BlockEncrypt

      Key is
              58 B3B0F68D D4432BFE 91AF80FC 822A3B16 D6D0E618


      X is
```

```
                                          6112E91C 0CAD6C1C

      X = BlockEncrypt(Key, X) is
                                          164907D9 2BF94019

      temp is
        8C09C342 0E2573AD 6112E91C 0CAD6C1C 164907D9 2BF94019

Block #1
Blockin   164907D9 2BF94019
Blockout  1E666F08 6A5CDA45

    ------------

      BlockEncrypt

      Key is
              58 B3B0F68D D4432BFE 91AF80FC 822A3B16 D6D0E618

      X is
                                          164907D9 2BF94019

      X = BlockEncrypt(Key, X) is
                                          1E666F08 6A5CDA45

      temp is
                                          8C09C342 0E2573AD
        6112E91C 0CAD6C1C 164907D9 2BF94019 1E666F08 6A5CDA45

      requested_bits is
                                                 8C 09C3420E
        2573AD61 12E91C0C AD6C1C16 4907D92B F940191E 666F086A

---------------------------

  Update

    provided_data is
```

                                                    8C 09C3420E
        2573AD61 12E91C0C AD6C1C16 4907D92B F940191E 666F086A

      While loop

      Key is
              66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

      V is
                                          CA8F5622 859AF6C1

Block #1
Blockin   CA8F5622 859AF6C1
Blockout 760BED7D 92B083B1

      output_block is
                                          760BED7D 92B083B1

      temp is
                                          760BED7D 92B083B1

      While loop

      Key is
              66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

      V is
                                          CA8F5622 859AF6C2

Block #1
Blockin   CA8F5622 859AF6C2
Blockout 0AF31CF0 656081EB

      output_block is
                                          0AF31CF0 656081EB

```
      temp is
                           760BED7D 92B083B1 0AF31CF0 656081EB


    ------------

      While loop

      Key is
              66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4


      V is
                                             CA8F5622 859AF6C3


Block #1
Blockin   CA8F5622 859AF6C3
Blockout  51D241F0 2DA51012

      output_block is
                                             51D241F0 2DA51012


      temp is
        760BED7D 92B083B1 0AF31CF0 656081EB 51D241F0 2DA51012


    ------------

      While loop

      Key is
              66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4


      V is
                                             CA8F5622 859AF6C4


Block #1
Blockin   CA8F5622 859AF6C4
Blockout  AAF72BA5 971324B4
```

```
      output_block is
                                                AAF72BA5 971324B4


      temp is
                                                760BED7D 92B083B1
        0AF31CF0 656081EB 51D241F0 2DA51012 AAF72BA5 971324B4


    temp XOR provided_data is
                                                         FA 022E3F9C
        95F01C6B E1F5EC69 CDEDF747 9B462906 5C500BB4 9144ADFD


    Key is
              FA 022E3F9C 95F01C6B E1F5EC69 CDEDF747 9B462906


    V is
                                                5C500BB4 9144ADFD


************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   5C500BB4 9144ADFE
Blockout  A29C1A8C 42FBC562

Block #1
Blockin   5C500BB4 9144ADFF
Blockout  D7D1DBA7 DC541FFE

---------------------------

  Update

    provided_data is
                                                         00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
```

```
    ------------

      While loop

      Key is
              FA 022E3F9C 95F01C6B E1F5EC69 CDEDF747 9B462906


      V is
                                            5C500BB4 9144AE00


Block #1
Blockin   5C500BB4 9144AE00
Blockout  7B6D52C6 92B78B5E

      output_block is
                                            7B6D52C6 92B78B5E


      temp is
                                            7B6D52C6 92B78B5E


    ------------

      While loop

      Key is
              FA 022E3F9C 95F01C6B E1F5EC69 CDEDF747 9B462906


      V is
                                            5C500BB4 9144AE01


Block #1
Blockin   5C500BB4 9144AE01
Blockout  0308AE1A D67FDE94

      output_block is
                                            0308AE1A D67FDE94


      temp is
```

```
                          7B6D52C6 92B78B5E 0308AE1A D67FDE94


    ------------

      While loop

      Key is
              FA 022E3F9C 95F01C6B E1F5EC69 CDEDF747 9B462906


      V is
                                            5C500BB4 9144AE02


Block #1
Blockin   5C500BB4 9144AE02
Blockout  85499C53 54CC8C48

      output_block is
                                            85499C53 54CC8C48


      temp is
        7B6D52C6 92B78B5E 0308AE1A D67FDE94 85499C53 54CC8C48


    ------------

      While loop

      Key is
              FA 022E3F9C 95F01C6B E1F5EC69 CDEDF747 9B462906


      V is
                                            5C500BB4 9144AE03


Block #1
Blockin   5C500BB4 9144AE03
Blockout  75283B3B 6F13FD25

      output_block is
                                            75283B3B 6F13FD25
```

```
      temp is
                                                7B6D52C6 92B78B5E
        0308AE1A D67FDE94 85499C53 54CC8C48 75283B3B 6F13FD25


    temp XOR provided_data is
                                                      7B 6D52C692
        B78B5E03 08AE1AD6 7FDE9485 499C5354 CC8C4875 283B3B6F


    Key is
              7B 6D52C692 B78B5E03 08AE1AD6 7FDE9485 499C5354


    V is
                                                CC8C4875 283B3B6F


rnd_val is
                           A29C1A8C 42FBC562 D7D1DBA7 DC541FFE


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                      A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


Generate FAILED: Reseed is required
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                                      C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC
```

```
    additional_input is
                                                        A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


----------------------------

  Block_Cipher_df

    input_str is
                                       C0C1 C2C3C4C5 C6C7C8C9
        CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCA0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


    number_of_bits_to_return = 232

    S is
        0000003A 0000001D C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCA0A1A2 A3A4A5A6 A7A8A9AA
        ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBC8000 00000000


    ------------

      BCC

      IV is
                                               00000000 00000000


      IV || S is
                                               00000000 00000000
        0000003A 0000001D C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCA0A1A2 A3A4A5A6 A7A8A9AA
        ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBC8000 00000000


    temp is
                                               D9863A5A 51A096BD


    ------------
```

```
  BCC

  IV is
                                          00000001 00000000


  IV || S is
                                          00000001 00000000
    0000003A 0000001D C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
    D0D1D2D3 D4D5D6D7 D8D9DADB DCA0A1A2 A3A4A5A6 A7A8A9AA
    ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBC8000 00000000


temp is
                     D9863A5A 51A096BD F2424B3F 81E02A6A


------------

  BCC

  IV is
                                          00000002 00000000


  IV || S is
                                          00000002 00000000
    0000003A 0000001D C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
    D0D1D2D3 D4D5D6D7 D8D9DADB DCA0A1A2 A3A4A5A6 A7A8A9AA
    ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBC8000 00000000


temp is
    D9863A5A 51A096BD F2424B3F 81E02A6A 451263CA 7D8B9E2A


------------

  BCC

  IV is
                                          00000003 00000000


  IV || S is
                                          00000003 00000000
```

```
        0000003A 0000001D C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCA0A1A2 A3A4A5A6 A7A8A9AA
        ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBC8000 00000000


    temp is
                                            D9863A5A 51A096BD
        F2424B3F 81E02A6A 451263CA 7D8B9E2A 7BDA3AEE 6EF73C33


    ------------

    Key is
              D9 863A5A51 A096BDF2 424B3F81 E02A6A45 1263CA7D


    X is
                                            8B9E2A7B DA3AEE6E


Block #1
Blockin   8B9E2A7B DA3AEE6E
Blockout  B1161FE3 3849916E

    ------------

      BlockEncrypt

      Key is
              D9 863A5A51 A096BDF2 424B3F81 E02A6A45 1263CA7D


      X is
                                            8B9E2A7B DA3AEE6E


      X = BlockEncrypt(Key, X) is
                                            B1161FE3 3849916E


      temp is
                                            B1161FE3 3849916E


Block #1
Blockin   B1161FE3 3849916E
```

```
Blockout  F1F20C6E 141630BE

    ------------

      BlockEncrypt

      Key is
              D9 863A5A51 A096BDF2 424B3F81 E02A6A45 1263CA7D


      X is
                                            B1161FE3 3849916E


      X = BlockEncrypt(Key, X) is
                                            F1F20C6E 141630BE


      temp is
                           B1161FE3 3849916E F1F20C6E 141630BE


Block #1
Blockin   F1F20C6E 141630BE
Blockout  20E312AC 5E3EDC6E

    ------------

      BlockEncrypt

      Key is
              D9 863A5A51 A096BDF2 424B3F81 E02A6A45 1263CA7D


      X is
                                            F1F20C6E 141630BE


      X = BlockEncrypt(Key, X) is
                                            20E312AC 5E3EDC6E


      temp is
        B1161FE3 3849916E F1F20C6E 141630BE 20E312AC 5E3EDC6E
```

```
Block #1
Blockin   20E312AC 5E3EDC6E
Blockout  7E5A819E D1AC80D7

    ------------

      BlockEncrypt

      Key is
              D9 863A5A51 A096BDF2 424B3F81 E02A6A45 1263CA7D


      X is
                                            20E312AC 5E3EDC6E


      X = BlockEncrypt(Key, X) is
                                            7E5A819E D1AC80D7


      temp is
                                           B1161FE3 3849916E
        F1F20C6E 141630BE 20E312AC 5E3EDC6E 7E5A819E D1AC80D7


      requested_bits is
                                                      B1 161FE338
        49916EF1 F20C6E14 1630BE20 E312AC5E 3EDC6E7E 5A819ED1


---------------------------

  Update

    provided_data is
                                                      B1 161FE338
        49916EF1 F20C6E14 1630BE20 E312AC5E 3EDC6E7E 5A819ED1


    ------------

      While loop

      Key is
              7B 6D52C692 B78B5E03 08AE1AD6 7FDE9485 499C5354
```

```
      V is
                                              CC8C4875 283B3B70


Block #1
Blockin   CC8C4875 283B3B70
Blockout  329590B9 A8D9D6A2

      output_block is
                                              329590B9 A8D9D6A2


      temp is
                                              329590B9 A8D9D6A2


    ------------

      While loop

      Key is
              7B 6D52C692 B78B5E03 08AE1AD6 7FDE9485 499C5354


      V is
                                              CC8C4875 283B3B71


Block #1
Blockin   CC8C4875 283B3B71
Blockout  8F259854 CFA4C60B

      output_block is
                                              8F259854 CFA4C60B


      temp is
                           329590B9 A8D9D6A2 8F259854 CFA4C60B


    ------------

      While loop

      Key is
```

```
              7B 6D52C692 B78B5E03 08AE1AD6 7FDE9485 499C5354


      V is
                                              CC8C4875 283B3B72


Block #1
Blockin   CC8C4875 283B3B72
Blockout  E98501FA E0C5B9A4

      output_block is
                                              E98501FA E0C5B9A4


      temp is
        329590B9 A8D9D6A2 8F259854 CFA4C60B E98501FA E0C5B9A4


    ------------

      While loop

      Key is
              7B 6D52C692 B78B5E03 08AE1AD6 7FDE9485 499C5354


      V is
                                              CC8C4875 283B3B73


Block #1
Blockin   CC8C4875 283B3B73
Blockout  BAA36330 5349000E

      output_block is
                                              BAA36330 5349000E


      temp is
                                              329590B9 A8D9D6A2
        8F259854 CFA4C60B E98501FA E0C5B9A4 BAA36330 5349000E


    temp XOR provided_data is
                                                    83 838F5A90
```

```
        9047CC7E D7943ADB B2F6B5C9 661356BE FB65CAC4 F9E2AE82


    Key is
              83 838F5A90 9047CC7E D7943ADB B2F6B5C9 661356BE


    V is
                                             FB65CAC4 F9E2AE82

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   FB65CAC4 F9E2AE83
Blockout  0BDA66B0 49429061

Block #1
Blockin   FB65CAC4 F9E2AE84
Blockout  C013E422 8C2F44C6

---------------------------

  Update

    provided_data is
                                                    00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
              83 838F5A90 9047CC7E D7943ADB B2F6B5C9 661356BE


      V is
                                             FB65CAC4 F9E2AE85
```

```
Block #1
Blockin   FB65CAC4 F9E2AE85
Blockout  BA356571 5D258747

      output_block is
                                            BA356571 5D258747


      temp is
                                            BA356571 5D258747


    ------------

      While loop

      Key is
              83 838F5A90 9047CC7E D7943ADB B2F6B5C9 661356BE


      V is
                                            FB65CAC4 F9E2AE86


Block #1
Blockin   FB65CAC4 F9E2AE86
Blockout  A6E2CEBA 632C9DD2

      output_block is
                                            A6E2CEBA 632C9DD2


      temp is
                           BA356571 5D258747 A6E2CEBA 632C9DD2


    ------------

      While loop

      Key is
              83 838F5A90 9047CC7E D7943ADB B2F6B5C9 661356BE
```

```
      V is
                                              FB65CAC4 F9E2AE87


Block #1
Blockin   FB65CAC4 F9E2AE87
Blockout  B66272C0 A231A14B

      output_block is
                                              B66272C0 A231A14B


      temp is
        BA356571 5D258747 A6E2CEBA 632C9DD2 B66272C0 A231A14B


    ------------

      While loop

      Key is
              83 838F5A90 9047CC7E D7943ADB B2F6B5C9 661356BE


      V is
                                              FB65CAC4 F9E2AE88


Block #1
Blockin   FB65CAC4 F9E2AE88
Blockout  DFCC9637 A4B325C9

      output_block is
                                              DFCC9637 A4B325C9


      temp is
                                              BA356571 5D258747
        A6E2CEBA 632C9DD2 B66272C0 A231A14B DFCC9637 A4B325C9


    temp XOR provided_data is
                                                    BA 3565715D
        258747A6 E2CEBA63 2C9DD2B6 6272C0A2 31A14BDF CC9637A4
```

```
    Key is
              BA 3565715D 258747A6 E2CEBA63 2C9DD2B6 6272C0A2


    V is
                                             31A14BDF CC9637A4


rnd_val is
                           0BDA66B0 49429061 C013E422 8C2F44C6


###############################################################

CTR_DRBG

    Requested Security Strength = 128

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                             00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                             80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                             C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    Nonce =
                                             20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************
```

```
CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    nonce is
                                                20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                            00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    number_of_bits_to_return = 256

    S is
                            00000028 00000020 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 80000000 00000000 00000000 00000000


    ------------

      BCC

      IV is
                            00000000 00000000 00000000 00000000


      IV || S is
                                                00000000 00000000
        00000000 00000000 00000028 00000020 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 80000000 00000000 00000000 00000000
```

```
temp is
                    834EBAD8 5C601126 1D1D9DF4 C42A1544


------------

  BCC

  IV is
                    00000001 00000000 00000000 00000000


  IV || S is
                                        00000001 00000000
    00000000 00000000 00000028 00000020 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 80000000 00000000 00000000 00000000


temp is
                                        834EBAD8 5C601126
    1D1D9DF4 C42A1544 8EA249C1 226F0474 F3C55519 CB3677D2


------------

Key is
                    834EBAD8 5C601126 1D1D9DF4 C42A1544


X is
                    8EA249C1 226F0474 F3C55519 CB3677D2


------------

  BlockEncrypt

  Key is
                    834EBAD8 5C601126 1D1D9DF4 C42A1544


  X is
                    8EA249C1 226F0474 F3C55519 CB3677D2
```

```
      X = BlockEncrypt(Key, X) is
                          B8823BC4 F3AFBB6B A0373C69 BC49E2F6


      temp is
                          B8823BC4 F3AFBB6B A0373C69 BC49E2F6


    ------------

      BlockEncrypt

      Key is
                          834EBAD8 5C601126 1D1D9DF4 C42A1544


      X is
                          B8823BC4 F3AFBB6B A0373C69 BC49E2F6


      X = BlockEncrypt(Key, X) is
                          560EDE12 D8335B64 F5647FA0 A644162B


      temp is
                                              B8823BC4 F3AFBB6B
        A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B


      requested_bits is
                                              B8823BC4 F3AFBB6B
        A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B


    seed_material is
                                              B8823BC4 F3AFBB6B
        A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B


---------------------------

  Update

    provided_data is
                                              B8823BC4 F3AFBB6B
```

```
    A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B


------------

  While loop

  Key is
                      00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000001


  output_block is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A


  temp is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A


------------

  While loop

  Key is
                      00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000002


  output_block is
                      0388DACE 60B6A392 F328C2B9 71B2FE78


  temp is
                                        58E2FCCE FA7E3061
    367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78


temp XOR provided_data is
                                        E060C70A 09D18B0A
```

```
        9648213E 18AEA7AC 558604DC B885F8F6 064CBD19 D7F6E853

    Key is
                         E060C70A 09D18B0A 9648213E 18AEA7AC

    V is
                         558604DC B885F8F6 064CBD19 D7F6E853

-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                                                 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                         E060C70A 09D18B0A 9648213E 18AEA7AC

      V is
                         558604DC B885F8F6 064CBD19 D7F6E856

      output_block is
                         06EFCAB8 8D90354C 705D9E1A 6597070D
```

```
      temp is
                          06EFCAB8 8D90354C 705D9E1A 6597070D


    ------------

      While loop

      Key is
                          E060C70A 09D18B0A 9648213E 18AEA7AC


      V is
                          558604DC B885F8F6 064CBD19 D7F6E857


      output_block is
                          EFCC61E1 D29E976B 28E06845 E4E31B55


      temp is
                                            06EFCAB8 8D90354C
        705D9E1A 6597070D EFCC61E1 D29E976B 28E06845 E4E31B55


    temp XOR provided_data is
                                            06EFCAB8 8D90354C
        705D9E1A 6597070D EFCC61E1 D29E976B 28E06845 E4E31B55


    Key is
                          06EFCAB8 8D90354C 705D9E1A 6597070D


    V is
                          EFCC61E1 D29E976B 28E06845 E4E31B55


rnd_val is
                                            8CF59C8C F6888B96
        EB1C1E3E 79D82387 AF08A9E5 FF75E23F 1FBCD455 9B6B997E


------------------------------------------------------------
```

```
Second call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                                                 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                          06EFCAB8 8D90354C 705D9E1A 6597070D


      V is
                          EFCC61E1 D29E976B 28E06845 E4E31B58


      output_block is
                          666D019E CB5C9650 0BA95E80 57F9E1B9


      temp is
                          666D019E CB5C9650 0BA95E80 57F9E1B9


    ------------

      While loop

      Key is
                          06EFCAB8 8D90354C 705D9E1A 6597070D
```

```
      V is
                          EFCC61E1 D29E976B 28E06845 E4E31B59

      output_block is
                          D6E7980D 821EF067 2874863C 4F086FE3

      temp is
                                                666D019E CB5C9650
        0BA95E80 57F9E1B9 D6E7980D 821EF067 2874863C 4F086FE3

    temp XOR provided_data is
                                                666D019E CB5C9650
        0BA95E80 57F9E1B9 D6E7980D 821EF067 2874863C 4F086FE3

    Key is
                          666D019E CB5C9650 0BA95E80 57F9E1B9

    V is
                          D6E7980D 821EF067 2874863C 4F086FE3

rnd_val is
                                                69CDEF91 2C692D61
        B1DA4C05 146B52EB 7B8849BD 87937835 328254EC 25A9180E

##############################################################

CTR_DRBG

    Requested Security Strength = 128

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F

    EntropyInput1 (for Reseed1) =
```

```
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    Nonce =
                                                20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    AdditionalInput2 =
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


##################################################################

******************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    nonce is
                                                20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------
```

```
Block_Cipher_df

  input_str is
                        00010203 04050607 08090A0B 0C0D0E0F
      10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


  number_of_bits_to_return = 256

  S is
                        00000028 00000020 00010203 04050607
      08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
      20212223 24252627 80000000 00000000 00000000 00000000


  ------------

    BCC

    IV is
                        00000000 00000000 00000000 00000000


    IV || S is
                                           00000000 00000000
      00000000 00000000 00000028 00000020 00010203 04050607
      08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
      20212223 24252627 80000000 00000000 00000000 00000000


  temp is
                        834EBAD8 5C601126 1D1D9DF4 C42A1544


  ------------

    BCC

    IV is
                        00000001 00000000 00000000 00000000


    IV || S is
                                           00000001 00000000
      00000000 00000000 00000028 00000020 00010203 04050607
      08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
```

```
    20212223 24252627 80000000 00000000 00000000 00000000


temp is
                                          834EBAD8 5C601126
    1D1D9DF4 C42A1544 8EA249C1 226F0474 F3C55519 CB3677D2


------------

Key is
                      834EBAD8 5C601126 1D1D9DF4 C42A1544


X is
                      8EA249C1 226F0474 F3C55519 CB3677D2


------------

  BlockEncrypt

  Key is
                      834EBAD8 5C601126 1D1D9DF4 C42A1544


  X is
                      8EA249C1 226F0474 F3C55519 CB3677D2


  X = BlockEncrypt(Key, X) is
                      B8823BC4 F3AFBB6B A0373C69 BC49E2F6


  temp is
                      B8823BC4 F3AFBB6B A0373C69 BC49E2F6


------------

  BlockEncrypt

  Key is
                      834EBAD8 5C601126 1D1D9DF4 C42A1544
```

```
      X is
                          B8823BC4 F3AFBB6B A0373C69 BC49E2F6

      X = BlockEncrypt(Key, X) is
                          560EDE12 D8335B64 F5647FA0 A644162B

      temp is
                                            B8823BC4 F3AFBB6B
        A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B

      requested_bits is
                                            B8823BC4 F3AFBB6B
        A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B

    seed_material is
                                            B8823BC4 F3AFBB6B
        A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B

---------------------------

  Update

    provided_data is
                                            B8823BC4 F3AFBB6B
        A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B

    ------------

      While loop

      Key is
                          00000000 00000000 00000000 00000000

      V is
                          00000000 00000000 00000000 00000001

      output_block is
                          58E2FCCE FA7E3061 367F1D57 A4E7455A
```

```
      temp is
                          58E2FCCE FA7E3061 367F1D57 A4E7455A


    ------------

      While loop

      Key is
                          00000000 00000000 00000000 00000000


      V is
                          00000000 00000000 00000000 00000002


      output_block is
                          0388DACE 60B6A392 F328C2B9 71B2FE78


      temp is
                                               58E2FCCE FA7E3061
        367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78


    temp XOR provided_data is
                                               E060C70A 09D18B0A
        9648213E 18AEA7AC 558604DC B885F8F6 064CBD19 D7F6E853


    Key is
                          E060C70A 09D18B0A 9648213E 18AEA7AC


    V is
                          558604DC B885F8F6 064CBD19 D7F6E853


------------------------------------------------------------

First call to Generate

************************************************************
```

```
CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                                60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


  additional_input <> NULL, process appropriately
----------------------------

  Block_Cipher_df

    input_str is
                                                60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    number_of_bits_to_return = 256

    S is
        00000020 00000020 60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000


    ------------

      BCC

      IV is
                           00000000 00000000 00000000 00000000


      IV || S is
                           00000000 00000000 00000000 00000000
        00000020 00000020 60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000


    temp is
                           1E28FC96 A28B1550 8D8FC557 2B37CD4A


    ------------
```

```
  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
                      00000001 00000000 00000000 00000000
    00000020 00000020 60616263 64656667 68696A6B 6C6D6E6F
    70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000


temp is
                                          1E28FC96 A28B1550
    8D8FC557 2B37CD4A 857D7807 8DB171BF 8894073D E0C07B85


------------

Key is
                      1E28FC96 A28B1550 8D8FC557 2B37CD4A


X is
                      857D7807 8DB171BF 8894073D E0C07B85


------------

  BlockEncrypt

  Key is
                      1E28FC96 A28B1550 8D8FC557 2B37CD4A


  X is
                      857D7807 8DB171BF 8894073D E0C07B85


  X = BlockEncrypt(Key, X) is
                      C9172CDC 185A4A36 9E62578A F8F7C107


  temp is
                      C9172CDC 185A4A36 9E62578A F8F7C107
```

```
    ------------

      BlockEncrypt

      Key is
                           1E28FC96 A28B1550 8D8FC557 2B37CD4A


      X is
                           C9172CDC 185A4A36 9E62578A F8F7C107


      X = BlockEncrypt(Key, X) is
                           62DC9AD4 254F6BE9 0497C56E DE6C9AA5


      temp is
                                             C9172CDC 185A4A36
        9E62578A F8F7C107 62DC9AD4 254F6BE9 0497C56E DE6C9AA5


      requested_bits is
                                             C9172CDC 185A4A36
        9E62578A F8F7C107 62DC9AD4 254F6BE9 0497C56E DE6C9AA5


---------------------------

  Update

    provided_data is
                                             C9172CDC 185A4A36
        9E62578A F8F7C107 62DC9AD4 254F6BE9 0497C56E DE6C9AA5


    ------------

      While loop

      Key is
                           E060C70A 09D18B0A 9648213E 18AEA7AC


      V is
                           558604DC B885F8F6 064CBD19 D7F6E854
```

```
      output_block is
                           8CF59C8C F6888B96 EB1C1E3E 79D82387

      temp is
                           8CF59C8C F6888B96 EB1C1E3E 79D82387

    ------------

      While loop

      Key is
                           E060C70A 09D18B0A 9648213E 18AEA7AC

      V is
                           558604DC B885F8F6 064CBD19 D7F6E855

      output_block is
                           AF08A9E5 FF75E23F 1FBCD455 9B6B997E

      temp is
                                                 8CF59C8C F6888B96
        EB1C1E3E 79D82387 AF08A9E5 FF75E23F 1FBCD455 9B6B997E

    temp XOR provided_data is
                                                 45E2B050 EED2C1A0
       757E49B4 812FE280 CDD43331 DA3A89D6 1B2B113B 450703DB

    Key is
                           45E2B050 EED2C1A0 757E49B4 812FE280

    V is
                           CDD43331 DA3A89D6 1B2B113B 450703DB

---------------------------
```

```
Update

  provided_data is
                                              C9172CDC 185A4A36
      9E62578A F8F7C107 62DC9AD4 254F6BE9 0497C56E DE6C9AA5


  ------------

    While loop

    Key is
                        45E2B050 EED2C1A0 757E49B4 812FE280


    V is
                        CDD43331 DA3A89D6 1B2B113B 450703DE


    output_block is
                        DD30431A 73450CF7 CB2BE2DC 06B9F4AE


    temp is
                        DD30431A 73450CF7 CB2BE2DC 06B9F4AE


  ------------

    While loop

    Key is
                        45E2B050 EED2C1A0 757E49B4 812FE280


    V is
                        CDD43331 DA3A89D6 1B2B113B 450703DF


    output_block is
                        F66934E9 C07C869A D456AEB6 CCEAFFC6


    temp is
                                              DD30431A 73450CF7
      CB2BE2DC 06B9F4AE F66934E9 C07C869A D456AEB6 CCEAFFC6
```

```
    temp XOR provided_data is
                                            14276FC6 6B1F46C1
        5549B556 FE4E35A9 94B5AE3D E533ED73 D0C16BD8 12866563


    Key is
                          14276FC6 6B1F46C1 5549B556 FE4E35A9


    V is
                          94B5AE3D E533ED73 D0C16BD8 12866563


rnd_val is
                                            E8C74A4B 7BFFB53B
        EB80E78C A86BB6DF 70E2032A EB473E0D D54D2339 CEFCE9D0


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


  additional_input <> NULL, process appropriately
--------------------------

  Block_Cipher_df

    input_str is
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    number_of_bits_to_return = 256
```

```
S is
    00000020 00000020 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
    B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000


------------

  BCC

  IV is
                     00000000 00000000 00000000 00000000


  IV || S is
                     00000000 00000000 00000000 00000000
    00000020 00000020 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
    B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000


temp is
                     2A2E34C4 CF921C78 51C82FB6 11B3AD80


------------

  BCC

  IV is
                     00000001 00000000 00000000 00000000


  IV || S is
                     00000001 00000000 00000000 00000000
    00000020 00000020 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
    B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000


temp is
                                        2A2E34C4 CF921C78
    51C82FB6 11B3AD80 AF942BCE FE572E5A 0ABD1E75 F20EC649


------------

Key is
```

```
                    2A2E34C4 CF921C78 51C82FB6 11B3AD80

X is
                    AF942BCE FE572E5A 0ABD1E75 F20EC649

------------

  BlockEncrypt

  Key is
                    2A2E34C4 CF921C78 51C82FB6 11B3AD80

  X is
                    AF942BCE FE572E5A 0ABD1E75 F20EC649

  X = BlockEncrypt(Key, X) is
                    83D41C94 8108B4D5 1B5D2980 046BD7F4

  temp is
                    83D41C94 8108B4D5 1B5D2980 046BD7F4

------------

  BlockEncrypt

  Key is
                    2A2E34C4 CF921C78 51C82FB6 11B3AD80

  X is
                    83D41C94 8108B4D5 1B5D2980 046BD7F4

  X = BlockEncrypt(Key, X) is
                    A6A7B2A0 DD3DD0C6 123C4186 842C1270

  temp is
                                      83D41C94 8108B4D5
    1B5D2980 046BD7F4 A6A7B2A0 DD3DD0C6 123C4186 842C1270
```

```
      requested_bits is
                                                83D41C94 8108B4D5
        1B5D2980 046BD7F4 A6A7B2A0 DD3DD0C6 123C4186 842C1270


---------------------------

  Update

    provided_data is
                                                83D41C94 8108B4D5
        1B5D2980 046BD7F4 A6A7B2A0 DD3DD0C6 123C4186 842C1270


    ------------

      While loop

      Key is
                           14276FC6 6B1F46C1 5549B556 FE4E35A9


      V is
                           94B5AE3D E533ED73 D0C16BD8 12866564


      output_block is
                           05F50BB2 529B7C91 BBD09DD8 58C7CA6A


      temp is
                           05F50BB2 529B7C91 BBD09DD8 58C7CA6A


    ------------

      While loop

      Key is
                           14276FC6 6B1F46C1 5549B556 FE4E35A9


      V is
                           94B5AE3D E533ED73 D0C16BD8 12866565
```

```
      output_block is
                           ACC0BF92 8CBD5A5F 7E9876CD D9CC2C40

      temp is
                                                 05F50BB2 529B7C91
        BBD09DD8 58C7CA6A ACC0BF92 8CBD5A5F 7E9876CD D9CC2C40

    temp XOR provided_data is
                                                 86211726 D393C844
        A08DB458 5CAC1D9E 0A670D32 51808A99 6CA4374B 5DE03E30

    Key is
                           86211726 D393C844 A08DB458 5CAC1D9E

    V is
                           0A670D32 51808A99 6CA4374B 5DE03E30

---------------------------

  Update

    provided_data is
                                                 83D41C94 8108B4D5
        1B5D2980 046BD7F4 A6A7B2A0 DD3DD0C6 123C4186 842C1270

    ------------

      While loop

      Key is
                           86211726 D393C844 A08DB458 5CAC1D9E

      V is
                           0A670D32 51808A99 6CA4374B 5DE03E33

      output_block is
```

```
                        F252A225 68371777 1DB64C49 EF80EAAC

      temp is
                        F252A225 68371777 1DB64C49 EF80EAAC

    ------------

      While loop

      Key is
                        86211726 D393C844 A08DB458 5CAC1D9E

      V is
                        0A670D32 51808A99 6CA4374B 5DE03E34

      output_block is
                        A4B5046C 96296D2C 0E9714AC 958FFFE2

      temp is
                                          F252A225 68371777
        1DB64C49 EF80EAAC A4B5046C 96296D2C 0E9714AC 958FFFE2

    temp XOR provided_data is
                                          7186BEB1 E93FA3A2
       06EB65C9 EBEB3D58 0212B6CC 4B14BDEA 1CAB552A 11A3ED92

    Key is
                        7186BEB1 E93FA3A2 06EB65C9 EBEB3D58

    V is
                        0212B6CC 4B14BDEA 1CAB552A 11A3ED92

rnd_val is
                                          26B3F823 B4DBAFC2
        3B141375 E10B3AEB 7A0B5DEF 1C7D760B 6F827D01 ECD17AC7
```

```
###############################################################

CTR_DRBG

    Requested Security Strength = 128

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                            00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                            80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                            C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    Nonce =
                                            20212223 24252627


    PersonalizationString =
                                            40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    AdditionalInput = <empty>

###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                                            00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    nonce is
                                            20212223 24252627
```

```
    personal_str is
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    prediction_resistance_flag = "No PredictionResistance"

--------------------------

  Block_Cipher_df

    input_str is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    number_of_bits_to_return = 256

    S is
        00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000


    ------------

      BCC

      IV is
                           00000000 00000000 00000000 00000000


      IV || S is
                           00000000 00000000 00000000 00000000
        00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000


    temp is
                           C4C14823 AE157968 6F2C4676 8030DE37
```

```
------------

  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
                      00000001 00000000 00000000 00000000
    00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
    40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
    58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000


temp is
                                        C4C14823 AE157968
    6F2C4676 8030DE37 95EC1158 E6CD251C 577C6047 EBFFB5FE


------------

Key is
                      C4C14823 AE157968 6F2C4676 8030DE37


X is
                      95EC1158 E6CD251C 577C6047 EBFFB5FE


------------

  BlockEncrypt

  Key is
                      C4C14823 AE157968 6F2C4676 8030DE37


  X is
                      95EC1158 E6CD251C 577C6047 EBFFB5FE


  X = BlockEncrypt(Key, X) is
```

```
                        C2659E6A EFBB0DFB 2096A598 CC1C509F

      temp is
                        C2659E6A EFBB0DFB 2096A598 CC1C509F

    ------------

      BlockEncrypt

      Key is
                        C4C14823 AE157968 6F2C4676 8030DE37

      X is
                        C2659E6A EFBB0DFB 2096A598 CC1C509F

      X = BlockEncrypt(Key, X) is
                        D926A4C1 E62F8936 D419709D 6124946A

      temp is
                                          C2659E6A EFBB0DFB
        2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

      requested_bits is
                                          C2659E6A EFBB0DFB
        2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

    seed_material is
                                          C2659E6A EFBB0DFB
        2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

---------------------------

  Update

    provided_data is
                                          C2659E6A EFBB0DFB
        2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A
```

```
------------

  While loop

  Key is
                      00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000001

  output_block is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A

  temp is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A

------------

  While loop

  Key is
                      00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000002

  output_block is
                      0388DACE 60B6A392 F328C2B9 71B2FE78

  temp is
                                        58E2FCCE FA7E3061
    367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78

temp XOR provided_data is
                                        9A8762A4 15C53D9A
    16E9B8CF 68FB15C5 DAAE7E0F 86992AA4 2731B224 10966A12
```

```
    Key is
                          9A8762A4 15C53D9A 16E9B8CF 68FB15C5

    V is
                          DAAE7E0F 86992AA4 2731B224 10966A12

-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                                                 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                          9A8762A4 15C53D9A 16E9B8CF 68FB15C5

      V is
                          DAAE7E0F 86992AA4 2731B224 10966A15

      output_block is
                          74723E58 EE02C39B 247A781A 780DC1AE
```

```
      temp is
                          74723E58 EE02C39B 247A781A 780DC1AE


    ------------

      While loop

      Key is
                          9A8762A4 15C53D9A 16E9B8CF 68FB15C5


      V is
                          DAAE7E0F 86992AA4 2731B224 10966A16


      output_block is
                          EAF09A38 8B7E7D0A BA59FDED 97C93019


      temp is
                                               74723E58 EE02C39B
        247A781A 780DC1AE EAF09A38 8B7E7D0A BA59FDED 97C93019


    temp XOR provided_data is
                                               74723E58 EE02C39B
        247A781A 780DC1AE EAF09A38 8B7E7D0A BA59FDED 97C93019


    Key is
                          74723E58 EE02C39B 247A781A 780DC1AE


    V is
                          EAF09A38 8B7E7D0A BA59FDED 97C93019


rnd_val is
                                               18FDEFBD C43D7A36
        D5D6D862 205765D1 D701C9F2 37007030 DF1B8E70 EE4EEE29


---------------------------------------------------------------

Second call to Generate
```

```
***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                                                 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                           74723E58 EE02C39B 247A781A 780DC1AE


      V is
                           EAF09A38 8B7E7D0A BA59FDED 97C9301C


      output_block is
                           7913991A 10063ACE DB602FDB 00AD2197


      temp is
                           7913991A 10063ACE DB602FDB 00AD2197


    ------------

      While loop

      Key is
                           74723E58 EE02C39B 247A781A 780DC1AE
```

```
      V is
                          EAF09A38 8B7E7D0A BA59FDED 97C9301D


      output_block is
                          F472A839 C98EE0A4 B7C5571C 6FDFF7D7


      temp is
                                                   7913991A 10063ACE
        DB602FDB 00AD2197 F472A839 C98EE0A4 B7C5571C 6FDFF7D7


    temp XOR provided_data is
                                                   7913991A 10063ACE
        DB602FDB 00AD2197 F472A839 C98EE0A4 B7C5571C 6FDFF7D7


    Key is
                          7913991A 10063ACE DB602FDB 00AD2197


    V is
                          F472A839 C98EE0A4 B7C5571C 6FDFF7D7


rnd_val is
                                                   9888F1D3 8BB1CCE3
        1B363AA1 BD9B3961 6876C30D EE1FF0B7 BD8C4C44 1715C833


################################################################

CTR_DRBG

    Requested Security Strength = 128

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                   00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                                   80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
```

```
    EntropyInput2 (for Reseed2) =
                                            C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF

    Nonce =
                                            20212223 24252627

    PersonalizationString =
                                            40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F

    AdditionalInput1 =
                                            60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F

    AdditionalInput2 =
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF

##################################################################

******************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                                            00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F

    nonce is
                                            20212223 24252627

    personal_str is
                                            40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
```

```
    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    number_of_bits_to_return = 256

    S is
        00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000


    ------------

      BCC

      IV is
                           00000000 00000000 00000000 00000000


      IV || S is
                           00000000 00000000 00000000 00000000
        00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000


    temp is
                           C4C14823 AE157968 6F2C4676 8030DE37


    ------------

      BCC

      IV is
```

```
                    00000001 00000000 00000000 00000000

  IV || S is
                    00000001 00000000 00000000 00000000
    00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
    40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
    58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000


temp is
                                        C4C14823 AE157968
    6F2C4676 8030DE37 95EC1158 E6CD251C 577C6047 EBFFB5FE


------------

Key is
                    C4C14823 AE157968 6F2C4676 8030DE37


X is
                    95EC1158 E6CD251C 577C6047 EBFFB5FE


------------

  BlockEncrypt

  Key is
                    C4C14823 AE157968 6F2C4676 8030DE37


  X is
                    95EC1158 E6CD251C 577C6047 EBFFB5FE


  X = BlockEncrypt(Key, X) is
                    C2659E6A EFBB0DFB 2096A598 CC1C509F


  temp is
                    C2659E6A EFBB0DFB 2096A598 CC1C509F
```

```
    ------------

      BlockEncrypt

      Key is
                          C4C14823 AE157968 6F2C4676 8030DE37


      X is
                          C2659E6A EFBB0DFB 2096A598 CC1C509F


      X = BlockEncrypt(Key, X) is
                          D926A4C1 E62F8936 D419709D 6124946A


      temp is
                                               C2659E6A EFBB0DFB
        2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A


      requested_bits is
                                               C2659E6A EFBB0DFB
        2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A


    seed_material is
                                               C2659E6A EFBB0DFB
        2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A


---------------------------

  Update

    provided_data is
                                               C2659E6A EFBB0DFB
        2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A


    ------------

      While loop

      Key is
                          00000000 00000000 00000000 00000000
```

```
  V is
                      00000000 00000000 00000000 00000001

  output_block is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A

  temp is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A

------------

  While loop

  Key is
                      00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000002

  output_block is
                      0388DACE 60B6A392 F328C2B9 71B2FE78

  temp is
                                        58E2FCCE FA7E3061
    367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78

temp XOR provided_data is
                                        9A8762A4 15C53D9A
    16E9B8CF 68FB15C5 DAAE7E0F 86992AA4 2731B224 10966A12

Key is
                      9A8762A4 15C53D9A 16E9B8CF 68FB15C5

V is
                      DAAE7E0F 86992AA4 2731B224 10966A12
```

```
---------------------------------------------------------------

First call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                                60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


  additional_input <> NULL, process appropriately
---------------------------

  Block_Cipher_df

    input_str is
                                                60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    number_of_bits_to_return = 256

    S is
        00000020 00000020 60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000


    ------------

      BCC

      IV is
                          00000000 00000000 00000000 00000000


      IV || S is
                          00000000 00000000 00000000 00000000
        00000020 00000020 60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000
```

```
temp is
                    1E28FC96 A28B1550 8D8FC557 2B37CD4A


------------

  BCC

  IV is
                    00000001 00000000 00000000 00000000


  IV || S is
                    00000001 00000000 00000000 00000000
    00000020 00000020 60616263 64656667 68696A6B 6C6D6E6F
    70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000


temp is
                                        1E28FC96 A28B1550
    8D8FC557 2B37CD4A 857D7807 8DB171BF 8894073D E0C07B85


------------

Key is
                    1E28FC96 A28B1550 8D8FC557 2B37CD4A


X is
                    857D7807 8DB171BF 8894073D E0C07B85


------------

  BlockEncrypt

  Key is
                    1E28FC96 A28B1550 8D8FC557 2B37CD4A


  X is
                    857D7807 8DB171BF 8894073D E0C07B85
```

```
      X = BlockEncrypt(Key, X) is
                          C9172CDC 185A4A36 9E62578A F8F7C107


      temp is
                          C9172CDC 185A4A36 9E62578A F8F7C107


    ------------

      BlockEncrypt

      Key is
                          1E28FC96 A28B1550 8D8FC557 2B37CD4A


      X is
                          C9172CDC 185A4A36 9E62578A F8F7C107


      X = BlockEncrypt(Key, X) is
                          62DC9AD4 254F6BE9 0497C56E DE6C9AA5


      temp is
                                              C9172CDC 185A4A36
        9E62578A F8F7C107 62DC9AD4 254F6BE9 0497C56E DE6C9AA5


      requested_bits is
                                              C9172CDC 185A4A36
        9E62578A F8F7C107 62DC9AD4 254F6BE9 0497C56E DE6C9AA5


---------------------------

  Update

    provided_data is
                                              C9172CDC 185A4A36
        9E62578A F8F7C107 62DC9AD4 254F6BE9 0497C56E DE6C9AA5


    ------------
```

```
  While loop

  Key is
                      9A8762A4 15C53D9A 16E9B8CF 68FB15C5


  V is
                      DAAE7E0F 86992AA4 2731B224 10966A13


  output_block is
                      18FDEFBD C43D7A36 D5D6D862 205765D1


  temp is
                      18FDEFBD C43D7A36 D5D6D862 205765D1


------------

  While loop

  Key is
                      9A8762A4 15C53D9A 16E9B8CF 68FB15C5


  V is
                      DAAE7E0F 86992AA4 2731B224 10966A14


  output_block is
                      D701C9F2 37007030 DF1B8E70 EE4EEE29


  temp is
                                        18FDEFBD C43D7A36
    D5D6D862 205765D1 D701C9F2 37007030 DF1B8E70 EE4EEE29


temp XOR provided_data is
                                        D1EAC361 DC673000
    4BB48FE8 D8A0A4D6 B5DD5326 124F1BD9 DB8C4B1E 3022748C


Key is
                      D1EAC361 DC673000 4BB48FE8 D8A0A4D6
```

```
    V is
                          B5DD5326 124F1BD9 DB8C4B1E 3022748C

---------------------------

  Update

    provided_data is
                                                C9172CDC 185A4A36
        9E62578A F8F7C107 62DC9AD4 254F6BE9 0497C56E DE6C9AA5


    ------------

      While loop

      Key is
                          D1EAC361 DC673000 4BB48FE8 D8A0A4D6


      V is
                          B5DD5326 124F1BD9 DB8C4B1E 3022748F


      output_block is
                          298D1882 F782A51E 7EBE2F26 C13E7517


      temp is
                          298D1882 F782A51E 7EBE2F26 C13E7517


    ------------

      While loop

      Key is
                          D1EAC361 DC673000 4BB48FE8 D8A0A4D6


      V is
                          B5DD5326 124F1BD9 DB8C4B1E 30227490
```

```
      output_block is
                          0CAEDD35 C87769FE D159CE86 E15868C2


      temp is
                                                 298D1882 F782A51E
        7EBE2F26 C13E7517 0CAEDD35 C87769FE D159CE86 E15868C2


    temp XOR provided_data is
                                                 E09A345E EFD8EF28
        E0DC78AC 39C9B410 6E7247E1 ED380217 D5CE0BE8 3F34F267


    Key is
                          E09A345E EFD8EF28 E0DC78AC 39C9B410


    V is
                          6E7247E1 ED380217 D5CE0BE8 3F34F267


rnd_val is
                                                 526CFB7F F19B8485
        D6283F06 7A4CB832 77A736E8 45E423AE 0A363E91 A9D95F3B


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                                 A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


  additional_input <> NULL, process appropriately
---------------------------
```

```
Block_Cipher_df

  input_str is
                                              A0A1A2A3 A4A5A6A7
      A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


  number_of_bits_to_return = 256

  S is
      00000020 00000020 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
      B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000


  ------------

    BCC

    IV is
                         00000000 00000000 00000000 00000000


    IV || S is
                         00000000 00000000 00000000 00000000
      00000020 00000020 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
      B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000


  temp is
                         2A2E34C4 CF921C78 51C82FB6 11B3AD80


  ------------

    BCC

    IV is
                         00000001 00000000 00000000 00000000


    IV || S is
                         00000001 00000000 00000000 00000000
      00000020 00000020 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
      B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000
```

```
temp is
                                          2A2E34C4 CF921C78
    51C82FB6 11B3AD80 AF942BCE FE572E5A 0ABD1E75 F20EC649


------------

Key is
                     2A2E34C4 CF921C78 51C82FB6 11B3AD80


X is
                     AF942BCE FE572E5A 0ABD1E75 F20EC649


------------

  BlockEncrypt

  Key is
                     2A2E34C4 CF921C78 51C82FB6 11B3AD80


  X is
                     AF942BCE FE572E5A 0ABD1E75 F20EC649


  X = BlockEncrypt(Key, X) is
                     83D41C94 8108B4D5 1B5D2980 046BD7F4


  temp is
                     83D41C94 8108B4D5 1B5D2980 046BD7F4


------------

  BlockEncrypt

  Key is
                     2A2E34C4 CF921C78 51C82FB6 11B3AD80


  X is
                     83D41C94 8108B4D5 1B5D2980 046BD7F4
```

```
      X = BlockEncrypt(Key, X) is
                          A6A7B2A0 DD3DD0C6 123C4186 842C1270


      temp is
                                               83D41C94 8108B4D5
        1B5D2980 046BD7F4 A6A7B2A0 DD3DD0C6 123C4186 842C1270


      requested_bits is
                                               83D41C94 8108B4D5
        1B5D2980 046BD7F4 A6A7B2A0 DD3DD0C6 123C4186 842C1270


---------------------------

  Update

    provided_data is
                                               83D41C94 8108B4D5
        1B5D2980 046BD7F4 A6A7B2A0 DD3DD0C6 123C4186 842C1270


    ------------

      While loop

      Key is
                          E09A345E EFD8EF28 E0DC78AC 39C9B410


      V is
                          6E7247E1 ED380217 D5CE0BE8 3F34F268


      output_block is
                          83C9B360 C168810E 431507FE 9793CADF


      temp is
                          83C9B360 C168810E 431507FE 9793CADF


    ------------
```

```
      While loop

      Key is
                           E09A345E EFD8EF28 E0DC78AC 39C9B410


      V is
                           6E7247E1 ED380217 D5CE0BE8 3F34F269


      output_block is
                           D3CEB5C1 7CF87AE1 69B8CB71 8E05FBB5


      temp is
                                                 83C9B360 C168810E
        431507FE 9793CADF D3CEB5C1 7CF87AE1 69B8CB71 8E05FBB5


    temp XOR provided_data is
                                                 001DAFF4 406035DB
       58482E7E 93F81D2B 75690761 A1C5AA27 7B848AF7 0A29E9C5


    Key is
                           001DAFF4 406035DB 58482E7E 93F81D2B


    V is
                           75690761 A1C5AA27 7B848AF7 0A29E9C5


---------------------------

  Update

    provided_data is
                                                 83D41C94 8108B4D5
       1B5D2980 046BD7F4 A6A7B2A0 DD3DD0C6 123C4186 842C1270


    ------------

      While loop

      Key is
```

```
                    001DAFF4 406035DB 58482E7E 93F81D2B

  V is
                    75690761 A1C5AA27 7B848AF7 0A29E9C8

  output_block is
                    2FD18B98 5F49C724 52E634A3 D7CE864C

  temp is
                    2FD18B98 5F49C724 52E634A3 D7CE864C

------------

  While loop

  Key is
                    001DAFF4 406035DB 58482E7E 93F81D2B

  V is
                    75690761 A1C5AA27 7B848AF7 0A29E9C9

  output_block is
                    9F216599 6645B418 D44FA297 E6A01492

  temp is
                                      2FD18B98 5F49C724
    52E634A3 D7CE864C 9F216599 6645B418 D44FA297 E6A01492

temp XOR provided_data is
                                      AC05970C DE4173F1
    49BB1D23 D3A551B8 3986D739 BB7864DE C673E311 628C06E2

Key is
                    AC05970C DE4173F1 49BB1D23 D3A551B8

V is
```

```
                          3986D739 BB7864DE C673E311 628C06E2


rnd_val is
                                                 FDDF99A0 8490FF79
        55D79C2F 8C372418 38813579 4C18B3D6 31E37B85 0FF5EB0F


################################################################

CTR_DRBG

    Requested Security Strength = 128

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                                 80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                                 C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    Nonce =
                                                 20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                                                 00010203 04050607
```

```
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    nonce is
                                            20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    number_of_bits_to_return = 256

    S is
                          00000028 00000020 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 80000000 00000000 00000000 00000000


    ------------

      BCC

      IV is
                          00000000 00000000 00000000 00000000


      IV || S is
                                            00000000 00000000
        00000000 00000000 00000028 00000020 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 80000000 00000000 00000000 00000000


    temp is
                          834EBAD8 5C601126 1D1D9DF4 C42A1544
```

```
------------

  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
                                              00000001 00000000
    00000000 00000000 00000028 00000020 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 80000000 00000000 00000000 00000000


temp is
                                              834EBAD8 5C601126
    1D1D9DF4 C42A1544 8EA249C1 226F0474 F3C55519 CB3677D2


------------

Key is
                      834EBAD8 5C601126 1D1D9DF4 C42A1544


X is
                      8EA249C1 226F0474 F3C55519 CB3677D2


------------

  BlockEncrypt

  Key is
                      834EBAD8 5C601126 1D1D9DF4 C42A1544


  X is
                      8EA249C1 226F0474 F3C55519 CB3677D2


  X = BlockEncrypt(Key, X) is
                      B8823BC4 F3AFBB6B A0373C69 BC49E2F6
```

```
      temp is
                          B8823BC4 F3AFBB6B A0373C69 BC49E2F6


    ------------

      BlockEncrypt

      Key is
                          834EBAD8 5C601126 1D1D9DF4 C42A1544


      X is
                          B8823BC4 F3AFBB6B A0373C69 BC49E2F6


      X = BlockEncrypt(Key, X) is
                          560EDE12 D8335B64 F5647FA0 A644162B


      temp is
                                            B8823BC4 F3AFBB6B
        A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B


      requested_bits is
                                            B8823BC4 F3AFBB6B
        A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B


    seed_material is
                                            B8823BC4 F3AFBB6B
        A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B


---------------------------

  Update

    provided_data is
                                            B8823BC4 F3AFBB6B
        A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B


    ------------
```

```
  While loop

  Key is
                      00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000001

  output_block is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A

  temp is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A

------------

  While loop

  Key is
                      00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000002

  output_block is
                      0388DACE 60B6A392 F328C2B9 71B2FE78

  temp is
                                        58E2FCCE FA7E3061
    367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78

temp XOR provided_data is
                                        E060C70A 09D18B0A
    9648213E 18AEA7AC 558604DC B885F8F6 064CBD19 D7F6E853

Key is
```

```
                          E060C70A 09D18B0A 9648213E 18AEA7AC

    V is
                          558604DC B885F8F6 064CBD19 D7F6E853

-----------------------------------------------------------

First call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                              80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    additional_input is  <empty>

---------------------------

  Block_Cipher_df

    input_str is
                                              80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    number_of_bits_to_return = 256

    S is
        00000020 00000020 80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F 80000000 00000000
```

```
------------

  BCC

  IV is
                      00000000 00000000 00000000 00000000


  IV || S is
                      00000000 00000000 00000000 00000000
    00000020 00000020 80818283 84858687 88898A8B 8C8D8E8F
    90919293 94959697 98999A9B 9C9D9E9F 80000000 00000000


temp is
                      6689B2EA B8B5547F E46D8E0B 6AD94B8C


------------

  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
                      00000001 00000000 00000000 00000000
    00000020 00000020 80818283 84858687 88898A8B 8C8D8E8F
    90919293 94959697 98999A9B 9C9D9E9F 80000000 00000000


temp is
                                         6689B2EA B8B5547F
    E46D8E0B 6AD94B8C 4578F39E C865C2E4 EADB493B A265794F


------------

Key is
                      6689B2EA B8B5547F E46D8E0B 6AD94B8C


X is
                      4578F39E C865C2E4 EADB493B A265794F
```

```
------------

  BlockEncrypt

  Key is
                      6689B2EA B8B5547F E46D8E0B 6AD94B8C


  X is
                      4578F39E C865C2E4 EADB493B A265794F


  X = BlockEncrypt(Key, X) is
                      E8B2120B 0673C751 090997D6 BEAC637D


  temp is
                      E8B2120B 0673C751 090997D6 BEAC637D


------------

  BlockEncrypt

  Key is
                      6689B2EA B8B5547F E46D8E0B 6AD94B8C


  X is
                      E8B2120B 0673C751 090997D6 BEAC637D


  X = BlockEncrypt(Key, X) is
                      79D7CA26 C10FEE1F EAC1E952 46CC5005


  temp is
                                        E8B2120B 0673C751
    090997D6 BEAC637D 79D7CA26 C10FEE1F EAC1E952 46CC5005


  requested_bits is
                                        E8B2120B 0673C751
    090997D6 BEAC637D 79D7CA26 C10FEE1F EAC1E952 46CC5005
```

```
---------------------------

  Update

    provided_data is
                                                E8B2120B 0673C751
        090997D6 BEAC637D 79D7CA26 C10FEE1F EAC1E952 46CC5005


    ------------

      While loop

      Key is
                           E060C70A 09D18B0A 9648213E 18AEA7AC


      V is
                           558604DC B885F8F6 064CBD19 D7F6E854


      output_block is
                           8CF59C8C F6888B96 EB1C1E3E 79D82387


      temp is
                           8CF59C8C F6888B96 EB1C1E3E 79D82387


    ------------

      While loop

      Key is
                           E060C70A 09D18B0A 9648213E 18AEA7AC


      V is
                           558604DC B885F8F6 064CBD19 D7F6E855


      output_block is
                           AF08A9E5 FF75E23F 1FBCD455 9B6B997E
```

```
      temp is
                                                8CF59C8C F6888B96
        EB1C1E3E 79D82387 AF08A9E5 FF75E23F 1FBCD455 9B6B997E


    temp XOR provided_data is
                                                64478E87 F0FB4CC7
        E21589E8 C77440FA D6DF63C3 3E7A0C20 F57D3D07 DDA7C97B


    Key is
                           64478E87 F0FB4CC7 E21589E8 C77440FA


    V is
                           D6DF63C3 3E7A0C20 F57D3D07 DDA7C97B


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                           64478E87 F0FB4CC7 E21589E8 C77440FA


      V is
                           D6DF63C3 3E7A0C20 F57D3D07 DDA7C97E
```

```
      output_block is
                          77FA8FD1 623711DB C4F78811 94359692

      temp is
                          77FA8FD1 623711DB C4F78811 94359692

    ------------

      While loop

      Key is
                          64478E87 F0FB4CC7 E21589E8 C77440FA

      V is
                          D6DF63C3 3E7A0C20 F57D3D07 DDA7C97F

      output_block is
                          3ED2ABE4 23A82FB0 DDD70D6D 2DB30EB3

      temp is
                                            77FA8FD1 623711DB
        C4F78811 94359692 3ED2ABE4 23A82FB0 DDD70D6D 2DB30EB3

    temp XOR provided_data is
                                            77FA8FD1 623711DB
        C4F78811 94359692 3ED2ABE4 23A82FB0 DDD70D6D 2DB30EB3

    Key is
                          77FA8FD1 623711DB C4F78811 94359692

    V is
                          3ED2ABE4 23A82FB0 DDD70D6D 2DB30EB3

rnd_val is
                                            BFF4B85D 68C84529
```

```
        F24F69F9 ACF1756E 29BA648D DEB825C2 25FA32BA 490EF4A9


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                            C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    additional_input is  <empty>

---------------------------

  Block_Cipher_df

    input_str is
                                            C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    number_of_bits_to_return = 256

    S is
        00000020 00000020 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF 80000000 00000000


    ------------

      BCC
```

```
  IV is
                    00000000 00000000 00000000 00000000


  IV || S is
                    00000000 00000000 00000000 00000000
    00000020 00000020 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
    D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF 80000000 00000000


temp is
                    72571427 A62CFFB3 105AA38D 4C701D8A


------------

  BCC

  IV is
                    00000001 00000000 00000000 00000000


  IV || S is
                    00000001 00000000 00000000 00000000
    00000020 00000020 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
    D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF 80000000 00000000


temp is
                                        72571427 A62CFFB3
    105AA38D 4C701D8A E90056D7 6C2480EE 096C3B48 059FD3F7


------------

Key is
                    72571427 A62CFFB3 105AA38D 4C701D8A


X is
                    E90056D7 6C2480EE 096C3B48 059FD3F7


------------
```

```
      BlockEncrypt

      Key is
                           72571427 A62CFFB3 105AA38D 4C701D8A


      X is
                           E90056D7 6C2480EE 096C3B48 059FD3F7


      X = BlockEncrypt(Key, X) is
                           ACEF0D4B 113B12C1 4E45C0A0 A9574DE6


      temp is
                           ACEF0D4B 113B12C1 4E45C0A0 A9574DE6


    ------------

      BlockEncrypt

      Key is
                           72571427 A62CFFB3 105AA38D 4C701D8A


      X is
                           ACEF0D4B 113B12C1 4E45C0A0 A9574DE6


      X = BlockEncrypt(Key, X) is
                           F20CF416 9FEF3831 76A7C304 F0066E66


      temp is
                                             ACEF0D4B 113B12C1
        4E45C0A0 A9574DE6 F20CF416 9FEF3831 76A7C304 F0066E66


      requested_bits is
                                             ACEF0D4B 113B12C1
        4E45C0A0 A9574DE6 F20CF416 9FEF3831 76A7C304 F0066E66


---------------------------
```

```
Update

  provided_data is
                                                ACEF0D4B 113B12C1
      4E45C0A0 A9574DE6 F20CF416 9FEF3831 76A7C304 F0066E66


  ------------

    While loop

    Key is
                         77FA8FD1 623711DB C4F78811 94359692


    V is
                         3ED2ABE4 23A82FB0 DDD70D6D 2DB30EB4


    output_block is
                         77B20847 D584D9C7 BF91AAAB 087F4615


    temp is
                         77B20847 D584D9C7 BF91AAAB 087F4615


  ------------

    While loop

    Key is
                         77FA8FD1 623711DB C4F78811 94359692


    V is
                         3ED2ABE4 23A82FB0 DDD70D6D 2DB30EB5


    output_block is
                         F31E70A8 B9ADF9A6 95229D64 BA9848AD


    temp is
                                                77B20847 D584D9C7
      BF91AAAB 087F4615 F31E70A8 B9ADF9A6 95229D64 BA9848AD
```

```
    temp XOR provided_data is
                                                DB5D050C C4BFCB06
        F1D46A0B A1280BF3 011284BE 2642C197 E3855E60 4A9E26CB


    Key is
                          DB5D050C C4BFCB06 F1D46A0B A1280BF3


    V is
                          011284BE 2642C197 E3855E60 4A9E26CB


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                          DB5D050C C4BFCB06 F1D46A0B A1280BF3


      V is
                          011284BE 2642C197 E3855E60 4A9E26CE


      output_block is
                          10A46DA7 3E72179C 696C3AFA A43474EC
```

```
      temp is
                          10A46DA7 3E72179C 696C3AFA A43474EC


    ------------

      While loop

      Key is
                          DB5D050C C4BFCB06 F1D46A0B A1280BF3


      V is
                          011284BE 2642C197 E3855E60 4A9E26CF


      output_block is
                          1CC0B5E0 56F167A8 8939447B 19C054F5


      temp is
                                            10A46DA7 3E72179C
        696C3AFA A43474EC 1CC0B5E0 56F167A8 8939447B 19C054F5


    temp XOR provided_data is
                                            10A46DA7 3E72179C
        696C3AFA A43474EC 1CC0B5E0 56F167A8 8939447B 19C054F5


    Key is
                          10A46DA7 3E72179C 696C3AFA A43474EC


    V is
                          1CC0B5E0 56F167A8 8939447B 19C054F5


rnd_val is
                                            9BD26351 37A52AF7
        D0FCBEFE FB97EA93 A0F4C438 BD98956C 0DACB04F 15EE25B3


################################################################
```

```
CTR_DRBG

    Requested Security Strength = 128

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    Nonce =
                                                20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    AdditionalInput2 =
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
```

```
    nonce is
                                                20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                           00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    number_of_bits_to_return = 256

    S is
                           00000028 00000020 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 80000000 00000000 00000000 00000000


    ------------

      BCC

      IV is
                           00000000 00000000 00000000 00000000


      IV || S is
                                                00000000 00000000
        00000000 00000000 00000028 00000020 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 80000000 00000000 00000000 00000000


    temp is
                           834EBAD8 5C601126 1D1D9DF4 C42A1544
```

```
------------

  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
                                           00000001 00000000
    00000000 00000000 00000028 00000020 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 80000000 00000000 00000000 00000000


temp is
                                           834EBAD8 5C601126
    1D1D9DF4 C42A1544 8EA249C1 226F0474 F3C55519 CB3677D2


------------

Key is
                      834EBAD8 5C601126 1D1D9DF4 C42A1544


X is
                      8EA249C1 226F0474 F3C55519 CB3677D2


------------

  BlockEncrypt

  Key is
                      834EBAD8 5C601126 1D1D9DF4 C42A1544


  X is
                      8EA249C1 226F0474 F3C55519 CB3677D2


  X = BlockEncrypt(Key, X) is
                      B8823BC4 F3AFBB6B A0373C69 BC49E2F6
```

```
      temp is
                          B8823BC4 F3AFBB6B A0373C69 BC49E2F6


    ------------

      BlockEncrypt

      Key is
                          834EBAD8 5C601126 1D1D9DF4 C42A1544


      X is
                          B8823BC4 F3AFBB6B A0373C69 BC49E2F6


      X = BlockEncrypt(Key, X) is
                          560EDE12 D8335B64 F5647FA0 A644162B


      temp is
                                            B8823BC4 F3AFBB6B
        A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B


      requested_bits is
                                            B8823BC4 F3AFBB6B
        A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B


    seed_material is
                                            B8823BC4 F3AFBB6B
        A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B


---------------------------

  Update

    provided_data is
                                            B8823BC4 F3AFBB6B
        A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B


    ------------
```

```
  While loop

  Key is
                      00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000001

  output_block is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A

  temp is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A

------------

  While loop

  Key is
                      00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000002

  output_block is
                      0388DACE 60B6A392 F328C2B9 71B2FE78

  temp is
                                        58E2FCCE FA7E3061
    367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78

temp XOR provided_data is
                                        E060C70A 09D18B0A
    9648213E 18AEA7AC 558604DC B885F8F6 064CBD19 D7F6E853

Key is
                      E060C70A 09D18B0A 9648213E 18AEA7AC
```

```
    V is
                          558604DC B885F8F6 064CBD19 D7F6E853


------------------------------------------------------------

First call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                            60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                            80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    additional_input is
                                            60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


--------------------------

  Block_Cipher_df

    input_str is
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F 60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
```

```
number_of_bits_to_return = 256

S is
                                          00000040 00000020
    80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
    98999A9B 9C9D9E9F 60616263 64656667 68696A6B 6C6D6E6F
    70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000


------------

  BCC

  IV is
                      00000000 00000000 00000000 00000000


  IV || S is
    00000000 00000000 00000000 00000000 00000040 00000020
    80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
    98999A9B 9C9D9E9F 60616263 64656667 68696A6B 6C6D6E6F
    70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000


temp is
                      EBE472ED 18D7D72C A576D5D0 4F951FF2


------------

  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
    00000001 00000000 00000000 00000000 00000040 00000020
    80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
    98999A9B 9C9D9E9F 60616263 64656667 68696A6B 6C6D6E6F
    70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000


temp is
                                          EBE472ED 18D7D72C
    A576D5D0 4F951FF2 E1753FDA 28CA0A50 0C8D0BE0 F45D9C20
```

```
------------

Key is
                     EBE472ED 18D7D72C A576D5D0 4F951FF2


X is
                     E1753FDA 28CA0A50 0C8D0BE0 F45D9C20


------------

  BlockEncrypt

  Key is
                     EBE472ED 18D7D72C A576D5D0 4F951FF2


  X is
                     E1753FDA 28CA0A50 0C8D0BE0 F45D9C20


  X = BlockEncrypt(Key, X) is
                     C1F7BD08 F11F831D FFE48696 8B706115


  temp is
                     C1F7BD08 F11F831D FFE48696 8B706115


------------

  BlockEncrypt

  Key is
                     EBE472ED 18D7D72C A576D5D0 4F951FF2


  X is
                     C1F7BD08 F11F831D FFE48696 8B706115


  X = BlockEncrypt(Key, X) is
                     7D71F428 FC13B31C 0AB3A4BB 7FA41524
```

```
      temp is
                                              C1F7BD08 F11F831D
        FFE48696 8B706115 7D71F428 FC13B31C 0AB3A4BB 7FA41524


      requested_bits is
                                              C1F7BD08 F11F831D
        FFE48696 8B706115 7D71F428 FC13B31C 0AB3A4BB 7FA41524


---------------------------

  Update

    provided_data is
                                              C1F7BD08 F11F831D
        FFE48696 8B706115 7D71F428 FC13B31C 0AB3A4BB 7FA41524


    ------------

      While loop

      Key is
                           E060C70A 09D18B0A 9648213E 18AEA7AC


      V is
                           558604DC B885F8F6 064CBD19 D7F6E854


      output_block is
                           8CF59C8C F6888B96 EB1C1E3E 79D82387


      temp is
                           8CF59C8C F6888B96 EB1C1E3E 79D82387


    ------------

      While loop

      Key is
```

```
                          E060C70A 09D18B0A 9648213E 18AEA7AC

      V is
                          558604DC B885F8F6 064CBD19 D7F6E855

      output_block is
                          AF08A9E5 FF75E23F 1FBCD455 9B6B997E

      temp is
                                                   8CF59C8C F6888B96
        EB1C1E3E 79D82387 AF08A9E5 FF75E23F 1FBCD455 9B6B997E

    temp XOR provided_data is
                                                   4D022184 0797088B
       14F898A8 F2A84292 D2795DCD 03665123 150F70EE E4CF8C5A

    Key is
                          4D022184 0797088B 14F898A8 F2A84292

    V is
                          D2795DCD 03665123 150F70EE E4CF8C5A

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                                                   00000000 00000000
       00000000 00000000 00000000 00000000 00000000 00000000
```

```
------------

  While loop

  Key is
                      4D022184 0797088B 14F898A8 F2A84292


  V is
                      D2795DCD 03665123 150F70EE E4CF8C5D


  output_block is
                      B3AAF086 5F3A5014 E5D54C6A 47184F14


  temp is
                      B3AAF086 5F3A5014 E5D54C6A 47184F14


------------

  While loop

  Key is
                      4D022184 0797088B 14F898A8 F2A84292


  V is
                      D2795DCD 03665123 150F70EE E4CF8C5E


  output_block is
                      213CABA6 26EB614F 28A2E5AD 17BAFE2B


  temp is
                                        B3AAF086 5F3A5014
    E5D54C6A 47184F14 213CABA6 26EB614F 28A2E5AD 17BAFE2B


temp XOR provided_data is
                                        B3AAF086 5F3A5014
    E5D54C6A 47184F14 213CABA6 26EB614F 28A2E5AD 17BAFE2B
```

```
    Key is
                          B3AAF086 5F3A5014 E5D54C6A 47184F14

    V is
                          213CABA6 26EB614F 28A2E5AD 17BAFE2B

rnd_val is
                                            4573AC8B BB33D7CC
        4DBEF3EE DF6EAE74 8B536C3A 1082CEE4 948CDB51 C83A7F9C

---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF

Generate FAILED: Reseed is required
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                            C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF

    additional_input is
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF

---------------------------

  Block_Cipher_df
```

```
input_str is
                     C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
    D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


number_of_bits_to_return = 256

S is
                                         00000040 00000020
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
    D8D9DADB DCDDDEDF A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
    B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000


------------

  BCC

  IV is
                     00000000 00000000 00000000 00000000


  IV || S is
    00000000 00000000 00000000 00000000 00000040 00000020
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
    D8D9DADB DCDDDEDF A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
    B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000


temp is
                     F57B5902 0636E7E2 20EDB29F 6EBCC72D


------------

  BCC

  IV is
                     00000001 00000000 00000000 00000000


  IV || S is
    00000001 00000000 00000000 00000000 00000040 00000020
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
```

```
    D8D9DADB DCDDDEDF A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
    B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000


temp is
                                        F57B5902 0636E7E2
    20EDB29F 6EBCC72D DFA80B3D A0FFF2E7 E81EE4ED 18CDECA6


------------

Key is
                     F57B5902 0636E7E2 20EDB29F 6EBCC72D


X is
                     DFA80B3D A0FFF2E7 E81EE4ED 18CDECA6


------------

  BlockEncrypt

  Key is
                     F57B5902 0636E7E2 20EDB29F 6EBCC72D


  X is
                     DFA80B3D A0FFF2E7 E81EE4ED 18CDECA6


  X = BlockEncrypt(Key, X) is
                     DC4290C1 50AD02F0 B68092DA E2472F86


  temp is
                     DC4290C1 50AD02F0 B68092DA E2472F86


------------

  BlockEncrypt

  Key is
                     F57B5902 0636E7E2 20EDB29F 6EBCC72D
```

```
      X is
                          DC4290C1 50AD02F0 B68092DA E2472F86

      X = BlockEncrypt(Key, X) is
                          AF2B9220 9762D534 4076FF12 D162E485

      temp is
                                            DC4290C1 50AD02F0
        B68092DA E2472F86 AF2B9220 9762D534 4076FF12 D162E485

      requested_bits is
                                            DC4290C1 50AD02F0
        B68092DA E2472F86 AF2B9220 9762D534 4076FF12 D162E485

----------------------------

  Update

    provided_data is
                                            DC4290C1 50AD02F0
        B68092DA E2472F86 AF2B9220 9762D534 4076FF12 D162E485

    ------------

      While loop

      Key is
                          B3AAF086 5F3A5014 E5D54C6A 47184F14

      V is
                          213CABA6 26EB614F 28A2E5AD 17BAFE2C

      output_block is
                          0A8E9ACF 2A4D283A 1BD44054 BBD51AC4

      temp is
                          0A8E9ACF 2A4D283A 1BD44054 BBD51AC4
```

```
    ------------

      While loop

      Key is
                           B3AAF086 5F3A5014 E5D54C6A 47184F14


      V is
                           213CABA6 26EB614F 28A2E5AD 17BAFE2D


      output_block is
                           D01DDA32 A4A752B2 AA21023F F30180D0


      temp is
                                                 0A8E9ACF 2A4D283A
        1BD44054 BBD51AC4 D01DDA32 A4A752B2 AA21023F F30180D0


    temp XOR provided_data is
                                                 D6CC0A0E 7AE02ACA
        AD54D28E 59923542 7F364812 33C58786 EA57FD2D 22636455


    Key is
                           D6CC0A0E 7AE02ACA AD54D28E 59923542


    V is
                           7F364812 33C58786 EA57FD2D 22636455


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------
```

```
Update

  provided_data is
                                                00000000 00000000
      00000000 00000000 00000000 00000000 00000000 00000000


  ------------

    While loop

    Key is
                         D6CC0A0E 7AE02ACA AD54D28E 59923542


    V is
                         7F364812 33C58786 EA57FD2D 22636458


    output_block is
                         89DE75C8 E0A4BCBA 0DD270E1 87E93EC7


    temp is
                         89DE75C8 E0A4BCBA 0DD270E1 87E93EC7


  ------------

    While loop

    Key is
                         D6CC0A0E 7AE02ACA AD54D28E 59923542


    V is
                         7F364812 33C58786 EA57FD2D 22636459


    output_block is
                         60B0D047 81606A14 BE1FE576 8405D9D1


    temp is
                                                89DE75C8 E0A4BCBA
      0DD270E1 87E93EC7 60B0D047 81606A14 BE1FE576 8405D9D1
```

```
    temp XOR provided_data is
                                            89DE75C8 E0A4BCBA
        0DD270E1 87E93EC7 60B0D047 81606A14 BE1FE576 8405D9D1


    Key is
                          89DE75C8 E0A4BCBA 0DD270E1 87E93EC7


    V is
                          60B0D047 81606A14 BE1FE576 8405D9D1


rnd_val is
                                            99C628CD D87BD8C2
        F1FE443A A7F761DA 16886436 32632335 4DA6311F FF5BC678


################################################################

CTR_DRBG

    Requested Security Strength = 128

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                            00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                            80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                            C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    Nonce =
                                            20212223 24252627
```

```
    PersonalizationString =
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    AdditionalInput = <empty>

################################################################

****************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    nonce is
                                                20212223 24252627


    personal_str is
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    number_of_bits_to_return = 256

    S is
        00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000
```

```
------------

  BCC

  IV is
                      00000000 00000000 00000000 00000000


  IV || S is
                      00000000 00000000 00000000 00000000
    00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
    40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
    58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000


temp is
                      C4C14823 AE157968 6F2C4676 8030DE37


------------

  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
                      00000001 00000000 00000000 00000000
    00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
    40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
    58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000


temp is
                                        C4C14823 AE157968
    6F2C4676 8030DE37 95EC1158 E6CD251C 577C6047 EBFFB5FE


------------

Key is
```

```
                    C4C14823 AE157968 6F2C4676 8030DE37

X is
                    95EC1158 E6CD251C 577C6047 EBFFB5FE

------------

  BlockEncrypt

  Key is
                    C4C14823 AE157968 6F2C4676 8030DE37

  X is
                    95EC1158 E6CD251C 577C6047 EBFFB5FE

  X = BlockEncrypt(Key, X) is
                    C2659E6A EFBB0DFB 2096A598 CC1C509F

  temp is
                    C2659E6A EFBB0DFB 2096A598 CC1C509F

------------

  BlockEncrypt

  Key is
                    C4C14823 AE157968 6F2C4676 8030DE37

  X is
                    C2659E6A EFBB0DFB 2096A598 CC1C509F

  X = BlockEncrypt(Key, X) is
                    D926A4C1 E62F8936 D419709D 6124946A

  temp is
                                      C2659E6A EFBB0DFB
    2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A
```

```
      requested_bits is
                                                C2659E6A EFBB0DFB
        2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A


    seed_material is
                                                C2659E6A EFBB0DFB
        2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A


---------------------------

  Update

    provided_data is
                                                C2659E6A EFBB0DFB
        2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A


    ------------

      While loop

      Key is
                           00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001


      output_block is
                           58E2FCCE FA7E3061 367F1D57 A4E7455A


      temp is
                           58E2FCCE FA7E3061 367F1D57 A4E7455A


    ------------

      While loop

      Key is
```

```
                        00000000 00000000 00000000 00000000

      V is
                        00000000 00000000 00000000 00000002

      output_block is
                        0388DACE 60B6A392 F328C2B9 71B2FE78

      temp is
                                                 58E2FCCE FA7E3061
        367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78

    temp XOR provided_data is
                                                 9A8762A4 15C53D9A
        16E9B8CF 68FB15C5 DAAE7E0F 86992AA4 2731B224 10966A12

    Key is
                        9A8762A4 15C53D9A 16E9B8CF 68FB15C5

    V is
                        DAAE7E0F 86992AA4 2731B224 10966A12

-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

CTR_DRBG_Reseed
```

```
    entropy_input is
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    additional_input is  <empty>

----------------------------

  Block_Cipher_df

    input_str is
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    number_of_bits_to_return = 256

    S is
        00000020 00000020 80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F 80000000 00000000


    ------------

      BCC

      IV is
                           00000000 00000000 00000000 00000000


      IV || S is
                           00000000 00000000 00000000 00000000
        00000020 00000020 80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F 80000000 00000000


    temp is
                           6689B2EA B8B5547F E46D8E0B 6AD94B8C


    ------------

      BCC

      IV is
```

```
                    00000001 00000000 00000000 00000000

  IV || S is
                    00000001 00000000 00000000 00000000
    00000020 00000020 80818283 84858687 88898A8B 8C8D8E8F
    90919293 94959697 98999A9B 9C9D9E9F 80000000 00000000

temp is
                                        6689B2EA B8B5547F
    E46D8E0B 6AD94B8C 4578F39E C865C2E4 EADB493B A265794F

------------

Key is
                    6689B2EA B8B5547F E46D8E0B 6AD94B8C

X is
                    4578F39E C865C2E4 EADB493B A265794F

------------

  BlockEncrypt

  Key is
                    6689B2EA B8B5547F E46D8E0B 6AD94B8C

  X is
                    4578F39E C865C2E4 EADB493B A265794F

  X = BlockEncrypt(Key, X) is
                    E8B2120B 0673C751 090997D6 BEAC637D

  temp is
                    E8B2120B 0673C751 090997D6 BEAC637D

------------
```

```
      BlockEncrypt

      Key is
                          6689B2EA B8B5547F E46D8E0B 6AD94B8C


      X is
                          E8B2120B 0673C751 090997D6 BEAC637D


      X = BlockEncrypt(Key, X) is
                          79D7CA26 C10FEE1F EAC1E952 46CC5005


      temp is
                                            E8B2120B 0673C751
        090997D6 BEAC637D 79D7CA26 C10FEE1F EAC1E952 46CC5005


      requested_bits is
                                            E8B2120B 0673C751
        090997D6 BEAC637D 79D7CA26 C10FEE1F EAC1E952 46CC5005


---------------------------

  Update

    provided_data is
                                            E8B2120B 0673C751
        090997D6 BEAC637D 79D7CA26 C10FEE1F EAC1E952 46CC5005


    ------------

      While loop

      Key is
                          9A8762A4 15C53D9A 16E9B8CF 68FB15C5


      V is
                          DAAE7E0F 86992AA4 2731B224 10966A13


      output_block is
```

```
                        18FDEFBD C43D7A36 D5D6D862 205765D1

      temp is
                        18FDEFBD C43D7A36 D5D6D862 205765D1

    ------------

      While loop

      Key is
                        9A8762A4 15C53D9A 16E9B8CF 68FB15C5

      V is
                        DAAE7E0F 86992AA4 2731B224 10966A14

      output_block is
                        D701C9F2 37007030 DF1B8E70 EE4EEE29

      temp is
                                          18FDEFBD C43D7A36
        D5D6D862 205765D1 D701C9F2 37007030 DF1B8E70 EE4EEE29

    temp XOR provided_data is
                                          F04FFDB6 C24EBD67
        DCDF4FB4 9EFB06AC AED603D4 F60F9E2F 35DA6722 A882BE2C

    Key is
                        F04FFDB6 C24EBD67 DCDF4FB4 9EFB06AC

    V is
                        AED603D4 F60F9E2F 35DA6722 A882BE2C

**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256
```

```
    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                                                  00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                          F04FFDB6 C24EBD67 DCDF4FB4 9EFB06AC


      V is
                          AED603D4 F60F9E2F 35DA6722 A882BE2F


      output_block is
                          30F4A36C EEC8FB06 461F757F 9FFF5865


      temp is
                          30F4A36C EEC8FB06 461F757F 9FFF5865


    ------------

      While loop

      Key is
                          F04FFDB6 C24EBD67 DCDF4FB4 9EFB06AC


      V is
                          AED603D4 F60F9E2F 35DA6722 A882BE30


      output_block is
                          7E1FC53A 8D9322D2 6F1A255B 2A19CEEB
```

```
      temp is
                                                30F4A36C EEC8FB06
        461F757F 9FFF5865 7E1FC53A 8D9322D2 6F1A255B 2A19CEEB


    temp XOR provided_data is
                                                30F4A36C EEC8FB06
        461F757F 9FFF5865 7E1FC53A 8D9322D2 6F1A255B 2A19CEEB


    Key is
                          30F4A36C EEC8FB06 461F757F 9FFF5865


    V is
                          7E1FC53A 8D9322D2 6F1A255B 2A19CEEB


rnd_val is
                                                F324104E 2FA14F79
        D8AA60DF 06B93B3B C1573249 58F0A7EE 1E193677 A70E0250


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
```

```
    additional_input is  <empty>

---------------------------

  Block_Cipher_df

    input_str is
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    number_of_bits_to_return = 256

    S is
        00000020 00000020 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF 80000000 00000000


    ------------

      BCC

      IV is
                          00000000 00000000 00000000 00000000


      IV || S is
                          00000000 00000000 00000000 00000000
        00000020 00000020 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF 80000000 00000000


    temp is
                          72571427 A62CFFB3 105AA38D 4C701D8A


    ------------

      BCC

      IV is
                          00000001 00000000 00000000 00000000


      IV || S is
```

```
                    00000001 00000000 00000000 00000000
    00000020 00000020 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
    D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF 80000000 00000000


temp is
                                        72571427 A62CFFB3
    105AA38D 4C701D8A E90056D7 6C2480EE 096C3B48 059FD3F7


------------

Key is
                    72571427 A62CFFB3 105AA38D 4C701D8A


X is
                    E90056D7 6C2480EE 096C3B48 059FD3F7


------------

  BlockEncrypt

  Key is
                    72571427 A62CFFB3 105AA38D 4C701D8A


  X is
                    E90056D7 6C2480EE 096C3B48 059FD3F7


  X = BlockEncrypt(Key, X) is
                    ACEF0D4B 113B12C1 4E45C0A0 A9574DE6


  temp is
                    ACEF0D4B 113B12C1 4E45C0A0 A9574DE6


------------

  BlockEncrypt

  Key is
                    72571427 A62CFFB3 105AA38D 4C701D8A
```

```
      X is
                          ACEF0D4B 113B12C1 4E45C0A0 A9574DE6


      X = BlockEncrypt(Key, X) is
                          F20CF416 9FEF3831 76A7C304 F0066E66


      temp is
                                            ACEF0D4B 113B12C1
        4E45C0A0 A9574DE6 F20CF416 9FEF3831 76A7C304 F0066E66


      requested_bits is
                                            ACEF0D4B 113B12C1
        4E45C0A0 A9574DE6 F20CF416 9FEF3831 76A7C304 F0066E66


----------------------------

  Update

    provided_data is
                                            ACEF0D4B 113B12C1
        4E45C0A0 A9574DE6 F20CF416 9FEF3831 76A7C304 F0066E66


    ------------

      While loop

      Key is
                          30F4A36C EEC8FB06 461F757F 9FFF5865


      V is
                          7E1FC53A 8D9322D2 6F1A255B 2A19CEEC


      output_block is
                          0083F230 2AA6069D 85CA5D62 7B134697


      temp is
```

```
                        0083F230 2AA6069D 85CA5D62 7B134697

    ------------

      While loop

      Key is
                        30F4A36C EEC8FB06 461F757F 9FFF5865

      V is
                        7E1FC53A 8D9322D2 6F1A255B 2A19CEED

      output_block is
                        900DBA47 8EB2A67A 54CC49AD FACCE41F

      temp is
                                          0083F230 2AA6069D
        85CA5D62 7B134697 900DBA47 8EB2A67A 54CC49AD FACCE41F

    temp XOR provided_data is
                                          AC6CFF7B 3B9D145C
        CB8F9DC2 D2440B71 62014E51 115D9E4B 226B8AA9 0ACA8A79

    Key is
                        AC6CFF7B 3B9D145C CB8F9DC2 D2440B71

    V is
                        62014E51 115D9E4B 226B8AA9 0ACA8A79

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------
```

```
Update

  provided_data is
                                                00000000 00000000
      00000000 00000000 00000000 00000000 00000000 00000000


  ------------

    While loop

    Key is
                         AC6CFF7B 3B9D145C CB8F9DC2 D2440B71


    V is
                         62014E51 115D9E4B 226B8AA9 0ACA8A7C


    output_block is
                         561A1088 01412E20 882B0B5A 682EC41D


    temp is
                         561A1088 01412E20 882B0B5A 682EC41D


  ------------

    While loop

    Key is
                         AC6CFF7B 3B9D145C CB8F9DC2 D2440B71


    V is
                         62014E51 115D9E4B 226B8AA9 0ACA8A7D


    output_block is
                         C972133D 67C2B62C 74196869 30001E57


    temp is
                                                561A1088 01412E20
```

```
        882B0B5A 682EC41D C972133D 67C2B62C 74196869 30001E57


    temp XOR provided_data is
                                            561A1088 01412E20
        882B0B5A 682EC41D C972133D 67C2B62C 74196869 30001E57


    Key is
                          561A1088 01412E20 882B0B5A 682EC41D


    V is
                          C972133D 67C2B62C 74196869 30001E57


rnd_val is
                                            78F4C840 134F40DC
        001BFAD3 A90B5EF4 DEBDBFAC 3CFDF0CD 69A89DC4 FD34713F


################################################################

CTR_DRBG

    Requested Security Strength = 128

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                            00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                            80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                            C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    Nonce =
                                            20212223 24252627
```

```
    PersonalizationString =
                                            40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    AdditionalInput1 =
                                            60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    AdditionalInput2 =
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


################################################################

****************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                                            00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    nonce is
                                            20212223 24252627


    personal_str is
                                            40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
```

```
number_of_bits_to_return = 256

S is
    00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
    40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
    58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000


------------

  BCC

  IV is
                      00000000 00000000 00000000 00000000


  IV || S is
                      00000000 00000000 00000000 00000000
    00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
    40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
    58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000


temp is
                      C4C14823 AE157968 6F2C4676 8030DE37


------------

  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
                      00000001 00000000 00000000 00000000
    00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
    40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
    58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000
```

```
temp is
                                        C4C14823 AE157968
    6F2C4676 8030DE37 95EC1158 E6CD251C 577C6047 EBFFB5FE


------------

Key is
                     C4C14823 AE157968 6F2C4676 8030DE37


X is
                     95EC1158 E6CD251C 577C6047 EBFFB5FE


------------

  BlockEncrypt

  Key is
                     C4C14823 AE157968 6F2C4676 8030DE37


  X is
                     95EC1158 E6CD251C 577C6047 EBFFB5FE


  X = BlockEncrypt(Key, X) is
                     C2659E6A EFBB0DFB 2096A598 CC1C509F


  temp is
                     C2659E6A EFBB0DFB 2096A598 CC1C509F


------------

  BlockEncrypt

  Key is
                     C4C14823 AE157968 6F2C4676 8030DE37


  X is
                     C2659E6A EFBB0DFB 2096A598 CC1C509F
```

```
      X = BlockEncrypt(Key, X) is
                          D926A4C1 E62F8936 D419709D 6124946A

      temp is
                                             C2659E6A EFBB0DFB
        2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

      requested_bits is
                                             C2659E6A EFBB0DFB
        2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

    seed_material is
                                             C2659E6A EFBB0DFB
        2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

---------------------------

  Update

    provided_data is
                                             C2659E6A EFBB0DFB
        2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

    ------------

      While loop

      Key is
                          00000000 00000000 00000000 00000000

      V is
                          00000000 00000000 00000000 00000001

      output_block is
                          58E2FCCE FA7E3061 367F1D57 A4E7455A
```

```
      temp is
                          58E2FCCE FA7E3061 367F1D57 A4E7455A


    ------------

      While loop

      Key is
                          00000000 00000000 00000000 00000000


      V is
                          00000000 00000000 00000000 00000002


      output_block is
                          0388DACE 60B6A392 F328C2B9 71B2FE78


      temp is
                                            58E2FCCE FA7E3061
        367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78


    temp XOR provided_data is
                                            9A8762A4 15C53D9A
        16E9B8CF 68FB15C5 DAAE7E0F 86992AA4 2731B224 10966A12


    Key is
                          9A8762A4 15C53D9A 16E9B8CF 68FB15C5


    V is
                          DAAE7E0F 86992AA4 2731B224 10966A12


------------------------------------------------------------

First call to Generate

************************************************************

CTR_DRBG_Generate
```

```
  requested_number_of_bits = 256

    additional_input is
                                                60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    additional_input is
                                                60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


---------------------------

  Block_Cipher_df

    input_str is
                           80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F 60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    number_of_bits_to_return = 256

    S is
                                                00000040 00000020
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F 60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000


    ------------

      BCC

      IV is
```

```
                    00000000 00000000 00000000 00000000

  IV || S is
    00000000 00000000 00000000 00000000 00000040 00000020
    80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
    98999A9B 9C9D9E9F 60616263 64656667 68696A6B 6C6D6E6F
    70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000

temp is
                    EBE472ED 18D7D72C A576D5D0 4F951FF2

------------

  BCC

  IV is
                    00000001 00000000 00000000 00000000

  IV || S is
    00000001 00000000 00000000 00000000 00000040 00000020
    80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
    98999A9B 9C9D9E9F 60616263 64656667 68696A6B 6C6D6E6F
    70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000

temp is
                                        EBE472ED 18D7D72C
    A576D5D0 4F951FF2 E1753FDA 28CA0A50 0C8D0BE0 F45D9C20

------------

Key is
                    EBE472ED 18D7D72C A576D5D0 4F951FF2

X is
                    E1753FDA 28CA0A50 0C8D0BE0 F45D9C20

------------
```

```
      BlockEncrypt

      Key is
                           EBE472ED 18D7D72C A576D5D0 4F951FF2


      X is
                           E1753FDA 28CA0A50 0C8D0BE0 F45D9C20


      X = BlockEncrypt(Key, X) is
                           C1F7BD08 F11F831D FFE48696 8B706115


      temp is
                           C1F7BD08 F11F831D FFE48696 8B706115


    ------------

      BlockEncrypt

      Key is
                           EBE472ED 18D7D72C A576D5D0 4F951FF2


      X is
                           C1F7BD08 F11F831D FFE48696 8B706115


      X = BlockEncrypt(Key, X) is
                           7D71F428 FC13B31C 0AB3A4BB 7FA41524


      temp is
                                               C1F7BD08 F11F831D
        FFE48696 8B706115 7D71F428 FC13B31C 0AB3A4BB 7FA41524


      requested_bits is
                                               C1F7BD08 F11F831D
        FFE48696 8B706115 7D71F428 FC13B31C 0AB3A4BB 7FA41524


--------------------------
```

```
Update

  provided_data is
                                                C1F7BD08 F11F831D
      FFE48696 8B706115 7D71F428 FC13B31C 0AB3A4BB 7FA41524


  ------------

    While loop

    Key is
                        9A8762A4 15C53D9A 16E9B8CF 68FB15C5


    V is
                        DAAE7E0F 86992AA4 2731B224 10966A13


    output_block is
                        18FDEFBD C43D7A36 D5D6D862 205765D1


    temp is
                        18FDEFBD C43D7A36 D5D6D862 205765D1


  ------------

    While loop

    Key is
                        9A8762A4 15C53D9A 16E9B8CF 68FB15C5


    V is
                        DAAE7E0F 86992AA4 2731B224 10966A14


    output_block is
                        D701C9F2 37007030 DF1B8E70 EE4EEE29


    temp is
                                                18FDEFBD C43D7A36
      D5D6D862 205765D1 D701C9F2 37007030 DF1B8E70 EE4EEE29
```

```
    temp XOR provided_data is
                                                D90A52B5 3522F92B
        2A325EF4 AB2704C4 AA703DDA CB13C32C D5A82ACB 91EAFB0D


    Key is
                          D90A52B5 3522F92B 2A325EF4 AB2704C4


    V is
                          AA703DDA CB13C32C D5A82ACB 91EAFB0D


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                          D90A52B5 3522F92B 2A325EF4 AB2704C4


      V is
                          AA703DDA CB13C32C D5A82ACB 91EAFB10


      output_block is
                          19ED3F6B 4C63004C 8E48DDF5 E8389046
```

```
      temp is
                          19ED3F6B 4C63004C 8E48DDF5 E8389046


    ------------

      While loop

      Key is
                          D90A52B5 3522F92B 2A325EF4 AB2704C4


      V is
                          AA703DDA CB13C32C D5A82ACB 91EAFB11


      output_block is
                          B51A544A 9C38D15D 30944D92 C709A151


      temp is
                                               19ED3F6B 4C63004C
        8E48DDF5 E8389046 B51A544A 9C38D15D 30944D92 C709A151


    temp XOR provided_data is
                                               19ED3F6B 4C63004C
        8E48DDF5 E8389046 B51A544A 9C38D15D 30944D92 C709A151


    Key is
                          19ED3F6B 4C63004C 8E48DDF5 E8389046


    V is
                          B51A544A 9C38D15D 30944D92 C709A151


rnd_val is
                                               87D6BDA1 9F461BF0
        B4E1D5BC 87A265A4 AE118AF2 8AB3D8E9 62827B79 08C76279


------------------------------------------------------------
```

```
Second call to Generate

****************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


Generate FAILED: Reseed is required
****************************************************************

CTR_DRBG_Reseed

    entropy_input is
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    additional_input is
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


---------------------------

  Block_Cipher_df

    input_str is
                           C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    number_of_bits_to_return = 256

    S is
                                                00000040 00000020
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000
```

```
------------

  BCC

  IV is
                      00000000 00000000 00000000 00000000


  IV || S is
    00000000 00000000 00000000 00000000 00000040 00000020
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
    D8D9DADB DCDDDEDF A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
    B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000


temp is
                      F57B5902 0636E7E2 20EDB29F 6EBCC72D


------------

  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
    00000001 00000000 00000000 00000000 00000040 00000020
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
    D8D9DADB DCDDDEDF A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
    B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000


temp is
                                        F57B5902 0636E7E2
    20EDB29F 6EBCC72D DFA80B3D A0FFF2E7 E81EE4ED 18CDECA6


------------

Key is
                      F57B5902 0636E7E2 20EDB29F 6EBCC72D
```

```
X is
                    DFA80B3D A0FFF2E7 E81EE4ED 18CDECA6


------------

  BlockEncrypt

  Key is
                    F57B5902 0636E7E2 20EDB29F 6EBCC72D


  X is
                    DFA80B3D A0FFF2E7 E81EE4ED 18CDECA6


  X = BlockEncrypt(Key, X) is
                    DC4290C1 50AD02F0 B68092DA E2472F86


  temp is
                    DC4290C1 50AD02F0 B68092DA E2472F86


------------

  BlockEncrypt

  Key is
                    F57B5902 0636E7E2 20EDB29F 6EBCC72D


  X is
                    DC4290C1 50AD02F0 B68092DA E2472F86


  X = BlockEncrypt(Key, X) is
                    AF2B9220 9762D534 4076FF12 D162E485


  temp is
                                      DC4290C1 50AD02F0
    B68092DA E2472F86 AF2B9220 9762D534 4076FF12 D162E485
```

```
      requested_bits is
                                                DC4290C1 50AD02F0
        B68092DA E2472F86 AF2B9220 9762D534 4076FF12 D162E485


---------------------------

  Update

    provided_data is
                                                DC4290C1 50AD02F0
        B68092DA E2472F86 AF2B9220 9762D534 4076FF12 D162E485


    ------------

      While loop

      Key is
                          19ED3F6B 4C63004C 8E48DDF5 E8389046


      V is
                          B51A544A 9C38D15D 30944D92 C709A152


      output_block is
                          DB89FDFE 2A4C1124 BE15D236 18668BE6


      temp is
                          DB89FDFE 2A4C1124 BE15D236 18668BE6


    ------------

      While loop

      Key is
                          19ED3F6B 4C63004C 8E48DDF5 E8389046


      V is
                          B51A544A 9C38D15D 30944D92 C709A153
```

```
      output_block is
                          F10F36FD 869D45CB 2FA79450 F27B30FF


      temp is
                                                 DB89FDFE 2A4C1124
        BE15D236 18668BE6 F10F36FD 869D45CB 2FA79450 F27B30FF


    temp XOR provided_data is
                                                 07CB6D3F 7AE113D4
        089540EC FA21A460 5E24A4DD 11FF90FF 6FD16B42 2319D47A


    Key is
                          07CB6D3F 7AE113D4 089540EC FA21A460


    V is
                          5E24A4DD 11FF90FF 6FD16B42 2319D47A


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                                                 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                          07CB6D3F 7AE113D4 089540EC FA21A460
```

```
  V is
                      5E24A4DD 11FF90FF 6FD16B42 2319D47D

  output_block is
                      E7950365 FE7156AA 4A8E253B 03021DE4

  temp is
                      E7950365 FE7156AA 4A8E253B 03021DE4

------------

  While loop

  Key is
                      07CB6D3F 7AE113D4 089540EC FA21A460

  V is
                      5E24A4DD 11FF90FF 6FD16B42 2319D47E

  output_block is
                      54C4DAE2 D0160479 C7C5529F 376DA9A7

  temp is
                                        E7950365 FE7156AA
    4A8E253B 03021DE4 54C4DAE2 D0160479 C7C5529F 376DA9A7

temp XOR provided_data is
                                        E7950365 FE7156AA
    4A8E253B 03021DE4 54C4DAE2 D0160479 C7C5529F 376DA9A7

Key is
                      E7950365 FE7156AA 4A8E253B 03021DE4

V is
                      54C4DAE2 D0160479 C7C5529F 376DA9A7
```

```
rnd_val is
                                                2D59B89D C71C48D6
        C327A7E2 C4328ECE AF85FB5F 8EE00226 1B0FC412 90ECE29F


################################################################

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                           00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                           80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                           C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    Nonce =
                                    20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                           00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
```

```
    nonce is
                                  20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                                                          00010203
        04050607 08090A0B 0C0D0E0F 10111213 14151617 18191A1B
        1C1D1E1F 20212223 24252627 20212223 24252627 28292A2B


    number_of_bits_to_return = 320

    S is
                          00000034 00000028 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 20212223 24252627 28292A2B 80000000


    ------------

      BCC

      IV is
                          00000000 00000000 00000000 00000000


      IV || S is
                                                 00000000 00000000
        00000000 00000000 00000034 00000028 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 20212223 24252627 28292A2B 80000000


    temp is
                          2D64B3D8 692984AD B6FBBA41 F69E74E1
```

```
------------

  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
                                           00000001 00000000
    00000000 00000000 00000034 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 80000000


temp is
                                           2D64B3D8 692984AD
    B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E 66616F2E 9F91BC31


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                                           00000002 00000000
    00000000 00000000 00000034 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 80000000


temp is
    2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E
    66616F2E 9F91BC31 C6ADE98F EB96A83C A6F71BF5 BCE6944D


------------

Key is
    2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E
```

```
X is
                    66616F2E 9F91BC31 C6ADE98F EB96A83C


------------

  BlockEncrypt

  Key is
    2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E


  X is
                    66616F2E 9F91BC31 C6ADE98F EB96A83C


  X = BlockEncrypt(Key, X) is
                    45EBC7A3 4CB5BFDB A58CBFCC A756DDCB


  temp is
                    45EBC7A3 4CB5BFDB A58CBFCC A756DDCB


------------

  BlockEncrypt

  Key is
    2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E


  X is
                    45EBC7A3 4CB5BFDB A58CBFCC A756DDCB


  X = BlockEncrypt(Key, X) is
                    7150F160 187803C2 0380FB02 636C8E59


  temp is
                                      45EBC7A3 4CB5BFDB
    A58CBFCC A756DDCB 7150F160 187803C2 0380FB02 636C8E59


------------
```

```
      BlockEncrypt

      Key is
        2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E


      X is
                           7150F160 187803C2 0380FB02 636C8E59


      X = BlockEncrypt(Key, X) is
                           B1A94E9C C2360559 9C002E3A 221F5C21


      temp is
        45EBC7A3 4CB5BFDB A58CBFCC A756DDCB 7150F160 187803C2
        0380FB02 636C8E59 B1A94E9C C2360559 9C002E3A 221F5C21


      requested_bits is
                           45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
        7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559


    seed_material is
                           45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
        7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559


---------------------------

  Update

    provided_data is
                           45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
        7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559


    ------------

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000
```

```
  V is
                      00000000 00000000 00000000 00000001

  output_block is
                      CD33B28A C773F74B A00ED1F3 12572435

  temp is
                      CD33B28A C773F74B A00ED1F3 12572435

------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000002

  output_block is
                      98E7247C 07F0FE41 1C267E43 84B0F600

  temp is
                                        CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600

------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000003
```

```
      output_block is
                          2A3493E6 6235EE67 DEECCD2F 3B393BD8


      temp is
        CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
        1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8


    temp XOR provided_data is
                          88D87529 8BC64890 05826E3F B501F9FE
        E9B7D51C 1F88FD83 1FA68541 E7DC7859 9B9DDD7A A003EB3E


    Key is
        88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83


    V is
                          1FA68541 E7DC7859 9B9DDD7A A003EB3E


---------------------------------------------------------------

First call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop
```

```
  Key is
    88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83


  V is
                       1FA68541 E7DC7859 9B9DDD7A A003EB41


  output_block is
                       FC55C88D AFA06880 F2C73C08 1E8FA294


  temp is
                       FC55C88D AFA06880 F2C73C08 1E8FA294


------------

  While loop

  Key is
    88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83


  V is
                       1FA68541 E7DC7859 9B9DDD7A A003EB42


  output_block is
                       DBE69237 CDB6EF72 96CE3A7B 114703B2


  temp is
                                         FC55C88D AFA06880
    F2C73C08 1E8FA294 DBE69237 CDB6EF72 96CE3A7B 114703B2


------------

  While loop

  Key is
    88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83
```

```
      V is
                          1FA68541 E7DC7859 9B9DDD7A A003EB43


      output_block is
                          8810183A 1A7C9CFC 14560D9C 4FE75670


      temp is
        FC55C88D AFA06880 F2C73C08 1E8FA294 DBE69237 CDB6EF72
        96CE3A7B 114703B2 8810183A 1A7C9CFC 14560D9C 4FE75670


    temp XOR provided_data is
                          FC55C88D AFA06880 F2C73C08 1E8FA294
        DBE69237 CDB6EF72 96CE3A7B 114703B2 8810183A 1A7C9CFC


    Key is
        FC55C88D AFA06880 F2C73C08 1E8FA294 DBE69237 CDB6EF72


    V is
                          96CE3A7B 114703B2 8810183A 1A7C9CFC


rnd_val is
                                             1A646BB1 D38BD2AE
        A30CF5C5 D812A624 B50D3ECA 99E508B2 5B5448A8 B96C0F2E


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update
```

```
provided_data is
                      00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


------------

  While loop

  Key is
    FC55C88D AFA06880 F2C73C08 1E8FA294 DBE69237 CDB6EF72


  V is
                      96CE3A7B 114703B2 8810183A 1A7C9CFF


  output_block is
                      2F3BBFBD 6D63C6B1 84E68CEC CC43AD6D


  temp is
                      2F3BBFBD 6D63C6B1 84E68CEC CC43AD6D


------------

  While loop

  Key is
    FC55C88D AFA06880 F2C73C08 1E8FA294 DBE69237 CDB6EF72


  V is
                      96CE3A7B 114703B2 8810183A 1A7C9D00


  output_block is
                      DF160344 BF7E8318 E7D017F5 94D5C087


  temp is
                                        2F3BBFBD 6D63C6B1
    84E68CEC CC43AD6D DF160344 BF7E8318 E7D017F5 94D5C087
```

```
    ------------

      While loop

      Key is
        FC55C88D AFA06880 F2C73C08 1E8FA294 DBE69237 CDB6EF72


      V is
                           96CE3A7B 114703B2 8810183A 1A7C9D01


      output_block is
                           DEDEBD95 523BD30A DC046C03 94AC5E42


      temp is
        2F3BBFBD 6D63C6B1 84E68CEC CC43AD6D DF160344 BF7E8318
        E7D017F5 94D5C087 DEDEBD95 523BD30A DC046C03 94AC5E42


    temp XOR provided_data is
                           2F3BBFBD 6D63C6B1 84E68CEC CC43AD6D
        DF160344 BF7E8318 E7D017F5 94D5C087 DEDEBD95 523BD30A


    Key is
        2F3BBFBD 6D63C6B1 84E68CEC CC43AD6D DF160344 BF7E8318


    V is
                           E7D017F5 94D5C087 DEDEBD95 523BD30A


rnd_val is
                                            0920CB32 A773E0FF
        4BBBF90A CB1D7044 E15B629A FB3C7F9F E26673E3 E7BE4727


################################################################

CTR_DRBG

    Requested Security Strength = 192
```

```
    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    Nonce =
                                   20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput1 =
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


    AdditionalInput2 =
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


##############################################################

**************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    nonce is
                                   20212223 24252627 28292A2B
```

```
    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                                                            00010203
        04050607 08090A0B 0C0D0E0F 10111213 14151617 18191A1B
        1C1D1E1F 20212223 24252627 20212223 24252627 28292A2B


    number_of_bits_to_return = 320

    S is
                          00000034 00000028 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 20212223 24252627 28292A2B 80000000


    ------------

      BCC

      IV is
                          00000000 00000000 00000000 00000000


      IV || S is
                                                00000000 00000000
        00000000 00000000 00000034 00000028 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 20212223 24252627 28292A2B 80000000


    temp is
                          2D64B3D8 692984AD B6FBBA41 F69E74E1


    ------------

      BCC
```

```
  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
                                           00000001 00000000
    00000000 00000000 00000034 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 80000000


temp is
                                           2D64B3D8 692984AD
    B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E 66616F2E 9F91BC31


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                                           00000002 00000000
    00000000 00000000 00000034 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 80000000


temp is
    2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E
    66616F2E 9F91BC31 C6ADE98F EB96A83C A6F71BF5 BCE6944D


------------

Key is
    2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E


X is
                      66616F2E 9F91BC31 C6ADE98F EB96A83C
```

```
------------

  BlockEncrypt

  Key is
    2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E


  X is
                       66616F2E 9F91BC31 C6ADE98F EB96A83C


  X = BlockEncrypt(Key, X) is
                       45EBC7A3 4CB5BFDB A58CBFCC A756DDCB


  temp is
                       45EBC7A3 4CB5BFDB A58CBFCC A756DDCB


------------

  BlockEncrypt

  Key is
    2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E


  X is
                       45EBC7A3 4CB5BFDB A58CBFCC A756DDCB


  X = BlockEncrypt(Key, X) is
                       7150F160 187803C2 0380FB02 636C8E59


  temp is
                                          45EBC7A3 4CB5BFDB
    A58CBFCC A756DDCB 7150F160 187803C2 0380FB02 636C8E59


------------

  BlockEncrypt

  Key is
```

```
      2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E


    X is
                         7150F160 187803C2 0380FB02 636C8E59


    X = BlockEncrypt(Key, X) is
                         B1A94E9C C2360559 9C002E3A 221F5C21


    temp is
      45EBC7A3 4CB5BFDB A58CBFCC A756DDCB 7150F160 187803C2
      0380FB02 636C8E59 B1A94E9C C2360559 9C002E3A 221F5C21


    requested_bits is
                         45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
      7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559


  seed_material is
                         45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
      7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559


---------------------------

  Update

    provided_data is
                         45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
      7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559


    ------------

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                         00000000 00000000 00000000 00000001
```

```
  output_block is
                      CD33B28A C773F74B A00ED1F3 12572435


  temp is
                      CD33B28A C773F74B A00ED1F3 12572435


------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000002


  output_block is
                      98E7247C 07F0FE41 1C267E43 84B0F600


  temp is
                                        CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000003


  output_block is
                      2A3493E6 6235EE67 DEECCD2F 3B393BD8
```

```
      temp is
        CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
        1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8


    temp XOR provided_data is
                          88D87529 8BC64890 05826E3F B501F9FE
        E9B7D51C 1F88FD83 1FA68541 E7DC7859 9B9DDD7A A003EB3E


    Key is
        88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83


    V is
                          1FA68541 E7DC7859 9B9DDD7A A003EB3E


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


  additional_input <> NULL, process appropriately
---------------------------

  Block_Cipher_df

    input_str is
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


    number_of_bits_to_return = 320

    S is
```

```
                    00000028 00000028 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 80000000 00000000 00000000 00000000


------------

  BCC

  IV is
                    00000000 00000000 00000000 00000000


  IV || S is
                                        00000000 00000000
    00000000 00000000 00000028 00000028 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 80000000 00000000 00000000 00000000


temp is
                    E5460ACC 5126F932 D56D1A29 1FC4A2A2


------------

  BCC

  IV is
                    00000001 00000000 00000000 00000000


  IV || S is
                                        00000001 00000000
    00000000 00000000 00000028 00000028 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 80000000 00000000 00000000 00000000


temp is
                                        E5460ACC 5126F932
    D56D1A29 1FC4A2A2 280D9844 33D9A0F7 BE003DAF 2996B5CF


------------
```

```
  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                                              00000002 00000000
    00000000 00000000 00000028 00000028 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 80000000 00000000 00000000 00000000


temp is
    E5460ACC 5126F932 D56D1A29 1FC4A2A2 280D9844 33D9A0F7
    BE003DAF 2996B5CF 5AD5C453 7046B98F C143E7B2 F9A465C4


------------

Key is
    E5460ACC 5126F932 D56D1A29 1FC4A2A2 280D9844 33D9A0F7


X is
                      BE003DAF 2996B5CF 5AD5C453 7046B98F


------------

  BlockEncrypt

  Key is
    E5460ACC 5126F932 D56D1A29 1FC4A2A2 280D9844 33D9A0F7


  X is
                      BE003DAF 2996B5CF 5AD5C453 7046B98F


  X = BlockEncrypt(Key, X) is
                      A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C


  temp is
                      A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C
```

```
------------

  BlockEncrypt

  Key is
    E5460ACC 5126F932 D56D1A29 1FC4A2A2 280D9844 33D9A0F7


  X is
                      A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C


  X = BlockEncrypt(Key, X) is
                      3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1


  temp is
                                        A2F76A3A 0305FCDE
    2DB7FA2D ED8DE90C 3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1


------------

  BlockEncrypt

  Key is
    E5460ACC 5126F932 D56D1A29 1FC4A2A2 280D9844 33D9A0F7


  X is
                      3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1


  X = BlockEncrypt(Key, X) is
                      B2AA5CA0 E45067DE 84D9D2FA FDA512C9


  temp is
    A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C 3E877DE5 FA752EB7
    2F7C3CA4 87B7C3F1 B2AA5CA0 E45067DE 84D9D2FA FDA512C9


  requested_bits is
                      A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C
```

```
        3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1 B2AA5CA0 E45067DE


---------------------------

  Update

    provided_data is
                          A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C
        3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1 B2AA5CA0 E45067DE


    ------------

      While loop

      Key is
        88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83


      V is
                          1FA68541 E7DC7859 9B9DDD7A A003EB3F


      output_block is
                          1A646BB1 D38BD2AE A30CF5C5 D812A624


      temp is
                          1A646BB1 D38BD2AE A30CF5C5 D812A624


    ------------

      While loop

      Key is
        88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83


      V is
                          1FA68541 E7DC7859 9B9DDD7A A003EB40


      output_block is
                          B50D3ECA 99E508B2 5B5448A8 B96C0F2E
```

```
      temp is
                                              1A646BB1 D38BD2AE
        A30CF5C5 D812A624 B50D3ECA 99E508B2 5B5448A8 B96C0F2E


    ------------

      While loop

      Key is
        88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83


      V is
                           1FA68541 E7DC7859 9B9DDD7A A003EB41


      output_block is
                           FC55C88D AFA06880 F2C73C08 1E8FA294


      temp is
        1A646BB1 D38BD2AE A30CF5C5 D812A624 B50D3ECA 99E508B2
        5B5448A8 B96C0F2E FC55C88D AFA06880 F2C73C08 1E8FA294


    temp XOR provided_data is
                           B893018B D08E2E70 8EBB0FE8 359F4F28
        8B8A432F 63902605 7428740C 3EDBCCDF 4EFF942D 4BF00F5E


    Key is
        B893018B D08E2E70 8EBB0FE8 359F4F28 8B8A432F 63902605


    V is
                           7428740C 3EDBCCDF 4EFF942D 4BF00F5E


---------------------------

  Update

    provided_data is
```

```
                     A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C
    3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1 B2AA5CA0 E45067DE


------------

  While loop

  Key is
    B893018B D08E2E70 8EBB0FE8 359F4F28 8B8A432F 63902605


  V is
                     7428740C 3EDBCCDF 4EFF942D 4BF00F61


  output_block is
                     E346B483 9677B724 7BE0AAB3 B1B969CA


  temp is
                     E346B483 9677B724 7BE0AAB3 B1B969CA


------------

  While loop

  Key is
    B893018B D08E2E70 8EBB0FE8 359F4F28 8B8A432F 63902605


  V is
                     7428740C 3EDBCCDF 4EFF942D 4BF00F62


  output_block is
                     B13C2105 AE36F9F1 27ECBD37 E72AB845


  temp is
                                       E346B483 9677B724
    7BE0AAB3 B1B969CA B13C2105 AE36F9F1 27ECBD37 E72AB845


------------
```

```
      While loop

      Key is
        B893018B D08E2E70 8EBB0FE8 359F4F28 8B8A432F 63902605


      V is
                          7428740C 3EDBCCDF 4EFF942D 4BF00F63


      output_block is
                          30C645C9 C33C3CA7 C827ACB0 825A11CF


      temp is
        E346B483 9677B724 7BE0AAB3 B1B969CA B13C2105 AE36F9F1
        27ECBD37 E72AB845 30C645C9 C33C3CA7 C827ACB0 825A11CF


    temp XOR provided_data is
                          41B1DEB9 95724BFA 5657509E 5C3480C6
        8FBB5CE0 5443D746 08908193 609D7BB4 826C1969 276C5B79


    Key is
        41B1DEB9 95724BFA 5657509E 5C3480C6 8FBB5CE0 5443D746


    V is
                          08908193 609D7BB4 826C1969 276C5B79


rnd_val is
                                             6157D6C6 22896303
        FE8E748C 18F2CE2E DF5C8A30 B8BBC26F D44C683D 7B150A97


------------------------------------------------------------

Second call to Generate

************************************************************

CTR_DRBG_Generate
```

```
  requested_number_of_bits = 256

    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


  additional_input <> NULL, process appropriately
----------------------------

  Block_Cipher_df

    input_str is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


    number_of_bits_to_return = 320

    S is
                          00000028 00000028 A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
        C0C1C2C3 C4C5C6C7 80000000 00000000 00000000 00000000


    ------------

      BCC

      IV is
                          00000000 00000000 00000000 00000000


      IV || S is
                                                00000000 00000000
        00000000 00000000 00000028 00000028 A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
        C0C1C2C3 C4C5C6C7 80000000 00000000 00000000 00000000


    temp is
                          0DEF5001 1B1229C8 3DD880BE E398BDD8


    ------------
```

```
  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
                                           00000001 00000000
    00000000 00000000 00000028 00000028 A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
    C0C1C2C3 C4C5C6C7 80000000 00000000 00000000 00000000


temp is
                                           0DEF5001 1B1229C8
    3DD880BE E398BDD8 61E3855F 743C9876 6CCEDC9B 90C1461E


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                                           00000002 00000000
    00000000 00000000 00000028 00000028 A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
    C0C1C2C3 C4C5C6C7 80000000 00000000 00000000 00000000


temp is
    0DEF5001 1B1229C8 3DD880BE E398BDD8 61E3855F 743C9876
    6CCEDC9B 90C1461E 92B6D6BA 30B91657 85E11146 2B2050F1


------------

Key is
    0DEF5001 1B1229C8 3DD880BE E398BDD8 61E3855F 743C9876


X is
                      6CCEDC9B 90C1461E 92B6D6BA 30B91657
```

```
------------

  BlockEncrypt

  Key is
    0DEF5001 1B1229C8 3DD880BE E398BDD8 61E3855F 743C9876


  X is
                       6CCEDC9B 90C1461E 92B6D6BA 30B91657


  X = BlockEncrypt(Key, X) is
                       1F2069F0 C00F3158 44CF0216 2913FC35


  temp is
                       1F2069F0 C00F3158 44CF0216 2913FC35


------------

  BlockEncrypt

  Key is
    0DEF5001 1B1229C8 3DD880BE E398BDD8 61E3855F 743C9876


  X is
                       1F2069F0 C00F3158 44CF0216 2913FC35


  X = BlockEncrypt(Key, X) is
                       F485B9DC 9EFDA069 E47E7C8D 674FECE1


  temp is
                                         1F2069F0 C00F3158
    44CF0216 2913FC35 F485B9DC 9EFDA069 E47E7C8D 674FECE1


------------

  BlockEncrypt
```

```
      Key is
        0DEF5001 1B1229C8 3DD880BE E398BDD8 61E3855F 743C9876


      X is
                           F485B9DC 9EFDA069 E47E7C8D 674FECE1


      X = BlockEncrypt(Key, X) is
                           3AB17BE9 025A1ACE F7E2A934 A3DDFD0B


      temp is
        1F2069F0 C00F3158 44CF0216 2913FC35 F485B9DC 9EFDA069
        E47E7C8D 674FECE1 3AB17BE9 025A1ACE F7E2A934 A3DDFD0B


      requested_bits is
                           1F2069F0 C00F3158 44CF0216 2913FC35
        F485B9DC 9EFDA069 E47E7C8D 674FECE1 3AB17BE9 025A1ACE


---------------------------

  Update

    provided_data is
                           1F2069F0 C00F3158 44CF0216 2913FC35
        F485B9DC 9EFDA069 E47E7C8D 674FECE1 3AB17BE9 025A1ACE


    ------------

      While loop

      Key is
        41B1DEB9 95724BFA 5657509E 5C3480C6 8FBB5CE0 5443D746


      V is
                           08908193 609D7BB4 826C1969 276C5B7A


      output_block is
                           D982D885 7401F676 F76F9E47 923C805D
```

```
  temp is
                      D982D885 7401F676 F76F9E47 923C805D


------------

  While loop

  Key is
    41B1DEB9 95724BFA 5657509E 5C3480C6 8FBB5CE0 5443D746


  V is
                      08908193 609D7BB4 826C1969 276C5B7B


  output_block is
                      100F2574 62B6A6D6 0DEFE841 138AA5F7


  temp is
                                        D982D885 7401F676
    F76F9E47 923C805D 100F2574 62B6A6D6 0DEFE841 138AA5F7


------------

  While loop

  Key is
    41B1DEB9 95724BFA 5657509E 5C3480C6 8FBB5CE0 5443D746


  V is
                      08908193 609D7BB4 826C1969 276C5B7C


  output_block is
                      D5D8AE6E 3D66D253 B4C1824D F6736A5C


  temp is
    D982D885 7401F676 F76F9E47 923C805D 100F2574 62B6A6D6
    0DEFE841 138AA5F7 D5D8AE6E 3D66D253 B4C1824D F6736A5C
```

```
    temp XOR provided_data is
                          C6A2B175 B40EC72E B3A09C51 BB2F7C68
        E48A9CA8 FC4B06BF E99194CC 74C54916 EF69D587 3F3CC89D


    Key is
        C6A2B175 B40EC72E B3A09C51 BB2F7C68 E48A9CA8 FC4B06BF


    V is
                          E99194CC 74C54916 EF69D587 3F3CC89D


---------------------------

  Update

    provided_data is
                          1F2069F0 C00F3158 44CF0216 2913FC35
        F485B9DC 9EFDA069 E47E7C8D 674FECE1 3AB17BE9 025A1ACE


    ------------

      While loop

      Key is
        C6A2B175 B40EC72E B3A09C51 BB2F7C68 E48A9CA8 FC4B06BF


      V is
                          E99194CC 74C54916 EF69D587 3F3CC8A0


      output_block is
                          6426D45A 9387D0FD EA65286E 3B751CEF


      temp is
                          6426D45A 9387D0FD EA65286E 3B751CEF


    ------------
```

```
  While loop

  Key is
    C6A2B175 B40EC72E B3A09C51 BB2F7C68 E48A9CA8 FC4B06BF


  V is
                      E99194CC 74C54916 EF69D587 3F3CC8A1


  output_block is
                      5CA13272 687E3828 0C24DBA3 36344980


  temp is
                                        6426D45A 9387D0FD
    EA65286E 3B751CEF 5CA13272 687E3828 0C24DBA3 36344980


------------

  While loop

  Key is
    C6A2B175 B40EC72E B3A09C51 BB2F7C68 E48A9CA8 FC4B06BF


  V is
                      E99194CC 74C54916 EF69D587 3F3CC8A2


  output_block is
                      AE880B7B 64CD81C1 1920D6B3 8112D7DE


  temp is
    6426D45A 9387D0FD EA65286E 3B751CEF 5CA13272 687E3828
    0C24DBA3 36344980 AE880B7B 64CD81C1 1920D6B3 8112D7DE


temp XOR provided_data is
                      7B06BDAA 5388E1A5 AEAA2A78 1266E0DA
    A8248BAE F6839841 E85AA72E 517BA561 94397092 66979B0F


Key is
```

```
        7B06BDAA 5388E1A5 AEAA2A78 1266E0DA A8248BAE F6839841


    V is
                           E85AA72E 517BA561 94397092 66979B0F


rnd_val is
                                              1F6DBD50 693817A1
        9EF22622 3AB727E1 67158848 35CA0C5B 3B46D570 B4DD975A


###############################################################

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                           00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                           80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                           C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    Nonce =
                                    20212223 24252627 28292A2B


    PersonalizationString =
                           40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    AdditionalInput = <empty>

###############################################################
```

```
************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    nonce is
                                   20212223 24252627 28292A2B


    personal_str is
                          40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                 00010203 04050607 08090A0B 0C0D0E0F 10111213
        14151617 18191A1B 1C1D1E1F 20212223 24252627 20212223
        24252627 28292A2B 40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    number_of_bits_to_return = 320

    S is
                          0000005C 00000028 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 20212223 24252627 28292A2B 40414243
        44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
        5C5D5E5F 60616263 64656667 80000000 00000000 00000000


    ------------

      BCC
```

```
  IV is
                    00000000 00000000 00000000 00000000


  IV || S is
                                             00000000 00000000
    00000000 00000000 0000005C 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 40414243
    44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
    5C5D5E5F 60616263 64656667 80000000 00000000 00000000


temp is
                    883662C0 53AC837C 186A91D7 0C5398FA


------------

  BCC

  IV is
                    00000001 00000000 00000000 00000000


  IV || S is
                                             00000001 00000000
    00000000 00000000 0000005C 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 40414243
    44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
    5C5D5E5F 60616263 64656667 80000000 00000000 00000000


temp is
                                             883662C0 53AC837C
    186A91D7 0C5398FA 9028263E F8303EE6 F7658E84 1E8EDDB4


------------

  BCC

  IV is
                    00000002 00000000 00000000 00000000
```

```
  IV || S is
                                              00000002 00000000
    00000000 00000000 0000005C 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 40414243
    44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
    5C5D5E5F 60616263 64656667 80000000 00000000 00000000


temp is
    883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6
    F7658E84 1E8EDDB4 BA630844 25877431 5143AC1F 156049EB


------------

Key is
    883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6


X is
                     F7658E84 1E8EDDB4 BA630844 25877431


------------

  BlockEncrypt

  Key is
    883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6


  X is
                     F7658E84 1E8EDDB4 BA630844 25877431


  X = BlockEncrypt(Key, X) is
                     AC49318E F0FA3331 F54CFB30 6C9B7B15


  temp is
                     AC49318E F0FA3331 F54CFB30 6C9B7B15


------------
```

```
  BlockEncrypt

  Key is
    883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6


  X is
                       AC49318E F0FA3331 F54CFB30 6C9B7B15


  X = BlockEncrypt(Key, X) is
                       9334B962 5E62F257 2431DA7D 0A5F7534


  temp is
                                         AC49318E F0FA3331
    F54CFB30 6C9B7B15 9334B962 5E62F257 2431DA7D 0A5F7534


------------

  BlockEncrypt

  Key is
    883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6


  X is
                       9334B962 5E62F257 2431DA7D 0A5F7534


  X = BlockEncrypt(Key, X) is
                       B22E0E89 FF0FF392 A7CECDBE 5A4E766F


  temp is
    AC49318E F0FA3331 F54CFB30 6C9B7B15 9334B962 5E62F257
    2431DA7D 0A5F7534 B22E0E89 FF0FF392 A7CECDBE 5A4E766F


  requested_bits is
                       AC49318E F0FA3331 F54CFB30 6C9B7B15
    9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392
```

```
    seed_material is
                           AC49318E F0FA3331 F54CFB30 6C9B7B15
        9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392


---------------------------

  Update

    provided_data is
                           AC49318E F0FA3331 F54CFB30 6C9B7B15
        9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392


    ------------

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001


      output_block is
                           CD33B28A C773F74B A00ED1F3 12572435


      temp is
                           CD33B28A C773F74B A00ED1F3 12572435


    ------------

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000002
```

```
      output_block is
                          98E7247C 07F0FE41 1C267E43 84B0F600

      temp is
                                               CD33B28A C773F74B
        A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600

    ------------

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000

      V is
                          00000000 00000000 00000000 00000003

      output_block is
                          2A3493E6 6235EE67 DEECCD2F 3B393BD8

      temp is
        CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
        1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8

    temp XOR provided_data is
                          617A8304 3789C47A 55422AC3 7ECC5F20
        0BD39D1E 59920C16 3817A43E 8EEF8334 981A9D6F 9D3A1DF5

    Key is
        617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16

    V is
                          3817A43E 8EEF8334 981A9D6F 9D3A1DF5

------------------------------------------------------------

First call to Generate
```

```
***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
        617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16


      V is
                          3817A43E 8EEF8334 981A9D6F 9D3A1DF8


      output_block is
                          6C0BA382 122A6E1E BEB51820 656D3D45


      temp is
                          6C0BA382 122A6E1E BEB51820 656D3D45


    ------------

      While loop

      Key is
        617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16
```

```
  V is
                      3817A43E 8EEF8334 981A9D6F 9D3A1DF9


  output_block is
                      B0B4DA3A EDAF317E 1A823DC4 D0A03B6C


  temp is
                                        6C0BA382 122A6E1E
    BEB51820 656D3D45 B0B4DA3A EDAF317E 1A823DC4 D0A03B6C


------------

  While loop

  Key is
    617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16


  V is
                      3817A43E 8EEF8334 981A9D6F 9D3A1DFA


  output_block is
                      2CE4F489 BB227382 A4FBC53E ACD12025


  temp is
    6C0BA382 122A6E1E BEB51820 656D3D45 B0B4DA3A EDAF317E
    1A823DC4 D0A03B6C 2CE4F489 BB227382 A4FBC53E ACD12025


temp XOR provided_data is
                      6C0BA382 122A6E1E BEB51820 656D3D45
    B0B4DA3A EDAF317E 1A823DC4 D0A03B6C 2CE4F489 BB227382


Key is
    6C0BA382 122A6E1E BEB51820 656D3D45 B0B4DA3A EDAF317E


V is
                      1A823DC4 D0A03B6C 2CE4F489 BB227382
```

```
rnd_val is
                                                E231244B 3235B085
        C8160442 4357E852 01E3828B 5C455686 79A5555F 867AAC8C


------------------------------------------------------------

Second call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
        6C0BA382 122A6E1E BEB51820 656D3D45 B0B4DA3A EDAF317E


      V is
                          1A823DC4 D0A03B6C 2CE4F489 BB227385


      output_block is
                          BC0C07EA E35CBFBF 88E428FC F551504C


      temp is
                          BC0C07EA E35CBFBF 88E428FC F551504C
```

```
------------

  While loop

  Key is
    6C0BA382 122A6E1E BEB51820 656D3D45 B0B4DA3A EDAF317E


  V is
                       1A823DC4 D0A03B6C 2CE4F489 BB227386


  output_block is
                       9CC98126 B9758E67 FB830F34 233D1F68


  temp is
                                         BC0C07EA E35CBFBF
    88E428FC F551504C 9CC98126 B9758E67 FB830F34 233D1F68


------------

  While loop

  Key is
    6C0BA382 122A6E1E BEB51820 656D3D45 B0B4DA3A EDAF317E


  V is
                       1A823DC4 D0A03B6C 2CE4F489 BB227387


  output_block is
                       46937CEF 28E4A716 11760A28 05C7ABA8


  temp is
    BC0C07EA E35CBFBF 88E428FC F551504C 9CC98126 B9758E67
    FB830F34 233D1F68 46937CEF 28E4A716 11760A28 05C7ABA8


temp XOR provided_data is
                       BC0C07EA E35CBFBF 88E428FC F551504C
    9CC98126 B9758E67 FB830F34 233D1F68 46937CEF 28E4A716
```

```
    Key is
        BC0C07EA E35CBFBF 88E428FC F551504C 9CC98126 B9758E67


    V is
                          FB830F34 233D1F68 46937CEF 28E4A716


rnd_val is
                                                DDD0F7BC CADADAA3
        1A676522 59CE569A 271DD85C F66C3D6A 7E9FAED6 1F38D219


###############################################################

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    Nonce =
                                   20212223 24252627 28292A2B


    PersonalizationString =
                          40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667
```

```
    AdditionalInput1 =
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


    AdditionalInput2 =
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    nonce is
                                   20212223 24252627 28292A2B


    personal_str is
                          40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                 00010203 04050607 08090A0B 0C0D0E0F 10111213
        14151617 18191A1B 1C1D1E1F 20212223 24252627 20212223
        24252627 28292A2B 40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    number_of_bits_to_return = 320

    S is
```

```
                    0000005C 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 40414243
    44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
    5C5D5E5F 60616263 64656667 80000000 00000000 00000000


------------

  BCC

  IV is
                    00000000 00000000 00000000 00000000


  IV || S is
                                       00000000 00000000
    00000000 00000000 0000005C 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 40414243
    44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
    5C5D5E5F 60616263 64656667 80000000 00000000 00000000


temp is
                    883662C0 53AC837C 186A91D7 0C5398FA


------------

  BCC

  IV is
                    00000001 00000000 00000000 00000000


  IV || S is
                                       00000001 00000000
    00000000 00000000 0000005C 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 40414243
    44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
    5C5D5E5F 60616263 64656667 80000000 00000000 00000000


temp is
```

```
                                          883662C0 53AC837C
    186A91D7 0C5398FA 9028263E F8303EE6 F7658E84 1E8EDDB4


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                                          00000002 00000000
    00000000 00000000 0000005C 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 40414243
    44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
    5C5D5E5F 60616263 64656667 80000000 00000000 00000000


temp is
    883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6
    F7658E84 1E8EDDB4 BA630844 25877431 5143AC1F 156049EB


------------

Key is
    883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6


X is
                      F7658E84 1E8EDDB4 BA630844 25877431


------------

  BlockEncrypt

  Key is
    883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6


  X is
                      F7658E84 1E8EDDB4 BA630844 25877431
```

```
  X = BlockEncrypt(Key, X) is
                      AC49318E F0FA3331 F54CFB30 6C9B7B15


  temp is
                      AC49318E F0FA3331 F54CFB30 6C9B7B15


------------

  BlockEncrypt

  Key is
    883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6


  X is
                      AC49318E F0FA3331 F54CFB30 6C9B7B15


  X = BlockEncrypt(Key, X) is
                      9334B962 5E62F257 2431DA7D 0A5F7534


  temp is
                                        AC49318E F0FA3331
    F54CFB30 6C9B7B15 9334B962 5E62F257 2431DA7D 0A5F7534


------------

  BlockEncrypt

  Key is
    883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6


  X is
                      9334B962 5E62F257 2431DA7D 0A5F7534


  X = BlockEncrypt(Key, X) is
                      B22E0E89 FF0FF392 A7CECDBE 5A4E766F
```

```
      temp is
        AC49318E F0FA3331 F54CFB30 6C9B7B15 9334B962 5E62F257
        2431DA7D 0A5F7534 B22E0E89 FF0FF392 A7CECDBE 5A4E766F


      requested_bits is
                           AC49318E F0FA3331 F54CFB30 6C9B7B15
        9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392


    seed_material is
                           AC49318E F0FA3331 F54CFB30 6C9B7B15
        9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392


---------------------------

  Update

    provided_data is
                           AC49318E F0FA3331 F54CFB30 6C9B7B15
        9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392


    ------------

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001


      output_block is
                           CD33B28A C773F74B A00ED1F3 12572435


      temp is
                           CD33B28A C773F74B A00ED1F3 12572435


    ------------
```

```
  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                       00000000 00000000 00000000 00000002


  output_block is
                       98E7247C 07F0FE41 1C267E43 84B0F600


  temp is
                                         CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                       00000000 00000000 00000000 00000003


  output_block is
                       2A3493E6 6235EE67 DEECCD2F 3B393BD8


  temp is
    CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
    1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8


temp XOR provided_data is
                       617A8304 3789C47A 55422AC3 7ECC5F20
    0BD39D1E 59920C16 3817A43E 8EEF8334 981A9D6F 9D3A1DF5
```

```
    Key is
        617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16


    V is
                          3817A43E 8EEF8334 981A9D6F 9D3A1DF5


---------------------------------------------------------------

First call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


  additional_input <> NULL, process appropriately
---------------------------

  Block_Cipher_df

    input_str is
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


    number_of_bits_to_return = 320

    S is
                          00000028 00000028 60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
        80818283 84858687 80000000 00000000 00000000 00000000


    ------------

      BCC

      IV is
```

```
                    00000000 00000000 00000000 00000000


  IV || S is
                                              00000000 00000000
    00000000 00000000 00000028 00000028 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 80000000 00000000 00000000 00000000


temp is
                    E5460ACC 5126F932 D56D1A29 1FC4A2A2


------------

  BCC

  IV is
                    00000001 00000000 00000000 00000000


  IV || S is
                                              00000001 00000000
    00000000 00000000 00000028 00000028 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 80000000 00000000 00000000 00000000


temp is
                                              E5460ACC 5126F932
    D56D1A29 1FC4A2A2 280D9844 33D9A0F7 BE003DAF 2996B5CF


------------

  BCC

  IV is
                    00000002 00000000 00000000 00000000


  IV || S is
                                              00000002 00000000
    00000000 00000000 00000028 00000028 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
```

```
    80818283 84858687 80000000 00000000 00000000 00000000


temp is
    E5460ACC 5126F932 D56D1A29 1FC4A2A2 280D9844 33D9A0F7
    BE003DAF 2996B5CF 5AD5C453 7046B98F C143E7B2 F9A465C4


------------

Key is
    E5460ACC 5126F932 D56D1A29 1FC4A2A2 280D9844 33D9A0F7


X is
                     BE003DAF 2996B5CF 5AD5C453 7046B98F


------------

  BlockEncrypt

  Key is
    E5460ACC 5126F932 D56D1A29 1FC4A2A2 280D9844 33D9A0F7


  X is
                     BE003DAF 2996B5CF 5AD5C453 7046B98F


  X = BlockEncrypt(Key, X) is
                     A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C


  temp is
                     A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C


------------

  BlockEncrypt

  Key is
    E5460ACC 5126F932 D56D1A29 1FC4A2A2 280D9844 33D9A0F7
```

```
      X is
                          A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C


      X = BlockEncrypt(Key, X) is
                          3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1


      temp is
                                               A2F76A3A 0305FCDE
        2DB7FA2D ED8DE90C 3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1


    ------------

      BlockEncrypt

      Key is
        E5460ACC 5126F932 D56D1A29 1FC4A2A2 280D9844 33D9A0F7


      X is
                          3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1


      X = BlockEncrypt(Key, X) is
                          B2AA5CA0 E45067DE 84D9D2FA FDA512C9


      temp is
        A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C 3E877DE5 FA752EB7
        2F7C3CA4 87B7C3F1 B2AA5CA0 E45067DE 84D9D2FA FDA512C9


      requested_bits is
                          A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C
        3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1 B2AA5CA0 E45067DE


---------------------------

  Update

    provided_data is
                          A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C
       3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1 B2AA5CA0 E45067DE
```

```
------------

  While loop

  Key is
    617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16


  V is
                       3817A43E 8EEF8334 981A9D6F 9D3A1DF6


  output_block is
                       E231244B 3235B085 C8160442 4357E852


  temp is
                       E231244B 3235B085 C8160442 4357E852


------------

  While loop

  Key is
    617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16


  V is
                       3817A43E 8EEF8334 981A9D6F 9D3A1DF7


  output_block is
                       01E3828B 5C455686 79A5555F 867AAC8C


  temp is
                                         E231244B 3235B085
    C8160442 4357E852 01E3828B 5C455686 79A5555F 867AAC8C


------------

  While loop
```

```
      Key is
        617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16


      V is
                           3817A43E 8EEF8334 981A9D6F 9D3A1DF8


      output_block is
                           6C0BA382 122A6E1E BEB51820 656D3D45


      temp is
        E231244B 3235B085 C8160442 4357E852 01E3828B 5C455686
        79A5555F 867AAC8C 6C0BA382 122A6E1E BEB51820 656D3D45


    temp XOR provided_data is
                           40C64E71 31304C5B E5A1FE6F AEDA015E
        3F64FF6E A6307831 56D969FB 01CD6F7D DEA1FF22 F67A09C0


    Key is
        40C64E71 31304C5B E5A1FE6F AEDA015E 3F64FF6E A6307831


    V is
                           56D969FB 01CD6F7D DEA1FF22 F67A09C0


---------------------------

  Update

    provided_data is
                           A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C
        3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1 B2AA5CA0 E45067DE


    ------------

      While loop

      Key is
        40C64E71 31304C5B E5A1FE6F AEDA015E 3F64FF6E A6307831
```

```
  V is
                      56D969FB 01CD6F7D DEA1FF22 F67A09C3


  output_block is
                      DEBD9695 37A6430F 0DB95ED7 3201DBE2


  temp is
                      DEBD9695 37A6430F 0DB95ED7 3201DBE2


------------

  While loop

  Key is
    40C64E71 31304C5B E5A1FE6F AEDA015E 3F64FF6E A6307831


  V is
                      56D969FB 01CD6F7D DEA1FF22 F67A09C4


  output_block is
                      EFBE2871 482A39AB 25F35788 F9A81DA9


  temp is
                                          DEBD9695 37A6430F
    0DB95ED7 3201DBE2 EFBE2871 482A39AB 25F35788 F9A81DA9


------------

  While loop

  Key is
    40C64E71 31304C5B E5A1FE6F AEDA015E 3F64FF6E A6307831


  V is
                      56D969FB 01CD6F7D DEA1FF22 F67A09C5
```

```
      output_block is
                          C720524A D46F4281 57BEFC8B 39800846


      temp is
        DEBD9695 37A6430F 0DB95ED7 3201DBE2 EFBE2871 482A39AB
        25F35788 F9A81DA9 C720524A D46F4281 57BEFC8B 39800846


    temp XOR provided_data is
                          7C4AFCAF 34A3BFD1 200EA4FA DF8C32EE
        D1395594 B25F171C 0A8F6B2C 7E1FDE58 758A0EEA 303F255F


    Key is
        7C4AFCAF 34A3BFD1 200EA4FA DF8C32EE D1395594 B25F171C


    V is
                          0A8F6B2C 7E1FDE58 758A0EEA 303F255F


rnd_val is
                                             242D0B6B 9598779C
        5CF5A50E DFD61C2C 95D383BC 493AC202 845FAC96 D276C092


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


  additional_input <> NULL, process appropriately
---------------------------
```

```
Block_Cipher_df

  input_str is
                        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
      B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


  number_of_bits_to_return = 320

  S is
                        00000028 00000028 A0A1A2A3 A4A5A6A7
      A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
      C0C1C2C3 C4C5C6C7 80000000 00000000 00000000 00000000


  ------------

    BCC

    IV is
                        00000000 00000000 00000000 00000000


    IV || S is
                                           00000000 00000000
      00000000 00000000 00000028 00000028 A0A1A2A3 A4A5A6A7
      A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
      C0C1C2C3 C4C5C6C7 80000000 00000000 00000000 00000000


  temp is
                        0DEF5001 1B1229C8 3DD880BE E398BDD8


  ------------

    BCC

    IV is
                        00000001 00000000 00000000 00000000


    IV || S is
                                           00000001 00000000
      00000000 00000000 00000028 00000028 A0A1A2A3 A4A5A6A7
      A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
```

```
    C0C1C2C3 C4C5C6C7 80000000 00000000 00000000 00000000


temp is
                                          0DEF5001 1B1229C8
    3DD880BE E398BDD8 61E3855F 743C9876 6CCEDC9B 90C1461E


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                                          00000002 00000000
    00000000 00000000 00000028 00000028 A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
    C0C1C2C3 C4C5C6C7 80000000 00000000 00000000 00000000


temp is
    0DEF5001 1B1229C8 3DD880BE E398BDD8 61E3855F 743C9876
    6CCEDC9B 90C1461E 92B6D6BA 30B91657 85E11146 2B2050F1


------------

Key is
    0DEF5001 1B1229C8 3DD880BE E398BDD8 61E3855F 743C9876


X is
                      6CCEDC9B 90C1461E 92B6D6BA 30B91657


------------

  BlockEncrypt

  Key is
    0DEF5001 1B1229C8 3DD880BE E398BDD8 61E3855F 743C9876
```

```
  X is
                      6CCEDC9B 90C1461E 92B6D6BA 30B91657


  X = BlockEncrypt(Key, X) is
                      1F2069F0 C00F3158 44CF0216 2913FC35


  temp is
                      1F2069F0 C00F3158 44CF0216 2913FC35


------------

  BlockEncrypt

  Key is
    0DEF5001 1B1229C8 3DD880BE E398BDD8 61E3855F 743C9876


  X is
                      1F2069F0 C00F3158 44CF0216 2913FC35


  X = BlockEncrypt(Key, X) is
                      F485B9DC 9EFDA069 E47E7C8D 674FECE1


  temp is
                                          1F2069F0 C00F3158
    44CF0216 2913FC35 F485B9DC 9EFDA069 E47E7C8D 674FECE1


------------

  BlockEncrypt

  Key is
    0DEF5001 1B1229C8 3DD880BE E398BDD8 61E3855F 743C9876


  X is
                      F485B9DC 9EFDA069 E47E7C8D 674FECE1


  X = BlockEncrypt(Key, X) is
```

```
                        3AB17BE9 025A1ACE F7E2A934 A3DDFD0B


      temp is
        1F2069F0 C00F3158 44CF0216 2913FC35 F485B9DC 9EFDA069
        E47E7C8D 674FECE1 3AB17BE9 025A1ACE F7E2A934 A3DDFD0B


      requested_bits is
                        1F2069F0 C00F3158 44CF0216 2913FC35
        F485B9DC 9EFDA069 E47E7C8D 674FECE1 3AB17BE9 025A1ACE


---------------------------

  Update

    provided_data is
                        1F2069F0 C00F3158 44CF0216 2913FC35
        F485B9DC 9EFDA069 E47E7C8D 674FECE1 3AB17BE9 025A1ACE


    ------------

      While loop

      Key is
        7C4AFCAF 34A3BFD1 200EA4FA DF8C32EE D1395594 B25F171C


      V is
                        0A8F6B2C 7E1FDE58 758A0EEA 303F2560


      output_block is
                        8494CE15 4602C729 EC414D3A 6A177D89


      temp is
                        8494CE15 4602C729 EC414D3A 6A177D89


    ------------

      While loop
```

```
  Key is
    7C4AFCAF 34A3BFD1 200EA4FA DF8C32EE D1395594 B25F171C


  V is
                      0A8F6B2C 7E1FDE58 758A0EEA 303F2561


  output_block is
                      0CDD1884 9A3CE775 6D0AE053 FF341BEB


  temp is
                                        8494CE15 4602C729
    EC414D3A 6A177D89 0CDD1884 9A3CE775 6D0AE053 FF341BEB


------------

  While loop

  Key is
    7C4AFCAF 34A3BFD1 200EA4FA DF8C32EE D1395594 B25F171C


  V is
                      0A8F6B2C 7E1FDE58 758A0EEA 303F2562


  output_block is
                      8DFBC57C 8F8C72CA 81E88545 88E0EE64


  temp is
    8494CE15 4602C729 EC414D3A 6A177D89 0CDD1884 9A3CE775
    6D0AE053 FF341BEB 8DFBC57C 8F8C72CA 81E88545 88E0EE64


temp XOR provided_data is
                      9BB4A7E5 860DF671 A88E4F2C 430481BC
    F858A158 04C1471C 89749CDE 987BF70A B74ABE95 8DD66804


Key is
    9BB4A7E5 860DF671 A88E4F2C 430481BC F858A158 04C1471C
```

```
    V is
                          89749CDE 987BF70A B74ABE95 8DD66804


---------------------------

  Update

    provided_data is
                          1F2069F0 C00F3158 44CF0216 2913FC35
        F485B9DC 9EFDA069 E47E7C8D 674FECE1 3AB17BE9 025A1ACE


    ------------

      While loop

      Key is
        9BB4A7E5 860DF671 A88E4F2C 430481BC F858A158 04C1471C


      V is
                          89749CDE 987BF70A B74ABE95 8DD66807


      output_block is
                          D05FC7BA 4F2B0E54 F0C3387A 1D51F568


      temp is
                          D05FC7BA 4F2B0E54 F0C3387A 1D51F568


    ------------

      While loop

      Key is
        9BB4A7E5 860DF671 A88E4F2C 430481BC F858A158 04C1471C


      V is
                          89749CDE 987BF70A B74ABE95 8DD66808
```

```
      output_block is
                          CB8871EC 046141F1 135D52C7 27DBB8F3


      temp is
                                               D05FC7BA 4F2B0E54
        F0C3387A 1D51F568 CB8871EC 046141F1 135D52C7 27DBB8F3


    ------------

      While loop

      Key is
        9BB4A7E5 860DF671 A88E4F2C 430481BC F858A158 04C1471C


      V is
                          89749CDE 987BF70A B74ABE95 8DD66809


      output_block is
                          6344C16B 719DEC7B 32A06AF0 44E269C7


      temp is
        D05FC7BA 4F2B0E54 F0C3387A 1D51F568 CB8871EC 046141F1
        135D52C7 27DBB8F3 6344C16B 719DEC7B 32A06AF0 44E269C7


    temp XOR provided_data is
                          CF7FAE4A 8F243F0C B40C3A6C 3442095D
        3F0DC830 9A9CE198 F7232E4A 40945412 59F5BA82 73C7F6B5


    Key is
        CF7FAE4A 8F243F0C B40C3A6C 3442095D 3F0DC830 9A9CE198


    V is
                          F7232E4A 40945412 59F5BA82 73C7F6B5


rnd_val is
                                               D2892F04 52967041
        4F098DA2 6684CB1E 9460F3A6 ED58BFC8 383A300B DAF284AD
```

```
################################################################

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    Nonce =
                                   20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    nonce is
                                   20212223 24252627 28292A2B
```

```
    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                                                            00010203
        04050607 08090A0B 0C0D0E0F 10111213 14151617 18191A1B
        1C1D1E1F 20212223 24252627 20212223 24252627 28292A2B


    number_of_bits_to_return = 320

    S is
                          00000034 00000028 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 20212223 24252627 28292A2B 80000000


    ------------

      BCC

      IV is
                          00000000 00000000 00000000 00000000


      IV || S is
                                                00000000 00000000
        00000000 00000000 00000034 00000028 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 20212223 24252627 28292A2B 80000000


    temp is
                          2D64B3D8 692984AD B6FBBA41 F69E74E1


    ------------

      BCC
```

```
  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
                                           00000001 00000000
    00000000 00000000 00000034 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 80000000


temp is
                                           2D64B3D8 692984AD
    B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E 66616F2E 9F91BC31


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                                           00000002 00000000
    00000000 00000000 00000034 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 80000000


temp is
    2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E
    66616F2E 9F91BC31 C6ADE98F EB96A83C A6F71BF5 BCE6944D


------------

Key is
    2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E


X is
                      66616F2E 9F91BC31 C6ADE98F EB96A83C
```

```
------------

  BlockEncrypt

  Key is
    2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E


  X is
                       66616F2E 9F91BC31 C6ADE98F EB96A83C


  X = BlockEncrypt(Key, X) is
                       45EBC7A3 4CB5BFDB A58CBFCC A756DDCB


  temp is
                       45EBC7A3 4CB5BFDB A58CBFCC A756DDCB


------------

  BlockEncrypt

  Key is
    2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E


  X is
                       45EBC7A3 4CB5BFDB A58CBFCC A756DDCB


  X = BlockEncrypt(Key, X) is
                       7150F160 187803C2 0380FB02 636C8E59


  temp is
                                          45EBC7A3 4CB5BFDB
    A58CBFCC A756DDCB 7150F160 187803C2 0380FB02 636C8E59


------------

  BlockEncrypt

  Key is
```

```
      2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E


    X is
                         7150F160 187803C2 0380FB02 636C8E59


    X = BlockEncrypt(Key, X) is
                         B1A94E9C C2360559 9C002E3A 221F5C21


    temp is
      45EBC7A3 4CB5BFDB A58CBFCC A756DDCB 7150F160 187803C2
      0380FB02 636C8E59 B1A94E9C C2360559 9C002E3A 221F5C21


    requested_bits is
                         45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
      7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559


  seed_material is
                         45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
      7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559


---------------------------

  Update

    provided_data is
                         45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
      7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559


    ------------

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                         00000000 00000000 00000000 00000001
```

```
  output_block is
                      CD33B28A C773F74B A00ED1F3 12572435


  temp is
                      CD33B28A C773F74B A00ED1F3 12572435


------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000002


  output_block is
                      98E7247C 07F0FE41 1C267E43 84B0F600


  temp is
                                        CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000003


  output_block is
                      2A3493E6 6235EE67 DEECCD2F 3B393BD8
```

```
      temp is
        CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
        1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8


    temp XOR provided_data is
                          88D87529 8BC64890 05826E3F B501F9FE
        E9B7D51C 1F88FD83 1FA68541 E7DC7859 9B9DDD7A A003EB3E


    Key is
        88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83


    V is
                          1FA68541 E7DC7859 9B9DDD7A A003EB3E


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

CTR_DRBG_Reseed

    entropy_input is
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    additional_input is  <empty>

--------------------------

  Block_Cipher_df
```

```
input_str is
                      80818283 84858687 88898A8B 8C8D8E8F
    90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


number_of_bits_to_return = 320

S is
                      00000028 00000028 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 80000000 00000000 00000000 00000000


------------

  BCC

  IV is
                      00000000 00000000 00000000 00000000


  IV || S is
                                        00000000 00000000
    00000000 00000000 00000028 00000028 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 80000000 00000000 00000000 00000000


temp is
                      D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD


------------

  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
                                        00000001 00000000
    00000000 00000000 00000028 00000028 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 80000000 00000000 00000000 00000000
```

```
temp is
                                          D4DC3DD9 64EB0CA9
    AFB81ED4 D728EACD D598A470 CD085CAD 313F0704 00084980


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                                          00000002 00000000
    00000000 00000000 00000028 00000028 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 80000000 00000000 00000000 00000000


temp is
    D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD D598A470 CD085CAD
    313F0704 00084980 E8128432 2968C4EB 2EA63668 13E2E7E3


------------

Key is
    D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD D598A470 CD085CAD


X is
                      313F0704 00084980 E8128432 2968C4EB


------------

  BlockEncrypt

  Key is
    D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD D598A470 CD085CAD


  X is
                      313F0704 00084980 E8128432 2968C4EB
```

```
  X = BlockEncrypt(Key, X) is
                      ECE25874 66228E78 6B45F5AA E1E7407B


  temp is
                      ECE25874 66228E78 6B45F5AA E1E7407B


------------

  BlockEncrypt

  Key is
    D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD D598A470 CD085CAD


  X is
                      ECE25874 66228E78 6B45F5AA E1E7407B


  X = BlockEncrypt(Key, X) is
                      C500EB8B 6D8EAD20 9217569B C032FAF6


  temp is
                                          ECE25874 66228E78
    6B45F5AA E1E7407B C500EB8B 6D8EAD20 9217569B C032FAF6


------------

  BlockEncrypt

  Key is
    D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD D598A470 CD085CAD


  X is
                      C500EB8B 6D8EAD20 9217569B C032FAF6


  X = BlockEncrypt(Key, X) is
                      8DCC82DB 4927187D 79D87935 70CCFCBC
```

```
      temp is
        ECE25874 66228E78 6B45F5AA E1E7407B C500EB8B 6D8EAD20
        9217569B C032FAF6 8DCC82DB 4927187D 79D87935 70CCFCBC


      requested_bits is
                           ECE25874 66228E78 6B45F5AA E1E7407B
        C500EB8B 6D8EAD20 9217569B C032FAF6 8DCC82DB 4927187D


----------------------------

  Update

    provided_data is
                           ECE25874 66228E78 6B45F5AA E1E7407B
        C500EB8B 6D8EAD20 9217569B C032FAF6 8DCC82DB 4927187D


    ------------

      While loop

      Key is
        88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83


      V is
                           1FA68541 E7DC7859 9B9DDD7A A003EB3F


      output_block is
                           1A646BB1 D38BD2AE A30CF5C5 D812A624


      temp is
                           1A646BB1 D38BD2AE A30CF5C5 D812A624


    ------------

      While loop

      Key is
        88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83
```

```
  V is
                      1FA68541 E7DC7859 9B9DDD7A A003EB40


  output_block is
                      B50D3ECA 99E508B2 5B5448A8 B96C0F2E


  temp is
                                           1A646BB1 D38BD2AE
    A30CF5C5 D812A624 B50D3ECA 99E508B2 5B5448A8 B96C0F2E


------------

  While loop

  Key is
    88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83


  V is
                      1FA68541 E7DC7859 9B9DDD7A A003EB41


  output_block is
                      FC55C88D AFA06880 F2C73C08 1E8FA294


  temp is
    1A646BB1 D38BD2AE A30CF5C5 D812A624 B50D3ECA 99E508B2
    5B5448A8 B96C0F2E FC55C88D AFA06880 F2C73C08 1E8FA294


temp XOR provided_data is
                      F68633C5 B5A95CD6 C849006F 39F5E65F
    700DD541 F46BA592 C9431E33 795EF5D8 71994A56 E68770FD


Key is
    F68633C5 B5A95CD6 C849006F 39F5E65F 700DD541 F46BA592


V is
```

```
                          C9431E33 795EF5D8 71994A56 E68770FD

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
        F68633C5 B5A95CD6 C849006F 39F5E65F 700DD541 F46BA592


      V is
                          C9431E33 795EF5D8 71994A56 E6877100


      output_block is
                          C122A362 565F8A65 E4F497AF 6EBEB1F1


      temp is
                          C122A362 565F8A65 E4F497AF 6EBEB1F1


    ------------

      While loop

      Key is
        F68633C5 B5A95CD6 C849006F 39F5E65F 700DD541 F46BA592
```

```
  V is
                      C9431E33 795EF5D8 71994A56 E6877101


  output_block is
                      001B843D 50205A56 8F09BEAE A5FF5ECD


  temp is
                                        C122A362 565F8A65
    E4F497AF 6EBEB1F1 001B843D 50205A56 8F09BEAE A5FF5ECD


------------

  While loop

  Key is
    F68633C5 B5A95CD6 C849006F 39F5E65F 700DD541 F46BA592


  V is
                      C9431E33 795EF5D8 71994A56 E6877102


  output_block is
                      0D3723AF 116550F7 B0D762A6 354F8AC7


  temp is
    C122A362 565F8A65 E4F497AF 6EBEB1F1 001B843D 50205A56
    8F09BEAE A5FF5ECD 0D3723AF 116550F7 B0D762A6 354F8AC7


temp XOR provided_data is
                      C122A362 565F8A65 E4F497AF 6EBEB1F1
    001B843D 50205A56 8F09BEAE A5FF5ECD 0D3723AF 116550F7


Key is
    C122A362 565F8A65 E4F497AF 6EBEB1F1 001B843D 50205A56


V is
```

```
                          8F09BEAE A5FF5ECD 0D3723AF 116550F7


rnd_val is
                                                D1C68E36 9E5AE5CF
        B6564317 13DC972E 54B87DA6 326D0D49 D1C11653 70049FDB


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    additional_input is  <empty>

---------------------------

  Block_Cipher_df

    input_str is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    number_of_bits_to_return = 320

    S is
                          00000028 00000028 C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
```

```
    E0E1E2E3 E4E5E6E7 80000000 00000000 00000000 00000000


------------

  BCC

  IV is
                     00000000 00000000 00000000 00000000


  IV || S is
                                          00000000 00000000
    00000000 00000000 00000028 00000028 C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
    E0E1E2E3 E4E5E6E7 80000000 00000000 00000000 00000000


temp is
                     98316F8D C09A27EA 960FDB96 D22C96D3


------------

  BCC

  IV is
                     00000001 00000000 00000000 00000000


  IV || S is
                                          00000001 00000000
    00000000 00000000 00000028 00000028 C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
    E0E1E2E3 E4E5E6E7 80000000 00000000 00000000 00000000


temp is
                                          98316F8D C09A27EA
    960FDB96 D22C96D3 C95E08EF DAB3E081 BDA51061 F9619651


------------

  BCC
```

```
  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                                              00000002 00000000
    00000000 00000000 00000028 00000028 C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
    E0E1E2E3 E4E5E6E7 80000000 00000000 00000000 00000000


temp is
    98316F8D C09A27EA 960FDB96 D22C96D3 C95E08EF DAB3E081
    BDA51061 F9619651 191D1E83 B09E52F5 1D6A9C00 B4889F28


------------

Key is
    98316F8D C09A27EA 960FDB96 D22C96D3 C95E08EF DAB3E081


X is
                      BDA51061 F9619651 191D1E83 B09E52F5


------------

  BlockEncrypt

  Key is
    98316F8D C09A27EA 960FDB96 D22C96D3 C95E08EF DAB3E081


  X is
                      BDA51061 F9619651 191D1E83 B09E52F5


  X = BlockEncrypt(Key, X) is
                      60C2CB2F DB52737D 19692CF5 E74AC177


  temp is
                      60C2CB2F DB52737D 19692CF5 E74AC177
```

```
------------

  BlockEncrypt

  Key is
    98316F8D C09A27EA 960FDB96 D22C96D3 C95E08EF DAB3E081


  X is
                      60C2CB2F DB52737D 19692CF5 E74AC177


  X = BlockEncrypt(Key, X) is
                      F94540C2 F7FCE903 859505EA BF87DB61


  temp is
                                        60C2CB2F DB52737D
    19692CF5 E74AC177 F94540C2 F7FCE903 859505EA BF87DB61


------------

  BlockEncrypt

  Key is
    98316F8D C09A27EA 960FDB96 D22C96D3 C95E08EF DAB3E081


  X is
                      F94540C2 F7FCE903 859505EA BF87DB61


  X = BlockEncrypt(Key, X) is
                      9FA75BC1 074138FE 9811C2BC F2A688DF


  temp is
    60C2CB2F DB52737D 19692CF5 E74AC177 F94540C2 F7FCE903
    859505EA BF87DB61 9FA75BC1 074138FE 9811C2BC F2A688DF


  requested_bits is
                      60C2CB2F DB52737D 19692CF5 E74AC177
    F94540C2 F7FCE903 859505EA BF87DB61 9FA75BC1 074138FE
```

```
---------------------------

  Update

    provided_data is
                          60C2CB2F DB52737D 19692CF5 E74AC177
        F94540C2 F7FCE903 859505EA BF87DB61 9FA75BC1 074138FE


    ------------

      While loop

      Key is
        C122A362 565F8A65 E4F497AF 6EBEB1F1 001B843D 50205A56


      V is
                          8F09BEAE A5FF5ECD 0D3723AF 116550F8


      output_block is
                          F9D4CFFA 99A2A750 F2EDAD7E 802EEFCE


      temp is
                          F9D4CFFA 99A2A750 F2EDAD7E 802EEFCE


    ------------

      While loop

      Key is
        C122A362 565F8A65 E4F497AF 6EBEB1F1 001B843D 50205A56


      V is
                          8F09BEAE A5FF5ECD 0D3723AF 116550F9


      output_block is
                          392BBCB4 09BB6C04 74E28DA4 473F2CAF
```

```
      temp is
                                                F9D4CFFA 99A2A750
        F2EDAD7E 802EEFCE 392BBCB4 09BB6C04 74E28DA4 473F2CAF


    ------------

      While loop

      Key is
        C122A362 565F8A65 E4F497AF 6EBEB1F1 001B843D 50205A56


      V is
                           8F09BEAE A5FF5ECD 0D3723AF 116550FA


      output_block is
                           D2175CBF 4AA9238E B659F6F3 467B046A


      temp is
        F9D4CFFA 99A2A750 F2EDAD7E 802EEFCE 392BBCB4 09BB6C04
        74E28DA4 473F2CAF D2175CBF 4AA9238E B659F6F3 467B046A


    temp XOR provided_data is
                           991604D5 42F0D42D EB84818B 67642EB9
        C06EFC76 FE478507 F177884E F8B8F7CE 4DB0077E 4DE81B70


    Key is
        991604D5 42F0D42D EB84818B 67642EB9 C06EFC76 FE478507


    V is
                           F177884E F8B8F7CE 4DB0077E 4DE81B70


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>
```

```
---------------------------

  Update

    provided_data is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
        991604D5 42F0D42D EB84818B 67642EB9 C06EFC76 FE478507


      V is
                          F177884E F8B8F7CE 4DB0077E 4DE81B73


      output_block is
                          621A3370 C857E028 253B3C45 D1E67351


      temp is
                          621A3370 C857E028 253B3C45 D1E67351


    ------------

      While loop

      Key is
        991604D5 42F0D42D EB84818B 67642EB9 C06EFC76 FE478507


      V is
                          F177884E F8B8F7CE 4DB0077E 4DE81B74


      output_block is
                          FA2EC31E DC76F7FF 6BA1806A F804F591
```

```
      temp is
                                              621A3370 C857E028
        253B3C45 D1E67351 FA2EC31E DC76F7FF 6BA1806A F804F591


    ------------

      While loop

      Key is
        991604D5 42F0D42D EB84818B 67642EB9 C06EFC76 FE478507


      V is
                           F177884E F8B8F7CE 4DB0077E 4DE81B75


      output_block is
                           AFC28095 D1B1505A 119E138B 76A9400A


      temp is
        621A3370 C857E028 253B3C45 D1E67351 FA2EC31E DC76F7FF
        6BA1806A F804F591 AFC28095 D1B1505A 119E138B 76A9400A


    temp XOR provided_data is
                           621A3370 C857E028 253B3C45 D1E67351
        FA2EC31E DC76F7FF 6BA1806A F804F591 AFC28095 D1B1505A


    Key is
        621A3370 C857E028 253B3C45 D1E67351 FA2EC31E DC76F7FF


    V is
                           6BA1806A F804F591 AFC28095 D1B1505A


rnd_val is
                                              615A2637 1F46583E
        A33ED757 09D0EE55 5C62EC04 433648A7 C62FD43D 2764D52F


################################################################
```

```
CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    Nonce =
                                   20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput1 =
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


    AdditionalInput2 =
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


##############################################################

**************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
```

```
    nonce is
                                  20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                                                          00010203
        04050607 08090A0B 0C0D0E0F 10111213 14151617 18191A1B
        1C1D1E1F 20212223 24252627 20212223 24252627 28292A2B


    number_of_bits_to_return = 320

    S is
                          00000034 00000028 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 20212223 24252627 28292A2B 80000000


    ------------

      BCC

      IV is
                          00000000 00000000 00000000 00000000


      IV || S is
                                                 00000000 00000000
        00000000 00000000 00000034 00000028 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 20212223 24252627 28292A2B 80000000


    temp is
                          2D64B3D8 692984AD B6FBBA41 F69E74E1
```

```
------------

  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
                                           00000001 00000000
    00000000 00000000 00000034 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 80000000


temp is
                                           2D64B3D8 692984AD
    B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E 66616F2E 9F91BC31


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                                           00000002 00000000
    00000000 00000000 00000034 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 80000000


temp is
    2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E
    66616F2E 9F91BC31 C6ADE98F EB96A83C A6F71BF5 BCE6944D


------------

Key is
    2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E
```

```
X is
                    66616F2E 9F91BC31 C6ADE98F EB96A83C


------------

  BlockEncrypt

  Key is
    2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E


  X is
                    66616F2E 9F91BC31 C6ADE98F EB96A83C


  X = BlockEncrypt(Key, X) is
                    45EBC7A3 4CB5BFDB A58CBFCC A756DDCB


  temp is
                    45EBC7A3 4CB5BFDB A58CBFCC A756DDCB


------------

  BlockEncrypt

  Key is
    2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E


  X is
                    45EBC7A3 4CB5BFDB A58CBFCC A756DDCB


  X = BlockEncrypt(Key, X) is
                    7150F160 187803C2 0380FB02 636C8E59


  temp is
                                      45EBC7A3 4CB5BFDB
    A58CBFCC A756DDCB 7150F160 187803C2 0380FB02 636C8E59


------------
```

```
      BlockEncrypt

      Key is
        2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EEFF1E


      X is
                           7150F160 187803C2 0380FB02 636C8E59


      X = BlockEncrypt(Key, X) is
                           B1A94E9C C2360559 9C002E3A 221F5C21


      temp is
        45EBC7A3 4CB5BFDB A58CBFCC A756DDCB 7150F160 187803C2
        0380FB02 636C8E59 B1A94E9C C2360559 9C002E3A 221F5C21


      requested_bits is
                           45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
        7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559


    seed_material is
                           45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
        7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559


---------------------------

  Update

    provided_data is
                           45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
        7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559


    ------------

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000
```

```
  V is
                      00000000 00000000 00000000 00000001

  output_block is
                      CD33B28A C773F74B A00ED1F3 12572435

  temp is
                      CD33B28A C773F74B A00ED1F3 12572435

------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000002

  output_block is
                      98E7247C 07F0FE41 1C267E43 84B0F600

  temp is
                                        CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600

------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000003
```

```
      output_block is
                          2A3493E6 6235EE67 DEECCD2F 3B393BD8


      temp is
        CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
        1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8


    temp XOR provided_data is
                          88D87529 8BC64890 05826E3F B501F9FE
        E9B7D51C 1F88FD83 1FA68541 E7DC7859 9B9DDD7A A003EB3E


    Key is
        88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83


    V is
                          1FA68541 E7DC7859 9B9DDD7A A003EB3E


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


Generate FAILED: Reseed is required
*************************************************************

CTR_DRBG_Reseed

    entropy_input is
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
```

```
    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


---------------------------

  Block_Cipher_df

    input_str is
                                               80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
        A0A1A2A3 A4A5A6A7 60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


    number_of_bits_to_return = 320

    S is
        00000050 00000028 80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 80000000 00000000


    ------------

      BCC

      IV is
                          00000000 00000000 00000000 00000000


      IV || S is
                          00000000 00000000 00000000 00000000
        00000050 00000028 80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 80000000 00000000


    temp is
                          FA46944A 0BDBB5EF A60EFAFE B9574E97
```

```
------------

  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
                      00000001 00000000 00000000 00000000
    00000050 00000028 80818283 84858687 88898A8B 8C8D8E8F
    90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
    60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
    78797A7B 7C7D7E7F 80818283 84858687 80000000 00000000


temp is
                                        FA46944A 0BDBB5EF
    A60EFAFE B9574E97 A1E88E07 AFFCD4EC E8EB2D2C ED3E4283


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                      00000002 00000000 00000000 00000000
    00000050 00000028 80818283 84858687 88898A8B 8C8D8E8F
    90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
    60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
    78797A7B 7C7D7E7F 80818283 84858687 80000000 00000000


temp is
    FA46944A 0BDBB5EF A60EFAFE B9574E97 A1E88E07 AFFCD4EC
    E8EB2D2C ED3E4283 8D8520E1 65EB3BDE BFAABC51 C44420CE


------------

Key is
    FA46944A 0BDBB5EF A60EFAFE B9574E97 A1E88E07 AFFCD4EC
```

```
X is
                      E8EB2D2C ED3E4283 8D8520E1 65EB3BDE


------------

  BlockEncrypt

  Key is
    FA46944A 0BDBB5EF A60EFAFE B9574E97 A1E88E07 AFFCD4EC


  X is
                      E8EB2D2C ED3E4283 8D8520E1 65EB3BDE


  X = BlockEncrypt(Key, X) is
                      D6D201B9 33F0FA92 A953C84C B739185C


  temp is
                      D6D201B9 33F0FA92 A953C84C B739185C


------------

  BlockEncrypt

  Key is
    FA46944A 0BDBB5EF A60EFAFE B9574E97 A1E88E07 AFFCD4EC


  X is
                      D6D201B9 33F0FA92 A953C84C B739185C


  X = BlockEncrypt(Key, X) is
                      5F353217 EFC411AD 5CD15D92 B481BEEF


  temp is
                                        D6D201B9 33F0FA92
    A953C84C B739185C 5F353217 EFC411AD 5CD15D92 B481BEEF
```

```
    ------------

      BlockEncrypt

      Key is
        FA46944A 0BDBB5EF A60EFAFE B9574E97 A1E88E07 AFFCD4EC


      X is
                           5F353217 EFC411AD 5CD15D92 B481BEEF


      X = BlockEncrypt(Key, X) is
                           7BDD58F3 8FD4827B 7A57A0F1 55ED8D8E


      temp is
        D6D201B9 33F0FA92 A953C84C B739185C 5F353217 EFC411AD
        5CD15D92 B481BEEF 7BDD58F3 8FD4827B 7A57A0F1 55ED8D8E


      requested_bits is
                           D6D201B9 33F0FA92 A953C84C B739185C
        5F353217 EFC411AD 5CD15D92 B481BEEF 7BDD58F3 8FD4827B


---------------------------

  Update

    provided_data is
                           D6D201B9 33F0FA92 A953C84C B739185C
        5F353217 EFC411AD 5CD15D92 B481BEEF 7BDD58F3 8FD4827B


    ------------

      While loop

      Key is
        88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83


      V is
                           1FA68541 E7DC7859 9B9DDD7A A003EB3F
```

```
  output_block is
                      1A646BB1 D38BD2AE A30CF5C5 D812A624

  temp is
                      1A646BB1 D38BD2AE A30CF5C5 D812A624

------------

  While loop

  Key is
    88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83

  V is
                      1FA68541 E7DC7859 9B9DDD7A A003EB40

  output_block is
                      B50D3ECA 99E508B2 5B5448A8 B96C0F2E

  temp is
                                        1A646BB1 D38BD2AE
    A30CF5C5 D812A624 B50D3ECA 99E508B2 5B5448A8 B96C0F2E

------------

  While loop

  Key is
    88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83

  V is
                      1FA68541 E7DC7859 9B9DDD7A A003EB41

  output_block is
                      FC55C88D AFA06880 F2C73C08 1E8FA294
```

```
      temp is
        1A646BB1 D38BD2AE A30CF5C5 D812A624 B50D3ECA 99E508B2
        5B5448A8 B96C0F2E FC55C88D AFA06880 F2C73C08 1E8FA294


    temp XOR provided_data is
                         CCB66A08 E07B283C 0A5F3D89 6F2BBE78
        EA380CDD 7621191F 0785153A 0DEDB1C1 8788907E 2074EAFB


    Key is
        CCB66A08 E07B283C 0A5F3D89 6F2BBE78 EA380CDD 7621191F


    V is
                         0785153A 0DEDB1C1 8788907E 2074EAFB


****************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                         00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
        CCB66A08 E07B283C 0A5F3D89 6F2BBE78 EA380CDD 7621191F


      V is
                         0785153A 0DEDB1C1 8788907E 2074EAFE
```

```
  output_block is
                      30DDEC5F 10795E1A 725319A0 DBF33FE5

  temp is
                      30DDEC5F 10795E1A 725319A0 DBF33FE5

------------

  While loop

  Key is
    CCB66A08 E07B283C 0A5F3D89 6F2BBE78 EA380CDD 7621191F

  V is
                      0785153A 0DEDB1C1 8788907E 2074EAFF

  output_block is
                      88C0ADCB 131B96B1 66AB4857 3E84F77C

  temp is
                                        30DDEC5F 10795E1A
    725319A0 DBF33FE5 88C0ADCB 131B96B1 66AB4857 3E84F77C

------------

  While loop

  Key is
    CCB66A08 E07B283C 0A5F3D89 6F2BBE78 EA380CDD 7621191F

  V is
                      0785153A 0DEDB1C1 8788907E 2074EB00

  output_block is
                      34709B9D 03C5D50D 60F4BE8A C3A926E8
```

```
      temp is
        30DDEC5F 10795E1A 725319A0 DBF33FE5 88C0ADCB 131B96B1
        66AB4857 3E84F77C 34709B9D 03C5D50D 60F4BE8A C3A926E8


    temp XOR provided_data is
                          30DDEC5F 10795E1A 725319A0 DBF33FE5
        88C0ADCB 131B96B1 66AB4857 3E84F77C 34709B9D 03C5D50D


    Key is
        30DDEC5F 10795E1A 725319A0 DBF33FE5 88C0ADCB 131B96B1


    V is
                          66AB4857 3E84F77C 34709B9D 03C5D50D


rnd_val is
                                            85C9EBEB 01415602
        991037DC B4E75C58 FF1638B6 98519565 25BA9FD2 BAB2F5DC


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


Generate FAILED: Reseed is required
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
```

```
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    additional_input is
                             A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


----------------------------

  Block_Cipher_df

    input_str is
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
        E0E1E2E3 E4E5E6E7 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


    number_of_bits_to_return = 320

    S is
        00000050 00000028 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 80000000 00000000


    ------------

      BCC

      IV is
                             00000000 00000000 00000000 00000000


      IV || S is
                             00000000 00000000 00000000 00000000
        00000050 00000028 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 80000000 00000000


    temp is
                             E7ABCDD0 A6525584 7CEC9281 848F4138
```

```
------------

  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
                      00000001 00000000 00000000 00000000
    00000050 00000028 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
    D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
    B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 80000000 00000000


temp is
                                          E7ABCDD0 A6525584
    7CEC9281 848F4138 55A14C04 0528CE89 199791EC 6E93B3E6


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                      00000002 00000000 00000000 00000000
    00000050 00000028 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
    D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
    B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 80000000 00000000


temp is
    E7ABCDD0 A6525584 7CEC9281 848F4138 55A14C04 0528CE89
    199791EC 6E93B3E6 62B20794 F25B3684 1E0EBF28 4BD7EB51


------------
```

```
Key is
    E7ABCDD0 A6525584 7CEC9281 848F4138 55A14C04 0528CE89


X is
                     199791EC 6E93B3E6 62B20794 F25B3684


------------

  BlockEncrypt

  Key is
    E7ABCDD0 A6525584 7CEC9281 848F4138 55A14C04 0528CE89


  X is
                     199791EC 6E93B3E6 62B20794 F25B3684


  X = BlockEncrypt(Key, X) is
                     F1BF2700 8A0E046B 826E30EF E8E34AA7


  temp is
                     F1BF2700 8A0E046B 826E30EF E8E34AA7


------------

  BlockEncrypt

  Key is
    E7ABCDD0 A6525584 7CEC9281 848F4138 55A14C04 0528CE89


  X is
                     F1BF2700 8A0E046B 826E30EF E8E34AA7


  X = BlockEncrypt(Key, X) is
                     BA2F6BC3 8CCDDBF2 31973B03 F26077D0


  temp is
                                       F1BF2700 8A0E046B
```

826E30EF E8E34AA7 BA2F6BC3 8CCDDBF2 31973B03 F26077D0

BlockEncrypt

Key is
E7ABCDD0 A6525584 7CEC9281 848F4138 55A14C04 0528CE89

X is
BA2F6BC3 8CCDDBF2 31973B03 F26077D0

X = BlockEncrypt(Key, X) is
442C7DA9 71F60F2D E8F43156 CAC4AB30

temp is
F1BF2700 8A0E046B 826E30EF E8E34AA7 BA2F6BC3 8CCDDBF2
31973B03 F26077D0 442C7DA9 71F60F2D E8F43156 CAC4AB30

requested_bits is
F1BF2700 8A0E046B 826E30EF E8E34AA7
BA2F6BC3 8CCDDBF2 31973B03 F26077D0 442C7DA9 71F60F2D

Update

provided_data is
F1BF2700 8A0E046B 826E30EF E8E34AA7
BA2F6BC3 8CCDDBF2 31973B03 F26077D0 442C7DA9 71F60F2D

While loop

Key is
30DDEC5F 10795E1A 725319A0 DBF33FE5 88C0ADCB 131B96B1

```
  V is
                      66AB4857 3E84F77C 34709B9D 03C5D50E

  output_block is
                      C0C92B2B 9EA1D51B CB8E6E98 6D802515

  temp is
                      C0C92B2B 9EA1D51B CB8E6E98 6D802515

------------

  While loop

  Key is
    30DDEC5F 10795E1A 725319A0 DBF33FE5 88C0ADCB 131B96B1

  V is
                      66AB4857 3E84F77C 34709B9D 03C5D50F

  output_block is
                      CC0E6B41 8D60E816 8DCEFBF8 C5416257

  temp is
                                        C0C92B2B 9EA1D51B
    CB8E6E98 6D802515 CC0E6B41 8D60E816 8DCEFBF8 C5416257

------------

  While loop

  Key is
    30DDEC5F 10795E1A 725319A0 DBF33FE5 88C0ADCB 131B96B1

  V is
                      66AB4857 3E84F77C 34709B9D 03C5D510

  output_block is
```

```
                          13DE1FA1 45BC29D4 ED919153 5367F330


      temp is
        C0C92B2B 9EA1D51B CB8E6E98 6D802515 CC0E6B41 8D60E816
        8DCEFBF8 C5416257 13DE1FA1 45BC29D4 ED919153 5367F330


    temp XOR provided_data is
                          31760C2B 14AFD170 49E05E77 85636FB2
        76210082 01AD33E4 BC59C0FB 37211587 57F26208 344A26F9


    Key is
        31760C2B 14AFD170 49E05E77 85636FB2 76210082 01AD33E4


    V is
                          BC59C0FB 37211587 57F26208 344A26F9


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
        31760C2B 14AFD170 49E05E77 85636FB2 76210082 01AD33E4
```

```
  V is
                      BC59C0FB 37211587 57F26208 344A26FC

  output_block is
                      53F2BFC5 E663EA33 20A6EB96 DD4D07E0

  temp is
                      53F2BFC5 E663EA33 20A6EB96 DD4D07E0

------------

  While loop

  Key is
    31760C2B 14AFD170 49E05E77 85636FB2 76210082 01AD33E4

  V is
                      BC59C0FB 37211587 57F26208 344A26FD

  output_block is
                      D5E8B942 B093FDE7 6264FFB5 EE0E948F

  temp is
                                        53F2BFC5 E663EA33
    20A6EB96 DD4D07E0 D5E8B942 B093FDE7 6264FFB5 EE0E948F

------------

  While loop

  Key is
    31760C2B 14AFD170 49E05E77 85636FB2 76210082 01AD33E4

  V is
                      BC59C0FB 37211587 57F26208 344A26FE

  output_block is
```

```
                        A29DC07B 6BC4CC60 A32F4C28 E8ACAD8D


      temp is
        53F2BFC5 E663EA33 20A6EB96 DD4D07E0 D5E8B942 B093FDE7
        6264FFB5 EE0E948F A29DC07B 6BC4CC60 A32F4C28 E8ACAD8D


    temp XOR provided_data is
                        53F2BFC5 E663EA33 20A6EB96 DD4D07E0
        D5E8B942 B093FDE7 6264FFB5 EE0E948F A29DC07B 6BC4CC60


    Key is
        53F2BFC5 E663EA33 20A6EB96 DD4D07E0 D5E8B942 B093FDE7


    V is
                        6264FFB5 EE0E948F A29DC07B 6BC4CC60


rnd_val is
                                            52D60B92 95D030CD
        5DF0740F 6298F7FB 0BCE9363 56179511 4A3C3FAF 3782C843


###############################################################

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                        00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                        80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7
```

```
    Nonce =
                                    20212223 24252627 28292A2B


    PersonalizationString =
                            40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    AdditionalInput = <empty>

#################################################################

*****************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                            00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    nonce is
                                    20212223 24252627 28292A2B


    personal_str is
                            40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                 00010203 04050607 08090A0B 0C0D0E0F 10111213
        14151617 18191A1B 1C1D1E1F 20212223 24252627 20212223
        24252627 28292A2B 40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667
```

```
number_of_bits_to_return = 320

S is
                     0000005C 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 40414243
    44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
    5C5D5E5F 60616263 64656667 80000000 00000000 00000000


------------

  BCC

  IV is
                     00000000 00000000 00000000 00000000


  IV || S is
                                        00000000 00000000
    00000000 00000000 0000005C 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 40414243
    44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
    5C5D5E5F 60616263 64656667 80000000 00000000 00000000


temp is
                     883662C0 53AC837C 186A91D7 0C5398FA


------------

  BCC

  IV is
                     00000001 00000000 00000000 00000000


  IV || S is
                                        00000001 00000000
    00000000 00000000 0000005C 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 40414243
    44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
    5C5D5E5F 60616263 64656667 80000000 00000000 00000000
```

```
temp is
                                          883662C0 53AC837C
    186A91D7 0C5398FA 9028263E F8303EE6 F7658E84 1E8EDDB4


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                                          00000002 00000000
    00000000 00000000 0000005C 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 40414243
    44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
    5C5D5E5F 60616263 64656667 80000000 00000000 00000000


temp is
    883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6
    F7658E84 1E8EDDB4 BA630844 25877431 5143AC1F 156049EB


------------

Key is
    883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6


X is
                      F7658E84 1E8EDDB4 BA630844 25877431


------------

  BlockEncrypt

  Key is
    883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6
```

```
  X is
                      F7658E84 1E8EDDB4 BA630844 25877431


  X = BlockEncrypt(Key, X) is
                      AC49318E F0FA3331 F54CFB30 6C9B7B15


  temp is
                      AC49318E F0FA3331 F54CFB30 6C9B7B15


------------

  BlockEncrypt

  Key is
    883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6


  X is
                      AC49318E F0FA3331 F54CFB30 6C9B7B15


  X = BlockEncrypt(Key, X) is
                      9334B962 5E62F257 2431DA7D 0A5F7534


  temp is
                                        AC49318E F0FA3331
    F54CFB30 6C9B7B15 9334B962 5E62F257 2431DA7D 0A5F7534


------------

  BlockEncrypt

  Key is
    883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6


  X is
                      9334B962 5E62F257 2431DA7D 0A5F7534
```

```
      X = BlockEncrypt(Key, X) is
                          B22E0E89 FF0FF392 A7CECDBE 5A4E766F


      temp is
        AC49318E F0FA3331 F54CFB30 6C9B7B15 9334B962 5E62F257
        2431DA7D 0A5F7534 B22E0E89 FF0FF392 A7CECDBE 5A4E766F


      requested_bits is
                          AC49318E F0FA3331 F54CFB30 6C9B7B15
        9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392


    seed_material is
                          AC49318E F0FA3331 F54CFB30 6C9B7B15
        9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392


---------------------------

  Update

    provided_data is
                          AC49318E F0FA3331 F54CFB30 6C9B7B15
        9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392


    ------------

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                          00000000 00000000 00000000 00000001


      output_block is
                          CD33B28A C773F74B A00ED1F3 12572435


      temp is
                          CD33B28A C773F74B A00ED1F3 12572435
```

```
------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                       00000000 00000000 00000000 00000002


  output_block is
                       98E7247C 07F0FE41 1C267E43 84B0F600


  temp is
                                            CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                       00000000 00000000 00000000 00000003


  output_block is
                       2A3493E6 6235EE67 DEECCD2F 3B393BD8


  temp is
    CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
    1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8


temp XOR provided_data is
                       617A8304 3789C47A 55422AC3 7ECC5F20
```

```
        0BD39D1E 59920C16 3817A43E 8EEF8334 981A9D6F 9D3A1DF5


    Key is
        617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16


    V is
                         3817A43E 8EEF8334 981A9D6F 9D3A1DF5


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

CTR_DRBG_Reseed

    entropy_input is
                         80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    additional_input is  <empty>

---------------------------

  Block_Cipher_df

    input_str is
                         80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    number_of_bits_to_return = 320
```

```
S is
                    00000028 00000028 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 80000000 00000000 00000000 00000000


------------

  BCC

  IV is
                    00000000 00000000 00000000 00000000


  IV || S is
                                       00000000 00000000
    00000000 00000000 00000028 00000028 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 80000000 00000000 00000000 00000000


temp is
                    D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD


------------

  BCC

  IV is
                    00000001 00000000 00000000 00000000


  IV || S is
                                       00000001 00000000
    00000000 00000000 00000028 00000028 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 80000000 00000000 00000000 00000000


temp is
                                       D4DC3DD9 64EB0CA9
    AFB81ED4 D728EACD D598A470 CD085CAD 313F0704 00084980


------------
```

```
  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                                           00000002 00000000
    00000000 00000000 00000028 00000028 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 80000000 00000000 00000000 00000000


temp is
    D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD D598A470 CD085CAD
    313F0704 00084980 E8128432 2968C4EB 2EA63668 13E2E7E3


------------

Key is
    D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD D598A470 CD085CAD


X is
                      313F0704 00084980 E8128432 2968C4EB


------------

  BlockEncrypt

  Key is
    D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD D598A470 CD085CAD


  X is
                      313F0704 00084980 E8128432 2968C4EB


  X = BlockEncrypt(Key, X) is
                      ECE25874 66228E78 6B45F5AA E1E7407B


  temp is
```

```
                    ECE25874 66228E78 6B45F5AA E1E7407B


------------

  BlockEncrypt

  Key is
    D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD D598A470 CD085CAD


  X is
                    ECE25874 66228E78 6B45F5AA E1E7407B


  X = BlockEncrypt(Key, X) is
                    C500EB8B 6D8EAD20 9217569B C032FAF6


  temp is
                                      ECE25874 66228E78
    6B45F5AA E1E7407B C500EB8B 6D8EAD20 9217569B C032FAF6


------------

  BlockEncrypt

  Key is
    D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD D598A470 CD085CAD


  X is
                    C500EB8B 6D8EAD20 9217569B C032FAF6


  X = BlockEncrypt(Key, X) is
                    8DCC82DB 4927187D 79D87935 70CCFCBC


  temp is
    ECE25874 66228E78 6B45F5AA E1E7407B C500EB8B 6D8EAD20
    9217569B C032FAF6 8DCC82DB 4927187D 79D87935 70CCFCBC


  requested_bits is
```

```
                        ECE25874 66228E78 6B45F5AA E1E7407B
        C500EB8B 6D8EAD20 9217569B C032FAF6 8DCC82DB 4927187D


----------------------------

  Update

    provided_data is
                        ECE25874 66228E78 6B45F5AA E1E7407B
        C500EB8B 6D8EAD20 9217569B C032FAF6 8DCC82DB 4927187D


    ------------

      While loop

      Key is
        617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16


      V is
                        3817A43E 8EEF8334 981A9D6F 9D3A1DF6


      output_block is
                        E231244B 3235B085 C8160442 4357E852


      temp is
                        E231244B 3235B085 C8160442 4357E852


    ------------

      While loop

      Key is
        617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16


      V is
                        3817A43E 8EEF8334 981A9D6F 9D3A1DF7


      output_block is
```

```
                        01E3828B 5C455686 79A5555F 867AAC8C


      temp is
                                              E231244B 3235B085
        C8160442 4357E852 01E3828B 5C455686 79A5555F 867AAC8C


    ------------

      While loop

      Key is
        617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16


      V is
                        3817A43E 8EEF8334 981A9D6F 9D3A1DF8


      output_block is
                        6C0BA382 122A6E1E BEB51820 656D3D45


      temp is
        E231244B 3235B085 C8160442 4357E852 01E3828B 5C455686
        79A5555F 867AAC8C 6C0BA382 122A6E1E BEB51820 656D3D45


    temp XOR provided_data is
                        0ED37C3F 54173EFD A353F1E8 A2B0A829
        C4E36900 31CBFBA6 EBB203C4 4648567A E1C72159 5B0D7663


    Key is
        0ED37C3F 54173EFD A353F1E8 A2B0A829 C4E36900 31CBFBA6


    V is
                        EBB203C4 4648567A E1C72159 5B0D7663


**************************************************************

CTR_DRBG_Generate
```

```
  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
        0ED37C3F 54173EFD A353F1E8 A2B0A829 C4E36900 31CBFBA6


      V is
                          EBB203C4 4648567A E1C72159 5B0D7666


      output_block is
                          941C5910 4692AC61 74F5BD51 9BF44FAA


      temp is
                          941C5910 4692AC61 74F5BD51 9BF44FAA


    ------------

      While loop

      Key is
        0ED37C3F 54173EFD A353F1E8 A2B0A829 C4E36900 31CBFBA6


      V is
                          EBB203C4 4648567A E1C72159 5B0D7667


      output_block is
```

```
                        37677E3E BA575D06 97D13841 1E0E3088


      temp is
                                              941C5910 4692AC61
        74F5BD51 9BF44FAA 37677E3E BA575D06 97D13841 1E0E3088


    ------------

      While loop

      Key is
        0ED37C3F 54173EFD A353F1E8 A2B0A829 C4E36900 31CBFBA6


      V is
                        EBB203C4 4648567A E1C72159 5B0D7668


      output_block is
                        8FCDC0E7 22EE559B 7967A230 92EF728F


      temp is
        941C5910 4692AC61 74F5BD51 9BF44FAA 37677E3E BA575D06
        97D13841 1E0E3088 8FCDC0E7 22EE559B 7967A230 92EF728F


    temp XOR provided_data is
                        941C5910 4692AC61 74F5BD51 9BF44FAA
        37677E3E BA575D06 97D13841 1E0E3088 8FCDC0E7 22EE559B


    Key is
        941C5910 4692AC61 74F5BD51 9BF44FAA 37677E3E BA575D06


    V is
                        97D13841 1E0E3088 8FCDC0E7 22EE559B


rnd_val is
                                              F780D4A2 C25CF8EE
        7407D948 EC0B724A 4235D8B2 0E650813 92755CA7 912AD7C0
```

```
---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    additional_input is  <empty>

---------------------------

  Block_Cipher_df

    input_str is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    number_of_bits_to_return = 320

    S is
                          00000028 00000028 C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
        E0E1E2E3 E4E5E6E7 80000000 00000000 00000000 00000000


    ------------

      BCC
```

```
  IV is
                      00000000 00000000 00000000 00000000


  IV || S is
                                              00000000 00000000
    00000000 00000000 00000028 00000028 C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
    E0E1E2E3 E4E5E6E7 80000000 00000000 00000000 00000000


temp is
                      98316F8D C09A27EA 960FDB96 D22C96D3


------------

  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
                                              00000001 00000000
    00000000 00000000 00000028 00000028 C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
    E0E1E2E3 E4E5E6E7 80000000 00000000 00000000 00000000


temp is
                                              98316F8D C09A27EA
    960FDB96 D22C96D3 C95E08EF DAB3E081 BDA51061 F9619651


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                                              00000002 00000000
    00000000 00000000 00000028 00000028 C0C1C2C3 C4C5C6C7
```

```
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
    E0E1E2E3 E4E5E6E7 80000000 00000000 00000000 00000000


temp is
    98316F8D C09A27EA 960FDB96 D22C96D3 C95E08EF DAB3E081
    BDA51061 F9619651 191D1E83 B09E52F5 1D6A9C00 B4889F28


------------

Key is
    98316F8D C09A27EA 960FDB96 D22C96D3 C95E08EF DAB3E081


X is
                      BDA51061 F9619651 191D1E83 B09E52F5


------------

  BlockEncrypt

  Key is
    98316F8D C09A27EA 960FDB96 D22C96D3 C95E08EF DAB3E081


  X is
                      BDA51061 F9619651 191D1E83 B09E52F5


  X = BlockEncrypt(Key, X) is
                      60C2CB2F DB52737D 19692CF5 E74AC177


  temp is
                      60C2CB2F DB52737D 19692CF5 E74AC177


------------

  BlockEncrypt

  Key is
    98316F8D C09A27EA 960FDB96 D22C96D3 C95E08EF DAB3E081
```

```
      X is
                          60C2CB2F DB52737D 19692CF5 E74AC177


      X = BlockEncrypt(Key, X) is
                          F94540C2 F7FCE903 859505EA BF87DB61


      temp is
                                               60C2CB2F DB52737D
        19692CF5 E74AC177 F94540C2 F7FCE903 859505EA BF87DB61


    ------------

      BlockEncrypt

      Key is
        98316F8D C09A27EA 960FDB96 D22C96D3 C95E08EF DAB3E081


      X is
                          F94540C2 F7FCE903 859505EA BF87DB61


      X = BlockEncrypt(Key, X) is
                          9FA75BC1 074138FE 9811C2BC F2A688DF


      temp is
        60C2CB2F DB52737D 19692CF5 E74AC177 F94540C2 F7FCE903
        859505EA BF87DB61 9FA75BC1 074138FE 9811C2BC F2A688DF


      requested_bits is
                          60C2CB2F DB52737D 19692CF5 E74AC177
        F94540C2 F7FCE903 859505EA BF87DB61 9FA75BC1 074138FE


---------------------------

  Update

    provided_data is
                          60C2CB2F DB52737D 19692CF5 E74AC177
```

```
    F94540C2 F7FCE903 859505EA BF87DB61 9FA75BC1 074138FE


------------

  While loop

  Key is
    941C5910 4692AC61 74F5BD51 9BF44FAA 37677E3E BA575D06


  V is
                       97D13841 1E0E3088 8FCDC0E7 22EE559C


  output_block is
                       78F91B65 6FB3D42E C4B48E70 4F34BCE9


  temp is
                       78F91B65 6FB3D42E C4B48E70 4F34BCE9


------------

  While loop

  Key is
    941C5910 4692AC61 74F5BD51 9BF44FAA 37677E3E BA575D06


  V is
                       97D13841 1E0E3088 8FCDC0E7 22EE559D


  output_block is
                       10A6A43B D0D2A7AC 70C91188 E109F0C0


  temp is
                                         78F91B65 6FB3D42E
    C4B48E70 4F34BCE9 10A6A43B D0D2A7AC 70C91188 E109F0C0


------------
```

```
      While loop

      Key is
        941C5910 4692AC61 74F5BD51 9BF44FAA 37677E3E BA575D06


      V is
                           97D13841 1E0E3088 8FCDC0E7 22EE559E


      output_block is
                           D6093035 63CD146C C94F91E8 D38A18F7


      temp is
        78F91B65 6FB3D42E C4B48E70 4F34BCE9 10A6A43B D0D2A7AC
        70C91188 E109F0C0 D6093035 63CD146C C94F91E8 D38A18F7


    temp XOR provided_data is
                           183BD04A B4E1A753 DDDDA285 A87E7D9E
        E9E3E4F9 272E4EAF F55C1462 5E8E2BA1 49AE6BF4 648C2C92


    Key is
        183BD04A B4E1A753 DDDDA285 A87E7D9E E9E3E4F9 272E4EAF


    V is
                           F55C1462 5E8E2BA1 49AE6BF4 648C2C92


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                           00000000 00000000 00000000 00000000
```

```
    00000000 00000000 00000000 00000000 00000000 00000000


------------

  While loop

  Key is
    183BD04A B4E1A753 DDDDA285 A87E7D9E E9E3E4F9 272E4EAF


  V is
                       F55C1462 5E8E2BA1 49AE6BF4 648C2C95


  output_block is
                       2FFD9DF2 057D5F9F 704B48CE 890646ED


  temp is
                       2FFD9DF2 057D5F9F 704B48CE 890646ED


------------

  While loop

  Key is
    183BD04A B4E1A753 DDDDA285 A87E7D9E E9E3E4F9 272E4EAF


  V is
                       F55C1462 5E8E2BA1 49AE6BF4 648C2C96


  output_block is
                       BFEAB396 648A7FC4 CA995C6F DAC51E3E


  temp is
                                         2FFD9DF2 057D5F9F
    704B48CE 890646ED BFEAB396 648A7FC4 CA995C6F DAC51E3E


------------
```

```
      While loop

      Key is
        183BD04A B4E1A753 DDDDA285 A87E7D9E E9E3E4F9 272E4EAF


      V is
                           F55C1462 5E8E2BA1 49AE6BF4 648C2C97


      output_block is
                           0F6B301A C1AC316E 2E4CBA0D 04A47306


      temp is
        2FFD9DF2 057D5F9F 704B48CE 890646ED BFEAB396 648A7FC4
        CA995C6F DAC51E3E 0F6B301A C1AC316E 2E4CBA0D 04A47306


    temp XOR provided_data is
                           2FFD9DF2 057D5F9F 704B48CE 890646ED
        BFEAB396 648A7FC4 CA995C6F DAC51E3E 0F6B301A C1AC316E


    Key is
        2FFD9DF2 057D5F9F 704B48CE 890646ED BFEAB396 648A7FC4


    V is
                           CA995C6F DAC51E3E 0F6B301A C1AC316E


rnd_val is
                                               BA14617F 915BA964
        CB79276B DADC840C 14B631BB D1A59097 054FA6DF F863B238


################################################################

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                           00010203 04050607 08090A0B 0C0D0E0F
```

```
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    Nonce =
                                   20212223 24252627 28292A2B


    PersonalizationString =
                          40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    AdditionalInput1 =
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


    AdditionalInput2 =
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    nonce is
                                   20212223 24252627 28292A2B
```

```
    personal_str is
                          40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                 00010203 04050607 08090A0B 0C0D0E0F 10111213
        14151617 18191A1B 1C1D1E1F 20212223 24252627 20212223
        24252627 28292A2B 40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    number_of_bits_to_return = 320

    S is
                          0000005C 00000028 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 20212223 24252627 28292A2B 40414243
        44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
        5C5D5E5F 60616263 64656667 80000000 00000000 00000000


    ------------

      BCC

      IV is
                          00000000 00000000 00000000 00000000


      IV || S is
                                                 00000000 00000000
        00000000 00000000 0000005C 00000028 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 20212223 24252627 28292A2B 40414243
        44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
        5C5D5E5F 60616263 64656667 80000000 00000000 00000000
```

```
temp is
                    883662C0 53AC837C 186A91D7 0C5398FA


------------

  BCC

  IV is
                    00000001 00000000 00000000 00000000


  IV || S is
                                             00000001 00000000
    00000000 00000000 0000005C 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 40414243
    44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
    5C5D5E5F 60616263 64656667 80000000 00000000 00000000


temp is
                                             883662C0 53AC837C
    186A91D7 0C5398FA 9028263E F8303EE6 F7658E84 1E8EDDB4


------------

  BCC

  IV is
                    00000002 00000000 00000000 00000000


  IV || S is
                                             00000002 00000000
    00000000 00000000 0000005C 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 40414243
    44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
    5C5D5E5F 60616263 64656667 80000000 00000000 00000000


temp is
    883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6
    F7658E84 1E8EDDB4 BA630844 25877431 5143AC1F 156049EB
```

```
------------

Key is
    883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6


X is
                     F7658E84 1E8EDDB4 BA630844 25877431


------------

  BlockEncrypt

  Key is
    883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6


  X is
                     F7658E84 1E8EDDB4 BA630844 25877431


  X = BlockEncrypt(Key, X) is
                     AC49318E F0FA3331 F54CFB30 6C9B7B15


  temp is
                     AC49318E F0FA3331 F54CFB30 6C9B7B15


------------

  BlockEncrypt

  Key is
    883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6


  X is
                     AC49318E F0FA3331 F54CFB30 6C9B7B15


  X = BlockEncrypt(Key, X) is
                     9334B962 5E62F257 2431DA7D 0A5F7534
```

```
      temp is
                                              AC49318E F0FA3331
        F54CFB30 6C9B7B15 9334B962 5E62F257 2431DA7D 0A5F7534


    ------------

      BlockEncrypt

      Key is
        883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6


      X is
                           9334B962 5E62F257 2431DA7D 0A5F7534


      X = BlockEncrypt(Key, X) is
                           B22E0E89 FF0FF392 A7CECDBE 5A4E766F


      temp is
        AC49318E F0FA3331 F54CFB30 6C9B7B15 9334B962 5E62F257
        2431DA7D 0A5F7534 B22E0E89 FF0FF392 A7CECDBE 5A4E766F


      requested_bits is
                           AC49318E F0FA3331 F54CFB30 6C9B7B15
        9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392


    seed_material is
                           AC49318E F0FA3331 F54CFB30 6C9B7B15
        9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392


---------------------------

  Update

    provided_data is
                           AC49318E F0FA3331 F54CFB30 6C9B7B15
        9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392
```

```
------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                       00000000 00000000 00000000 00000001


  output_block is
                       CD33B28A C773F74B A00ED1F3 12572435


  temp is
                       CD33B28A C773F74B A00ED1F3 12572435


------------

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                       00000000 00000000 00000000 00000002


  output_block is
                       98E7247C 07F0FE41 1C267E43 84B0F600


  temp is
                                            CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


------------

  While loop
```

```
      Key is
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000003


      output_block is
                           2A3493E6 6235EE67 DEECCD2F 3B393BD8


      temp is
        CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
        1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8


    temp XOR provided_data is
                           617A8304 3789C47A 55422AC3 7ECC5F20
        0BD39D1E 59920C16 3817A43E 8EEF8334 981A9D6F 9D3A1DF5


    Key is
        617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16


    V is
                           3817A43E 8EEF8334 981A9D6F 9D3A1DF5


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                           60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


Generate FAILED: Reseed is required
```

```
**************************************************************

CTR_DRBG_Reseed

    entropy_input is
                           80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    additional_input is
                           60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


---------------------------

  Block_Cipher_df

    input_str is
                                                 80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
        A0A1A2A3 A4A5A6A7 60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


    number_of_bits_to_return = 320

    S is
        00000050 00000028 80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 80000000 00000000


    ------------

      BCC

      IV is
                           00000000 00000000 00000000 00000000


      IV || S is
                           00000000 00000000 00000000 00000000
        00000050 00000028 80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
```

```
    60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
    78797A7B 7C7D7E7F 80818283 84858687 80000000 00000000


temp is
                     FA46944A 0BDBB5EF A60EFAFE B9574E97


------------

  BCC

  IV is
                     00000001 00000000 00000000 00000000


  IV || S is
                     00000001 00000000 00000000 00000000
    00000050 00000028 80818283 84858687 88898A8B 8C8D8E8F
    90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
    60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
    78797A7B 7C7D7E7F 80818283 84858687 80000000 00000000


temp is
                                        FA46944A 0BDBB5EF
    A60EFAFE B9574E97 A1E88E07 AFFCD4EC E8EB2D2C ED3E4283


------------

  BCC

  IV is
                     00000002 00000000 00000000 00000000


  IV || S is
                     00000002 00000000 00000000 00000000
    00000050 00000028 80818283 84858687 88898A8B 8C8D8E8F
    90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
    60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
    78797A7B 7C7D7E7F 80818283 84858687 80000000 00000000


temp is
```

```
    FA46944A 0BDBB5EF A60EFAFE B9574E97 A1E88E07 AFFCD4EC
    E8EB2D2C ED3E4283 8D8520E1 65EB3BDE BFAABC51 C44420CE


------------

Key is
    FA46944A 0BDBB5EF A60EFAFE B9574E97 A1E88E07 AFFCD4EC


X is
                     E8EB2D2C ED3E4283 8D8520E1 65EB3BDE


------------

  BlockEncrypt

  Key is
    FA46944A 0BDBB5EF A60EFAFE B9574E97 A1E88E07 AFFCD4EC


  X is
                     E8EB2D2C ED3E4283 8D8520E1 65EB3BDE


  X = BlockEncrypt(Key, X) is
                     D6D201B9 33F0FA92 A953C84C B739185C


  temp is
                     D6D201B9 33F0FA92 A953C84C B739185C


------------

  BlockEncrypt

  Key is
    FA46944A 0BDBB5EF A60EFAFE B9574E97 A1E88E07 AFFCD4EC


  X is
                     D6D201B9 33F0FA92 A953C84C B739185C
```

```
      X = BlockEncrypt(Key, X) is
                          5F353217 EFC411AD 5CD15D92 B481BEEF


      temp is
                                               D6D201B9 33F0FA92
        A953C84C B739185C 5F353217 EFC411AD 5CD15D92 B481BEEF


    ------------

      BlockEncrypt

      Key is
        FA46944A 0BDBB5EF A60EFAFE B9574E97 A1E88E07 AFFCD4EC


      X is
                          5F353217 EFC411AD 5CD15D92 B481BEEF


      X = BlockEncrypt(Key, X) is
                          7BDD58F3 8FD4827B 7A57A0F1 55ED8D8E


      temp is
        D6D201B9 33F0FA92 A953C84C B739185C 5F353217 EFC411AD
        5CD15D92 B481BEEF 7BDD58F3 8FD4827B 7A57A0F1 55ED8D8E


      requested_bits is
                          D6D201B9 33F0FA92 A953C84C B739185C
        5F353217 EFC411AD 5CD15D92 B481BEEF 7BDD58F3 8FD4827B


---------------------------

  Update

    provided_data is
                          D6D201B9 33F0FA92 A953C84C B739185C
        5F353217 EFC411AD 5CD15D92 B481BEEF 7BDD58F3 8FD4827B


    ------------
```

```
  While loop

  Key is
    617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16


  V is
                      3817A43E 8EEF8334 981A9D6F 9D3A1DF6


  output_block is
                      E231244B 3235B085 C8160442 4357E852


  temp is
                      E231244B 3235B085 C8160442 4357E852


------------

  While loop

  Key is
    617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16


  V is
                      3817A43E 8EEF8334 981A9D6F 9D3A1DF7


  output_block is
                      01E3828B 5C455686 79A5555F 867AAC8C


  temp is
                                          E231244B 3235B085
    C8160442 4357E852 01E3828B 5C455686 79A5555F 867AAC8C


------------

  While loop

  Key is
    617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16
```

```
      V is
                          3817A43E 8EEF8334 981A9D6F 9D3A1DF8


      output_block is
                          6C0BA382 122A6E1E BEB51820 656D3D45


      temp is
        E231244B 3235B085 C8160442 4357E852 01E3828B 5C455686
        79A5555F 867AAC8C 6C0BA382 122A6E1E BEB51820 656D3D45


    temp XOR provided_data is
                          34E325F2 01C54A17 6145CC0E F46EF00E
        5ED6B09C B381472B 257408CD 32FB1263 17D6FB71 9DFEEC65


    Key is
        34E325F2 01C54A17 6145CC0E F46EF00E 5ED6B09C B381472B


    V is
                          257408CD 32FB1263 17D6FB71 9DFEEC65


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------
```

```
  While loop

  Key is
    34E325F2 01C54A17 6145CC0E F46EF00E 5ED6B09C B381472B


  V is
                      257408CD 32FB1263 17D6FB71 9DFEEC68


  output_block is
                      A8E263CA 208C8E9C 14A130E7 86501B95


  temp is
                      A8E263CA 208C8E9C 14A130E7 86501B95


------------

  While loop

  Key is
    34E325F2 01C54A17 6145CC0E F46EF00E 5ED6B09C B381472B


  V is
                      257408CD 32FB1263 17D6FB71 9DFEEC69


  output_block is
                      C8BFE1A5 73158D8E DBAA41D2 AEBD2648


  temp is
                                          A8E263CA 208C8E9C
    14A130E7 86501B95 C8BFE1A5 73158D8E DBAA41D2 AEBD2648


------------

  While loop

  Key is
    34E325F2 01C54A17 6145CC0E F46EF00E 5ED6B09C B381472B
```

```
      V is
                          257408CD 32FB1263 17D6FB71 9DFEEC6A


      output_block is
                          3FC73970 BB89187C 0A48CD51 23703346


      temp is
        A8E263CA 208C8E9C 14A130E7 86501B95 C8BFE1A5 73158D8E
        DBAA41D2 AEBD2648 3FC73970 BB89187C 0A48CD51 23703346


    temp XOR provided_data is
                          A8E263CA 208C8E9C 14A130E7 86501B95
        C8BFE1A5 73158D8E DBAA41D2 AEBD2648 3FC73970 BB89187C


    Key is
        A8E263CA 208C8E9C 14A130E7 86501B95 C8BFE1A5 73158D8E


    V is
                          DBAA41D2 AEBD2648 3FC73970 BB89187C


rnd_val is
                                             01AFE09F 7BA5D683
        8BCAB837 75F9C286 E6132674 06560F2C 069DB758 98DE5D3F


------------------------------------------------------------

Second call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7
```

```
Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


---------------------------

  Block_Cipher_df

    input_str is
                                             C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
        E0E1E2E3 E4E5E6E7 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


    number_of_bits_to_return = 320

    S is
        00000050 00000028 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 80000000 00000000


    ------------

      BCC

      IV is
                          00000000 00000000 00000000 00000000


      IV || S is
                          00000000 00000000 00000000 00000000
```

```
    00000050 00000028 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
    D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
    B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 80000000 00000000


temp is
                     E7ABCDD0 A6525584 7CEC9281 848F4138


------------

  BCC

  IV is
                     00000001 00000000 00000000 00000000


  IV || S is
                     00000001 00000000 00000000 00000000
    00000050 00000028 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
    D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
    B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 80000000 00000000


temp is
                                        E7ABCDD0 A6525584
    7CEC9281 848F4138 55A14C04 0528CE89 199791EC 6E93B3E6


------------

  BCC

  IV is
                     00000002 00000000 00000000 00000000


  IV || S is
                     00000002 00000000 00000000 00000000
    00000050 00000028 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
    D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
    B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 80000000 00000000
```

```
temp is
    E7ABCDD0 A6525584 7CEC9281 848F4138 55A14C04 0528CE89
    199791EC 6E93B3E6 62B20794 F25B3684 1E0EBF28 4BD7EB51


------------

Key is
    E7ABCDD0 A6525584 7CEC9281 848F4138 55A14C04 0528CE89


X is
                     199791EC 6E93B3E6 62B20794 F25B3684


------------

  BlockEncrypt

  Key is
    E7ABCDD0 A6525584 7CEC9281 848F4138 55A14C04 0528CE89


  X is
                     199791EC 6E93B3E6 62B20794 F25B3684


  X = BlockEncrypt(Key, X) is
                     F1BF2700 8A0E046B 826E30EF E8E34AA7


  temp is
                     F1BF2700 8A0E046B 826E30EF E8E34AA7


------------

  BlockEncrypt

  Key is
    E7ABCDD0 A6525584 7CEC9281 848F4138 55A14C04 0528CE89


  X is
                     F1BF2700 8A0E046B 826E30EF E8E34AA7
```

```
      X = BlockEncrypt(Key, X) is
                          BA2F6BC3 8CCDDBF2 31973B03 F26077D0


      temp is
                                               F1BF2700 8A0E046B
        826E30EF E8E34AA7 BA2F6BC3 8CCDDBF2 31973B03 F26077D0


    ------------

      BlockEncrypt

      Key is
        E7ABCDD0 A6525584 7CEC9281 848F4138 55A14C04 0528CE89


      X is
                          BA2F6BC3 8CCDDBF2 31973B03 F26077D0


      X = BlockEncrypt(Key, X) is
                          442C7DA9 71F60F2D E8F43156 CAC4AB30


      temp is
        F1BF2700 8A0E046B 826E30EF E8E34AA7 BA2F6BC3 8CCDDBF2
        31973B03 F26077D0 442C7DA9 71F60F2D E8F43156 CAC4AB30


      requested_bits is
                          F1BF2700 8A0E046B 826E30EF E8E34AA7
        BA2F6BC3 8CCDDBF2 31973B03 F26077D0 442C7DA9 71F60F2D


---------------------------

  Update

    provided_data is
                          F1BF2700 8A0E046B 826E30EF E8E34AA7
        BA2F6BC3 8CCDDBF2 31973B03 F26077D0 442C7DA9 71F60F2D
```

```
------------

  While loop

  Key is
    A8E263CA 208C8E9C 14A130E7 86501B95 C8BFE1A5 73158D8E


  V is
                       DBAA41D2 AEBD2648 3FC73970 BB89187D


  output_block is
                       42BFE34F 5E9BBD3A F3687CD7 1E272A79


  temp is
                       42BFE34F 5E9BBD3A F3687CD7 1E272A79


------------

  While loop

  Key is
    A8E263CA 208C8E9C 14A130E7 86501B95 C8BFE1A5 73158D8E


  V is
                       DBAA41D2 AEBD2648 3FC73970 BB89187E


  output_block is
                       0D1E7656 27674349 A90BCAA4 593E524A


  temp is
                                         42BFE34F 5E9BBD3A
    F3687CD7 1E272A79 0D1E7656 27674349 A90BCAA4 593E524A


------------

  While loop

  Key is
```

```
        A8E263CA 208C8E9C 14A130E7 86501B95 C8BFE1A5 73158D8E


      V is
                           DBAA41D2 AEBD2648 3FC73970 BB89187F


      output_block is
                           09EEBE39 A6D92E93 5BDDA9B4 85228F47


      temp is
        42BFE34F 5E9BBD3A F3687CD7 1E272A79 0D1E7656 27674349
        A90BCAA4 593E524A 09EEBE39 A6D92E93 5BDDA9B4 85228F47


    temp XOR provided_data is
                           B300C44F D495B951 71064C38 F6C460DE
        B7311D95 ABAA98BB 989CF1A7 AB5E259A 4DC2C390 D72F21BE


    Key is
        B300C44F D495B951 71064C38 F6C460DE B7311D95 ABAA98BB


    V is
                           989CF1A7 AB5E259A 4DC2C390 D72F21BE


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
                           00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
```

```
------------

  While loop

  Key is
    B300C44F D495B951 71064C38 F6C460DE B7311D95 ABAA98BB


  V is
                      989CF1A7 AB5E259A 4DC2C390 D72F21C1


  output_block is
                      DB8BD973 74F50B22 666645C0 BA1B793F


  temp is
                      DB8BD973 74F50B22 666645C0 BA1B793F


------------

  While loop

  Key is
    B300C44F D495B951 71064C38 F6C460DE B7311D95 ABAA98BB


  V is
                      989CF1A7 AB5E259A 4DC2C390 D72F21C2


  output_block is
                      E4CB777D 0C8A7763 32537E93 15B9A355


  temp is
                                          DB8BD973 74F50B22
    666645C0 BA1B793F E4CB777D 0C8A7763 32537E93 15B9A355


------------

  While loop

  Key is
```

```
        B300C44F D495B951 71064C38 F6C460DE B7311D95 ABAA98BB


      V is
                           989CF1A7 AB5E259A 4DC2C390 D72F21C3


      output_block is
                           6C7A241D 6EC6C460 218F1E3B 355A264B


      temp is
        DB8BD973 74F50B22 666645C0 BA1B793F E4CB777D 0C8A7763
        32537E93 15B9A355 6C7A241D 6EC6C460 218F1E3B 355A264B


    temp XOR provided_data is
                           DB8BD973 74F50B22 666645C0 BA1B793F
        E4CB777D 0C8A7763 32537E93 15B9A355 6C7A241D 6EC6C460


    Key is
        DB8BD973 74F50B22 666645C0 BA1B793F E4CB777D 0C8A7763


    V is
                           32537E93 15B9A355 6C7A241D 6EC6C460


rnd_val is
                                              28730443 3D9D7301
        8DB647F8 459775BD 4EB52AF0 85D764AF A52D1DEE D8DACCDD


################################################################

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
```

```
    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    nonce is
                          20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
        28292A2B 2C2D2E2F 20212223 24252627 28292A2B 2C2D2E2F
```

```
number_of_bits_to_return = 384

S is
                                          00000040 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000


------------

  BCC

  IV is
                      00000000 00000000 00000000 00000000


  IV || S is
    00000000 00000000 00000000 00000000 00000040 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000


temp is
                      4BC4520F E87668A3 A2CE3DCB 5F564BA9


------------

  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
    00000001 00000000 00000000 00000000 00000040 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000


temp is
                                          4BC4520F E87668A3
```

```
    A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
    00000002 00000000 00000000 00000000 00000040 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000


temp is
    4BC4520F E87668A3 A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB
    9C275423 0F4E6DC4 8283F162 52D8520F D651F481 64D42EC9


------------

Key is
                                        4BC4520F E87668A3
    A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4


X is
                      8283F162 52D8520F D651F481 64D42EC9


------------

  BlockEncrypt

  Key is
                                        4BC4520F E87668A3
    A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4


  X is
                      8283F162 52D8520F D651F481 64D42EC9
```

```
  X = BlockEncrypt(Key, X) is
                      DF1F3CA3 8349478C CDFE738A 222E0645


  temp is
                      DF1F3CA3 8349478C CDFE738A 222E0645


------------

  BlockEncrypt

  Key is
                                          4BC4520F E87668A3
    A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4


  X is
                      DF1F3CA3 8349478C CDFE738A 222E0645


  X = BlockEncrypt(Key, X) is
                      494008AD CEFBE237 13596A7E AE41BBCD


  temp is
                                          DF1F3CA3 8349478C
    CDFE738A 222E0645 494008AD CEFBE237 13596A7E AE41BBCD


------------

  BlockEncrypt

  Key is
                                          4BC4520F E87668A3
    A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4


  X is
                      494008AD CEFBE237 13596A7E AE41BBCD


  X = BlockEncrypt(Key, X) is
                      C66368D7 8DA21092 840E23C8 995CE6D2
```

```
      temp is
        DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
        13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2


      requested_bits is
        DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
        13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2


    seed_material is
        DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
        13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2


---------------------------

  Update

    provided_data is
        DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
        13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2


    ------------

      While loop

      Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001


      output_block is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


      temp is
                           530F8AFB C74536B9 A963B4F1 C4CB738B
```

```
------------

  While loop

  Key is
                                              00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000002


  output_block is
                      CEA7403D 4D606B6E 074EC5D3 BAF39D18


  temp is
                                              530F8AFB C74536B9
    A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18


------------

  While loop

  Key is
                                              00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000003


  output_block is
                      726003CA 37A62A74 D1A2F58E 7506358E


  temp is
    530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
    074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


temp XOR provided_data is
```

```
        8C10B658 440C7135 649DC77B E6E575CE 87E74890 839B8959
        1417AFAD 14B226D5 B4036B1D BA043AE6 55ACD646 EC5AD35C


    Key is
                                            8C10B658 440C7135
        649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5


    V is
                          B4036B1D BA043AE6 55ACD646 EC5AD35C


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                                            8C10B658 440C7135
        649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5


      V is
                          B4036B1D BA043AE6 55ACD646 EC5AD35F
```

```
  output_block is
                      68F2F51A 364601AF 9533C864 F25DA997

  temp is
                      68F2F51A 364601AF 9533C864 F25DA997

------------

  While loop

  Key is
                                          8C10B658 440C7135
    649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5

  V is
                      B4036B1D BA043AE6 55ACD646 EC5AD360

  output_block is
                      7D095ACE B5DE8DA2 333C4085 8D88DE5B

  temp is
                                          68F2F51A 364601AF
    9533C864 F25DA997 7D095ACE B5DE8DA2 333C4085 8D88DE5B

------------

  While loop

  Key is
                                          8C10B658 440C7135
    649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5

  V is
                      B4036B1D BA043AE6 55ACD646 EC5AD361

  output_block is
                      33B6B005 72CE4C19 9D0284FA 8BADA00B
```

```
      temp is
        68F2F51A 364601AF 9533C864 F25DA997 7D095ACE B5DE8DA2
        333C4085 8D88DE5B 33B6B005 72CE4C19 9D0284FA 8BADA00B


    temp XOR provided_data is
        68F2F51A 364601AF 9533C864 F25DA997 7D095ACE B5DE8DA2
        333C4085 8D88DE5B 33B6B005 72CE4C19 9D0284FA 8BADA00B


    Key is
                                           68F2F51A 364601AF
        9533C864 F25DA997 7D095ACE B5DE8DA2 333C4085 8D88DE5B


    V is
                          33B6B005 72CE4C19 9D0284FA 8BADA00B


rnd_val is
                                           E686DD55 F758FD91
        BA7CB726 FE0B573A 180AB674 39FFBDFE 5EC28FB3 7A16A53B


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
```

```
------------

  While loop

  Key is
                                          68F2F51A 364601AF
    9533C864 F25DA997 7D095ACE B5DE8DA2 333C4085 8D88DE5B


  V is
                      33B6B005 72CE4C19 9D0284FA 8BADA00E


  output_block is
                      54789912 FE730A2F 836836F4 DA7246F6


  temp is
                      54789912 FE730A2F 836836F4 DA7246F6


------------

  While loop

  Key is
                                          68F2F51A 364601AF
    9533C864 F25DA997 7D095ACE B5DE8DA2 333C4085 8D88DE5B


  V is
                      33B6B005 72CE4C19 9D0284FA 8BADA00F


  output_block is
                      C52195FF 4AD1D913 8E38D01E FB037FEF


  temp is
                                          54789912 FE730A2F
    836836F4 DA7246F6 C52195FF 4AD1D913 8E38D01E FB037FEF


------------
```

```
      While loop

      Key is
                                              68F2F51A 364601AF
        9533C864 F25DA997 7D095ACE B5DE8DA2 333C4085 8D88DE5B


      V is
                           33B6B005 72CE4C19 9D0284FA 8BADA010


      output_block is
                           659CE64A 4923FB20 CAFB265F 1004328E


      temp is
        54789912 FE730A2F 836836F4 DA7246F6 C52195FF 4AD1D913
        8E38D01E FB037FEF 659CE64A 4923FB20 CAFB265F 1004328E


    temp XOR provided_data is
        54789912 FE730A2F 836836F4 DA7246F6 C52195FF 4AD1D913
        8E38D01E FB037FEF 659CE64A 4923FB20 CAFB265F 1004328E


    Key is
                                              54789912 FE730A2F
        836836F4 DA7246F6 C52195FF 4AD1D913 8E38D01E FB037FEF


    V is
                           659CE64A 4923FB20 CAFB265F 1004328E


rnd_val is
                                              8DA6CC59 E703CED0
        7D58D96E 5B6D7836 C3259973 5B734F88 C1A73B53 C7A6D82E


###############################################################

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "NOT ENABLED"
```

```
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput1 =
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


    AdditionalInput2 =
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    nonce is
                          20212223 24252627 28292A2B 2C2D2E2F
```

```
    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
        28292A2B 2C2D2E2F 20212223 24252627 28292A2B 2C2D2E2F


    number_of_bits_to_return = 384

    S is
                                               00000040 00000030
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
        20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000


    ------------

      BCC

      IV is
                          00000000 00000000 00000000 00000000


      IV || S is
        00000000 00000000 00000000 00000000 00000040 00000030
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
        20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000


    temp is
                          4BC4520F E87668A3 A2CE3DCB 5F564BA9


    ------------

      BCC
```

```
  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
    00000001 00000000 00000000 00000000 00000040 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000


temp is
                                        4BC4520F E87668A3
    A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
    00000002 00000000 00000000 00000000 00000040 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000


temp is
    4BC4520F E87668A3 A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB
    9C275423 0F4E6DC4 8283F162 52D8520F D651F481 64D42EC9


------------

Key is
                                        4BC4520F E87668A3
    A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4


X is
                      8283F162 52D8520F D651F481 64D42EC9
```

```
------------

  BlockEncrypt

  Key is
                                          4BC4520F E87668A3
    A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4


  X is
                     8283F162 52D8520F D651F481 64D42EC9


  X = BlockEncrypt(Key, X) is
                     DF1F3CA3 8349478C CDFE738A 222E0645


  temp is
                     DF1F3CA3 8349478C CDFE738A 222E0645


------------

  BlockEncrypt

  Key is
                                          4BC4520F E87668A3
    A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4


  X is
                     DF1F3CA3 8349478C CDFE738A 222E0645


  X = BlockEncrypt(Key, X) is
                     494008AD CEFBE237 13596A7E AE41BBCD


  temp is
                                          DF1F3CA3 8349478C
    CDFE738A 222E0645 494008AD CEFBE237 13596A7E AE41BBCD


------------
```

```
      BlockEncrypt

      Key is
                                              4BC4520F E87668A3
        A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4


      X is
                          494008AD CEFBE237 13596A7E AE41BBCD


      X = BlockEncrypt(Key, X) is
                          C66368D7 8DA21092 840E23C8 995CE6D2


      temp is
        DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
        13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2


      requested_bits is
        DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
        13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2


    seed_material is
        DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
        13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2


---------------------------

  Update

    provided_data is
        DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
        13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2


    ------------

      While loop

      Key is
                                              00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
```

```
  V is
                      00000000 00000000 00000000 00000001

  output_block is
                      530F8AFB C74536B9 A963B4F1 C4CB738B

  temp is
                      530F8AFB C74536B9 A963B4F1 C4CB738B

------------

  While loop

  Key is
                                            00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000002

  output_block is
                      CEA7403D 4D606B6E 074EC5D3 BAF39D18

  temp is
                                            530F8AFB C74536B9
    A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18

------------

  While loop

  Key is
                                            00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000

  V is
```

```
                          00000000 00000000 00000000 00000003


      output_block is
                          726003CA 37A62A74 D1A2F58E 7506358E


      temp is
        530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
        074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


    temp XOR provided_data is
        8C10B658 440C7135 649DC77B E6E575CE 87E74890 839B8959
        1417AFAD 14B226D5 B4036B1D BA043AE6 55ACD646 EC5AD35C


    Key is
                                            8C10B658 440C7135
        649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5


    V is
                          B4036B1D BA043AE6 55ACD646 EC5AD35C


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


  additional_input <> NULL, process appropriately
---------------------------

  Block_Cipher_df
```

```
input_str is
    60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
    78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


number_of_bits_to_return = 384

S is
                     00000030 00000030 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000


------------

  BCC

  IV is
                     00000000 00000000 00000000 00000000


  IV || S is
                                        00000000 00000000
    00000000 00000000 00000030 00000030 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000


temp is
                     DE8D1951 762E5557 CFAE1170 EEF4B933


------------

  BCC

  IV is
                     00000001 00000000 00000000 00000000


  IV || S is
                                        00000001 00000000
    00000000 00000000 00000030 00000030 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000
```

```
temp is
                                        DE8D1951 762E5557
    CFAE1170 EEF4B933 F9C0BD35 6D5244B9 158CEE79 08C40855


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                                        00000002 00000000
    00000000 00000000 00000030 00000030 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000


temp is
    DE8D1951 762E5557 CFAE1170 EEF4B933 F9C0BD35 6D5244B9
    158CEE79 08C40855 6254BE89 B2960465 D4879231 3E993E48


------------

Key is
                                        DE8D1951 762E5557
    CFAE1170 EEF4B933 F9C0BD35 6D5244B9 158CEE79 08C40855


X is
                      6254BE89 B2960465 D4879231 3E993E48


------------

  BlockEncrypt

  Key is
                                        DE8D1951 762E5557
    CFAE1170 EEF4B933 F9C0BD35 6D5244B9 158CEE79 08C40855
```

```
  X is
                      6254BE89 B2960465 D4879231 3E993E48


  X = BlockEncrypt(Key, X) is
                      4D8C89E0 1B308B59 E99AE0AD 702902F8


  temp is
                      4D8C89E0 1B308B59 E99AE0AD 702902F8


------------

  BlockEncrypt

  Key is
                                        DE8D1951 762E5557
    CFAE1170 EEF4B933 F9C0BD35 6D5244B9 158CEE79 08C40855


  X is
                      4D8C89E0 1B308B59 E99AE0AD 702902F8


  X = BlockEncrypt(Key, X) is
                      249768D0 97B4C73B CCFCD763 CD5AC761


  temp is
                                        4D8C89E0 1B308B59
    E99AE0AD 702902F8 249768D0 97B4C73B CCFCD763 CD5AC761


------------

  BlockEncrypt

  Key is
                                        DE8D1951 762E5557
    CFAE1170 EEF4B933 F9C0BD35 6D5244B9 158CEE79 08C40855


  X is
                      249768D0 97B4C73B CCFCD763 CD5AC761
```

```
      X = BlockEncrypt(Key, X) is
                          9267624C 0952CA7B A8ACDFCC E2A669D5


      temp is
        4D8C89E0 1B308B59 E99AE0AD 702902F8 249768D0 97B4C73B
        CCFCD763 CD5AC761 9267624C 0952CA7B A8ACDFCC E2A669D5


      requested_bits is
        4D8C89E0 1B308B59 E99AE0AD 702902F8 249768D0 97B4C73B
        CCFCD763 CD5AC761 9267624C 0952CA7B A8ACDFCC E2A669D5


---------------------------

  Update

    provided_data is
        4D8C89E0 1B308B59 E99AE0AD 702902F8 249768D0 97B4C73B
        CCFCD763 CD5AC761 9267624C 0952CA7B A8ACDFCC E2A669D5


    ------------

      While loop

      Key is
                                              8C10B658 440C7135
        649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5


      V is
                          B4036B1D BA043AE6 55ACD646 EC5AD35D


      output_block is
                          E686DD55 F758FD91 BA7CB726 FE0B573A


      temp is
                          E686DD55 F758FD91 BA7CB726 FE0B573A


    ------------
```

```
  While loop

  Key is
                                          8C10B658 440C7135
    649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5


  V is
                      B4036B1D BA043AE6 55ACD646 EC5AD35E


  output_block is
                      180AB674 39FFBDFE 5EC28FB3 7A16A53B


  temp is
                                          E686DD55 F758FD91
    BA7CB726 FE0B573A 180AB674 39FFBDFE 5EC28FB3 7A16A53B


------------

  While loop

  Key is
                                          8C10B658 440C7135
    649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5


  V is
                      B4036B1D BA043AE6 55ACD646 EC5AD35F


  output_block is
                      68F2F51A 364601AF 9533C864 F25DA997


  temp is
    E686DD55 F758FD91 BA7CB726 FE0B573A 180AB674 39FFBDFE
    5EC28FB3 7A16A53B 68F2F51A 364601AF 9533C864 F25DA997


temp XOR provided_data is
    AB0A54B5 EC6876C8 53E6578B 8E2255C2 3C9DDEA4 AE4B7AC5
    923E58D0 B74C625A FA959756 3F14CBD4 3D9F17A8 10FBC042
```

```
    Key is
                                              AB0A54B5 EC6876C8
        53E6578B 8E2255C2 3C9DDEA4 AE4B7AC5 923E58D0 B74C625A


    V is
                         FA959756 3F14CBD4 3D9F17A8 10FBC042


---------------------------

  Update

    provided_data is
        4D8C89E0 1B308B59 E99AE0AD 702902F8 249768D0 97B4C73B
        CCFCD763 CD5AC761 9267624C 0952CA7B A8ACDFCC E2A669D5


    ------------

      While loop

      Key is
                                              AB0A54B5 EC6876C8
        53E6578B 8E2255C2 3C9DDEA4 AE4B7AC5 923E58D0 B74C625A


      V is
                         FA959756 3F14CBD4 3D9F17A8 10FBC045


      output_block is
                         C66418B2 D26BFCC0 74F6B220 09C389BE


      temp is
                         C66418B2 D26BFCC0 74F6B220 09C389BE


    ------------

      While loop

      Key is
```

```
                                          AB0A54B5 EC6876C8
    53E6578B 8E2255C2 3C9DDEA4 AE4B7AC5 923E58D0 B74C625A


  V is
                      FA959756 3F14CBD4 3D9F17A8 10FBC046


  output_block is
                      6A0A2310 DE0CCE9E 05AA0F03 C83D8AFF


  temp is
                                          C66418B2 D26BFCC0
    74F6B220 09C389BE 6A0A2310 DE0CCE9E 05AA0F03 C83D8AFF


------------

  While loop

  Key is
                                          AB0A54B5 EC6876C8
    53E6578B 8E2255C2 3C9DDEA4 AE4B7AC5 923E58D0 B74C625A


  V is
                      FA959756 3F14CBD4 3D9F17A8 10FBC047


  output_block is
                      4CA3EC53 574253AC E3F17918 B3B50877


  temp is
    C66418B2 D26BFCC0 74F6B220 09C389BE 6A0A2310 DE0CCE9E
    05AA0F03 C83D8AFF 4CA3EC53 574253AC E3F17918 B3B50877


temp XOR provided_data is
    8BE89152 C95B7799 9D6C528D 79EA8B46 4E9D4BC0 49B809A5
    C956D860 05674D9E DEC48E1F 5E1099D7 4B5DA6D4 511361A2


Key is
                                          8BE89152 C95B7799
```

```
        9D6C528D 79EA8B46 4E9D4BC0 49B809A5 C956D860 05674D9E


    V is
                           DEC48E1F 5E1099D7 4B5DA6D4 511361A2


rnd_val is
                                                 498D25F7 124327CD
        FEBAF7F0 1559AFF8 4813F609 74BA5BD8 96C0CD5F 88BA5E32


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


  additional_input <> NULL, process appropriately
---------------------------

  Block_Cipher_df

    input_str is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    number_of_bits_to_return = 384

    S is
                           00000030 00000030 A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000


    ------------
```

```
  BCC

  IV is
                      00000000 00000000 00000000 00000000


  IV || S is
                                              00000000 00000000
    00000000 00000000 00000030 00000030 A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000


temp is
                      BC61575C 5D4B8037 C9E380B9 3E376057


------------

  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
                                              00000001 00000000
    00000000 00000000 00000030 00000030 A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000


temp is
                                              BC61575C 5D4B8037
    C9E380B9 3E376057 2C0B3606 11252C52 85BDEC6C 567C9B5A


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000
```

```
  IV || S is
                                                00000002 00000000
    00000000 00000000 00000030 00000030 A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000


temp is
    BC61575C 5D4B8037 C9E380B9 3E376057 2C0B3606 11252C52
    85BDEC6C 567C9B5A F6259D1D 3848CC93 296E04B5 AD60A97F


------------

Key is
                                                BC61575C 5D4B8037
    C9E380B9 3E376057 2C0B3606 11252C52 85BDEC6C 567C9B5A


X is
                      F6259D1D 3848CC93 296E04B5 AD60A97F


------------

  BlockEncrypt

  Key is
                                                BC61575C 5D4B8037
    C9E380B9 3E376057 2C0B3606 11252C52 85BDEC6C 567C9B5A


  X is
                      F6259D1D 3848CC93 296E04B5 AD60A97F


  X = BlockEncrypt(Key, X) is
                      FBD01F35 7D143F63 0DC0E7F9 B48DAC71


  temp is
                      FBD01F35 7D143F63 0DC0E7F9 B48DAC71


------------
```

```
  BlockEncrypt

  Key is
                                          BC61575C 5D4B8037
    C9E380B9 3E376057 2C0B3606 11252C52 85BDEC6C 567C9B5A


  X is
                      FBD01F35 7D143F63 0DC0E7F9 B48DAC71


  X = BlockEncrypt(Key, X) is
                      440CD750 A626DDB6 7744FD19 DFA9D223


  temp is
                                          FBD01F35 7D143F63
    0DC0E7F9 B48DAC71 440CD750 A626DDB6 7744FD19 DFA9D223


------------

  BlockEncrypt

  Key is
                                          BC61575C 5D4B8037
    C9E380B9 3E376057 2C0B3606 11252C52 85BDEC6C 567C9B5A


  X is
                      440CD750 A626DDB6 7744FD19 DFA9D223


  X = BlockEncrypt(Key, X) is
                      FB21DE23 A5E64CE0 712FE847 AF490C39


  temp is
    FBD01F35 7D143F63 0DC0E7F9 B48DAC71 440CD750 A626DDB6
    7744FD19 DFA9D223 FB21DE23 A5E64CE0 712FE847 AF490C39


  requested_bits is
    FBD01F35 7D143F63 0DC0E7F9 B48DAC71 440CD750 A626DDB6
    7744FD19 DFA9D223 FB21DE23 A5E64CE0 712FE847 AF490C39
```

```
---------------------------

  Update

    provided_data is
        FBD01F35 7D143F63 0DC0E7F9 B48DAC71 440CD750 A626DDB6
        7744FD19 DFA9D223 FB21DE23 A5E64CE0 712FE847 AF490C39


    ------------

      While loop

      Key is
                                              8BE89152 C95B7799
        9D6C528D 79EA8B46 4E9D4BC0 49B809A5 C956D860 05674D9E


      V is
                           DEC48E1F 5E1099D7 4B5DA6D4 511361A3


      output_block is
                           DCA0E245 D8F0260D 9DDAB936 54755CA0


      temp is
                           DCA0E245 D8F0260D 9DDAB936 54755CA0


    ------------

      While loop

      Key is
                                              8BE89152 C95B7799
        9D6C528D 79EA8B46 4E9D4BC0 49B809A5 C956D860 05674D9E


      V is
                           DEC48E1F 5E1099D7 4B5DA6D4 511361A4


      output_block is
                           82EDC0CF 4B852CCE 877A1669 CD904C99
```

```
      temp is
                                              DCA0E245 D8F0260D
        9DDAB936 54755CA0 82EDC0CF 4B852CCE 877A1669 CD904C99


    ------------

      While loop

      Key is
                                              8BE89152 C95B7799
        9D6C528D 79EA8B46 4E9D4BC0 49B809A5 C956D860 05674D9E


      V is
                           DEC48E1F 5E1099D7 4B5DA6D4 511361A5


      output_block is
                           050B4A10 6405F911 1D600B2C AD9634CC


      temp is
        DCA0E245 D8F0260D 9DDAB936 54755CA0 82EDC0CF 4B852CCE
        877A1669 CD904C99 050B4A10 6405F911 1D600B2C AD9634CC


    temp XOR provided_data is
        2770FD70 A5E4196E 901A5ECF E0F8F0D1 C6E1179F EDA3F178
        F03EEB70 12399EBA FE2A9433 C1E3B5F1 6C4FE36B 02DF38F5


    Key is
                                              2770FD70 A5E4196E
        901A5ECF E0F8F0D1 C6E1179F EDA3F178 F03EEB70 12399EBA


    V is
                           FE2A9433 C1E3B5F1 6C4FE36B 02DF38F5


---------------------------

  Update
```

```
provided_data is
    FBD01F35 7D143F63 0DC0E7F9 B48DAC71 440CD750 A626DDB6
    7744FD19 DFA9D223 FB21DE23 A5E64CE0 712FE847 AF490C39


------------

  While loop

  Key is
                                        2770FD70 A5E4196E
    901A5ECF E0F8F0D1 C6E1179F EDA3F178 F03EEB70 12399EBA


  V is
                      FE2A9433 C1E3B5F1 6C4FE36B 02DF38F8


  output_block is
                      B0B737AF E2DDCB5C 9DBF368E 333CA850


  temp is
                      B0B737AF E2DDCB5C 9DBF368E 333CA850


------------

  While loop

  Key is
                                        2770FD70 A5E4196E
    901A5ECF E0F8F0D1 C6E1179F EDA3F178 F03EEB70 12399EBA


  V is
                      FE2A9433 C1E3B5F1 6C4FE36B 02DF38F9


  output_block is
                      8B3EB1AA 3B9DEBFA 903BD057 130CC025


  temp is
                                        B0B737AF E2DDCB5C
```

```
        9DBF368E 333CA850 8B3EB1AA 3B9DEBFA 903BD057 130CC025


    ------------

      While loop

      Key is
                                              2770FD70 A5E4196E
        901A5ECF E0F8F0D1 C6E1179F EDA3F178 F03EEB70 12399EBA


      V is
                           FE2A9433 C1E3B5F1 6C4FE36B 02DF38FA


      output_block is
                           524C2048 99A54528 C304AE71 1F5A57DF


      temp is
        B0B737AF E2DDCB5C 9DBF368E 333CA850 8B3EB1AA 3B9DEBFA
        903BD057 130CC025 524C2048 99A54528 C304AE71 1F5A57DF


    temp XOR provided_data is
        4B67289A 9FC9F43F 907FD177 87B10421 CF3266FA 9DBB364C
        E77F2D4E CCA51206 A96DFE6B 3C4309C8 B22B4636 B0135BE6


    Key is
                                              4B67289A 9FC9F43F
        907FD177 87B10421 CF3266FA 9DBB364C E77F2D4E CCA51206


    V is
                           A96DFE6B 3C4309C8 B22B4636 B0135BE6


rnd_val is
                                              81DAAF98 00C34FF0
        A104E51D 87E36F5B 17EB14B9 ABC5064C ADDA976E C4F77D34


##############################################################
```

```
CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    Nonce =
                            20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString =
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    AdditionalInput = <empty>

###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    nonce is
                            20212223 24252627 28292A2B 2C2D2E2F
```

```
    personal_str is
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                         00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
        28292A2B 2C2D2E2F 20212223 24252627 28292A2B 2C2D2E2F
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    number_of_bits_to_return = 384

    S is
                                               00000070 00000030
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
        20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
        60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000


    ------------

      BCC

      IV is
                         00000000 00000000 00000000 00000000


      IV || S is
        00000000 00000000 00000000 00000000 00000070 00000030
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
        20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
        60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000
```

```
temp is
                    8A0B0FB5 AA3FA8FD 4B9E8708 FACD2A08


------------

  BCC

  IV is
                    00000001 00000000 00000000 00000000


  IV || S is
    00000001 00000000 00000000 00000070 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
    48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
    60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000


temp is
                                        8A0B0FB5 AA3FA8FD
    4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718


------------

  BCC

  IV is
                    00000002 00000000 00000000 00000000


  IV || S is
    00000002 00000000 00000000 00000070 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
    48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
    60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000


temp is
    8A0B0FB5 AA3FA8FD 4B9E8708 FACD2A08 A13B6B8D A420CCBC
```

```
    43CF57C7 F3A7C718 2B4B429F EDFD2D2D 937CA4B4 71B86606


------------

Key is
                                        8A0B0FB5 AA3FA8FD
    4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718


X is
                     2B4B429F EDFD2D2D 937CA4B4 71B86606


------------

  BlockEncrypt

  Key is
                                        8A0B0FB5 AA3FA8FD
    4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718


  X is
                     2B4B429F EDFD2D2D 937CA4B4 71B86606


  X = BlockEncrypt(Key, X) is
                     31D82952 CBF4754A 1354F1A9 184841B4


  temp is
                     31D82952 CBF4754A 1354F1A9 184841B4


------------

  BlockEncrypt

  Key is
                                        8A0B0FB5 AA3FA8FD
    4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718


  X is
                     31D82952 CBF4754A 1354F1A9 184841B4
```

```
      X = BlockEncrypt(Key, X) is
                          C0812181 C179FD79 547E5367 AB8C9FA4


      temp is
                                               31D82952 CBF4754A
        1354F1A9 184841B4 C0812181 C179FD79 547E5367 AB8C9FA4


    ------------

      BlockEncrypt

      Key is
                                               8A0B0FB5 AA3FA8FD
        4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718


      X is
                          C0812181 C179FD79 547E5367 AB8C9FA4


      X = BlockEncrypt(Key, X) is
                          51223D14 E89B833F 62FC5EF8 0034A200


      temp is
        31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
        547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200


      requested_bits is
        31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
        547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200


    seed_material is
        31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
        547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200


---------------------------

  Update
```

```
provided_data is
    31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
    547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200


------------

  While loop

  Key is
                                          00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000001


  output_block is
                      530F8AFB C74536B9 A963B4F1 C4CB738B


  temp is
                      530F8AFB C74536B9 A963B4F1 C4CB738B


------------

  While loop

  Key is
                                          00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000002


  output_block is
                      CEA7403D 4D606B6E 074EC5D3 BAF39D18


  temp is
                                          530F8AFB C74536B9
```

```
        A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18


    ------------

      While loop

      Key is
                                              00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000003


      output_block is
                           726003CA 37A62A74 D1A2F58E 7506358E


      temp is
        530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
        074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


    temp XOR provided_data is
        62D7A3A9 0CB143F3 BA374558 DC83323F 0E2661BC 8C199617
        533096B4 117F02BC 23423EDE DF3DA94B B35EAB76 7532978E


    Key is
                                              62D7A3A9 0CB143F3
        BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC


    V is
                           23423EDE DF3DA94B B35EAB76 7532978E


------------------------------------------------------------

First call to Generate

************************************************************

CTR_DRBG_Generate
```

```
  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                                              62D7A3A9 0CB143F3
        BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC


      V is
                           23423EDE DF3DA94B B35EAB76 75329791


      output_block is
                           40A4397E 72F15782 98F8B8FB 54A8BAD1


      temp is
                           40A4397E 72F15782 98F8B8FB 54A8BAD1


    ------------

      While loop

      Key is
                                              62D7A3A9 0CB143F3
        BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC


      V is
                           23423EDE DF3DA94B B35EAB76 75329792
```

```
  output_block is
                      6526C8ED 91619BBF 3F3FEEA1 5FCB3AF5


  temp is
                                          40A4397E 72F15782
    98F8B8FB 54A8BAD1 6526C8ED 91619BBF 3F3FEEA1 5FCB3AF5


------------

  While loop

  Key is
                                          62D7A3A9 0CB143F3
    BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC


  V is
                      23423EDE DF3DA94B B35EAB76 75329793


  output_block is
                      E901923A FE17A74F 53B00B2F 3E5148B5


  temp is
    40A4397E 72F15782 98F8B8FB 54A8BAD1 6526C8ED 91619BBF
    3F3FEEA1 5FCB3AF5 E901923A FE17A74F 53B00B2F 3E5148B5


temp XOR provided_data is
    40A4397E 72F15782 98F8B8FB 54A8BAD1 6526C8ED 91619BBF
    3F3FEEA1 5FCB3AF5 E901923A FE17A74F 53B00B2F 3E5148B5


Key is
                                          40A4397E 72F15782
    98F8B8FB 54A8BAD1 6526C8ED 91619BBF 3F3FEEA1 5FCB3AF5


V is
                      E901923A FE17A74F 53B00B2F 3E5148B5
```

```
rnd_val is
                                                99BB703C DD820609
        903F1241 EA856E27 A54C2B75 EEA7775B 68093FCD 47B52E7F


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                                                40A4397E 72F15782
        98F8B8FB 54A8BAD1 6526C8ED 91619BBF 3F3FEEA1 5FCB3AF5


      V is
                           E901923A FE17A74F 53B00B2F 3E5148B8


      output_block is
                           97308A02 E0455DC1 73380181 249766FC


      temp is
                           97308A02 E0455DC1 73380181 249766FC
```

```
------------

  While loop

  Key is
                                          40A4397E 72F15782
    98F8B8FB 54A8BAD1 6526C8ED 91619BBF 3F3FEEA1 5FCB3AF5


  V is
                      E901923A FE17A74F 53B00B2F 3E5148B9


  output_block is
                      79B62BE6 8C41B2F2 748E07E0 E4D0AF8B


  temp is
                                          97308A02 E0455DC1
    73380181 249766FC 79B62BE6 8C41B2F2 748E07E0 E4D0AF8B


------------

  While loop

  Key is
                                          40A4397E 72F15782
    98F8B8FB 54A8BAD1 6526C8ED 91619BBF 3F3FEEA1 5FCB3AF5


  V is
                      E901923A FE17A74F 53B00B2F 3E5148BA


  output_block is
                      D0938581 D7C44751 1FF4F5C9 00972CE0


  temp is
    97308A02 E0455DC1 73380181 249766FC 79B62BE6 8C41B2F2
    748E07E0 E4D0AF8B D0938581 D7C44751 1FF4F5C9 00972CE0
```

```
    temp XOR provided_data is
        97308A02 E0455DC1 73380181 249766FC 79B62BE6 8C41B2F2
        748E07E0 E4D0AF8B D0938581 D7C44751 1FF4F5C9 00972CE0


    Key is
                                            97308A02 E0455DC1
        73380181 249766FC 79B62BE6 8C41B2F2 748E07E0 E4D0AF8B


    V is
                          D0938581 D7C44751 1FF4F5C9 00972CE0


rnd_val is
                                            BB2A0F5F 0CA6D306
        34BA6068 EB94AAE8 701437DB 7223A1B5 AFE87715 47DA3CEE


################################################################

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString =
```

```
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    AdditionalInput1 =
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


    AdditionalInput2 =
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    nonce is
                         20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                         00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
        28292A2B 2C2D2E2F 20212223 24252627 28292A2B 2C2D2E2F
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F
```

```
number_of_bits_to_return = 384

S is
                                          00000070 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
    48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
    60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000


------------

  BCC

  IV is
                      00000000 00000000 00000000 00000000


  IV || S is
    00000000 00000000 00000000 00000000 00000070 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
    48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
    60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000


temp is
                      8A0B0FB5 AA3FA8FD 4B9E8708 FACD2A08


------------

  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
    00000001 00000000 00000000 00000000 00000070 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
```

```
    20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
    48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
    60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000


temp is
                                        8A0B0FB5 AA3FA8FD
    4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
    00000002 00000000 00000000 00000000 00000070 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
    48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
    60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000


temp is
    8A0B0FB5 AA3FA8FD 4B9E8708 FACD2A08 A13B6B8D A420CCBC
    43CF57C7 F3A7C718 2B4B429F EDFD2D2D 937CA4B4 71B86606


------------

Key is
                                        8A0B0FB5 AA3FA8FD
    4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718


X is
                      2B4B429F EDFD2D2D 937CA4B4 71B86606


------------

  BlockEncrypt
```

```
  Key is
                                          8A0B0FB5 AA3FA8FD
    4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718


  X is
                      2B4B429F EDFD2D2D 937CA4B4 71B86606


  X = BlockEncrypt(Key, X) is
                      31D82952 CBF4754A 1354F1A9 184841B4


  temp is
                      31D82952 CBF4754A 1354F1A9 184841B4


------------

  BlockEncrypt

  Key is
                                          8A0B0FB5 AA3FA8FD
    4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718


  X is
                      31D82952 CBF4754A 1354F1A9 184841B4


  X = BlockEncrypt(Key, X) is
                      C0812181 C179FD79 547E5367 AB8C9FA4


  temp is
                                          31D82952 CBF4754A
    1354F1A9 184841B4 C0812181 C179FD79 547E5367 AB8C9FA4


------------

  BlockEncrypt

  Key is
                                          8A0B0FB5 AA3FA8FD
```

```
        4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718


      X is
                           C0812181 C179FD79 547E5367 AB8C9FA4


      X = BlockEncrypt(Key, X) is
                           51223D14 E89B833F 62FC5EF8 0034A200


      temp is
        31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
        547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200


      requested_bits is
        31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
        547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200


    seed_material is
        31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
        547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200


---------------------------

  Update

    provided_data is
        31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
        547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200


    ------------

      While loop

      Key is
                                               00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001
```

```
  output_block is
                      530F8AFB C74536B9 A963B4F1 C4CB738B

  temp is
                      530F8AFB C74536B9 A963B4F1 C4CB738B

------------

  While loop

  Key is
                                          00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000002

  output_block is
                      CEA7403D 4D606B6E 074EC5D3 BAF39D18

  temp is
                                          530F8AFB C74536B9
    A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18

------------

  While loop

  Key is
                                          00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000003

  output_block is
```

```
                          726003CA 37A62A74 D1A2F58E 7506358E


      temp is
        530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
        074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


    temp XOR provided_data is
        62D7A3A9 0CB143F3 BA374558 DC83323F 0E2661BC 8C199617
        533096B4 117F02BC 23423EDE DF3DA94B B35EAB76 7532978E


    Key is
                                            62D7A3A9 0CB143F3
        BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC


    V is
                          23423EDE DF3DA94B B35EAB76 7532978E


---------------------------------------------------------------

First call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


  additional_input <> NULL, process appropriately
---------------------------

  Block_Cipher_df

    input_str is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F
```

```
number_of_bits_to_return = 384

S is
                      00000030 00000030 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000


------------

  BCC

  IV is
                      00000000 00000000 00000000 00000000


  IV || S is
                                        00000000 00000000
    00000000 00000000 00000030 00000030 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000


temp is
                      DE8D1951 762E5557 CFAE1170 EEF4B933


------------

  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
                                        00000001 00000000
    00000000 00000000 00000030 00000030 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000


temp is
                                        DE8D1951 762E5557
    CFAE1170 EEF4B933 F9C0BD35 6D5244B9 158CEE79 08C40855
```

```
------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                                           00000002 00000000
    00000000 00000000 00000030 00000030 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000


temp is
    DE8D1951 762E5557 CFAE1170 EEF4B933 F9C0BD35 6D5244B9
    158CEE79 08C40855 6254BE89 B2960465 D4879231 3E993E48


------------

Key is
                                           DE8D1951 762E5557
    CFAE1170 EEF4B933 F9C0BD35 6D5244B9 158CEE79 08C40855


X is
                      6254BE89 B2960465 D4879231 3E993E48


------------

  BlockEncrypt

  Key is
                                           DE8D1951 762E5557
    CFAE1170 EEF4B933 F9C0BD35 6D5244B9 158CEE79 08C40855


  X is
                      6254BE89 B2960465 D4879231 3E993E48
```

```
  X = BlockEncrypt(Key, X) is
                      4D8C89E0 1B308B59 E99AE0AD 702902F8


  temp is
                      4D8C89E0 1B308B59 E99AE0AD 702902F8


------------

  BlockEncrypt

  Key is
                                        DE8D1951 762E5557
    CFAE1170 EEF4B933 F9C0BD35 6D5244B9 158CEE79 08C40855


  X is
                      4D8C89E0 1B308B59 E99AE0AD 702902F8


  X = BlockEncrypt(Key, X) is
                      249768D0 97B4C73B CCFCD763 CD5AC761


  temp is
                                        4D8C89E0 1B308B59
    E99AE0AD 702902F8 249768D0 97B4C73B CCFCD763 CD5AC761


------------

  BlockEncrypt

  Key is
                                        DE8D1951 762E5557
    CFAE1170 EEF4B933 F9C0BD35 6D5244B9 158CEE79 08C40855


  X is
                      249768D0 97B4C73B CCFCD763 CD5AC761


  X = BlockEncrypt(Key, X) is
                      9267624C 0952CA7B A8ACDFCC E2A669D5
```

```
      temp is
        4D8C89E0 1B308B59 E99AE0AD 702902F8 249768D0 97B4C73B
        CCFCD763 CD5AC761 9267624C 0952CA7B A8ACDFCC E2A669D5


      requested_bits is
        4D8C89E0 1B308B59 E99AE0AD 702902F8 249768D0 97B4C73B
        CCFCD763 CD5AC761 9267624C 0952CA7B A8ACDFCC E2A669D5


---------------------------

  Update

    provided_data is
        4D8C89E0 1B308B59 E99AE0AD 702902F8 249768D0 97B4C73B
        CCFCD763 CD5AC761 9267624C 0952CA7B A8ACDFCC E2A669D5


    ------------

      While loop

      Key is
                                              62D7A3A9 0CB143F3
        BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC


      V is
                           23423EDE DF3DA94B B35EAB76 7532978F


      output_block is
                           99BB703C DD820609 903F1241 EA856E27


      temp is
                           99BB703C DD820609 903F1241 EA856E27


    ------------

      While loop

      Key is
```

```
                                          62D7A3A9 0CB143F3
    BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC


  V is
                      23423EDE DF3DA94B B35EAB76 75329790


  output_block is
                      A54C2B75 EEA7775B 68093FCD 47B52E7F


  temp is
                                          99BB703C DD820609
    903F1241 EA856E27 A54C2B75 EEA7775B 68093FCD 47B52E7F


------------

  While loop

  Key is
                                          62D7A3A9 0CB143F3
    BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC


  V is
                      23423EDE DF3DA94B B35EAB76 75329791


  output_block is
                      40A4397E 72F15782 98F8B8FB 54A8BAD1


  temp is
    99BB703C DD820609 903F1241 EA856E27 A54C2B75 EEA7775B
    68093FCD 47B52E7F 40A4397E 72F15782 98F8B8FB 54A8BAD1


temp XOR provided_data is
    D437F9DC C6B28D50 79A5F2EC 9AAC6CDF 81DB43A5 7913B060
    A4F5E8AE 8AEFE91E D2C35B32 7BA39DF9 30546737 B60ED304


Key is
                                          D437F9DC C6B28D50
```

```
        79A5F2EC 9AAC6CDF 81DB43A5 7913B060 A4F5E8AE 8AEFE91E


    V is
                          D2C35B32 7BA39DF9 30546737 B60ED304


----------------------------

  Update

    provided_data is
        4D8C89E0 1B308B59 E99AE0AD 702902F8 249768D0 97B4C73B
        CCFCD763 CD5AC761 9267624C 0952CA7B A8ACDFCC E2A669D5


    ------------

      While loop

      Key is
                                            D437F9DC C6B28D50
        79A5F2EC 9AAC6CDF 81DB43A5 7913B060 A4F5E8AE 8AEFE91E


      V is
                          D2C35B32 7BA39DF9 30546737 B60ED307


      output_block is
                          94AC6E07 4D46CB0B 15C13188 C79E747F


      temp is
                          94AC6E07 4D46CB0B 15C13188 C79E747F


    ------------

      While loop

      Key is
                                            D437F9DC C6B28D50
        79A5F2EC 9AAC6CDF 81DB43A5 7913B060 A4F5E8AE 8AEFE91E
```

```
  V is
                      D2C35B32 7BA39DF9 30546737 B60ED308


  output_block is
                      26AE0E89 253EAFF2 A663DC6E 9347201D


  temp is
                                        94AC6E07 4D46CB0B
    15C13188 C79E747F 26AE0E89 253EAFF2 A663DC6E 9347201D


------------

  While loop

  Key is
                                        D437F9DC C6B28D50
    79A5F2EC 9AAC6CDF 81DB43A5 7913B060 A4F5E8AE 8AEFE91E


  V is
                      D2C35B32 7BA39DF9 30546737 B60ED309


  output_block is
                      67A42F29 2DFD819B 1A2BE5DD 18496C49


  temp is
    94AC6E07 4D46CB0B 15C13188 C79E747F 26AE0E89 253EAFF2
    A663DC6E 9347201D 67A42F29 2DFD819B 1A2BE5DD 18496C49


temp XOR provided_data is
    D920E7E7 56764052 FC5BD125 B7B77687 02396659 B28A68C9
    6A9F0B0D 5E1DE77C F5C34D65 24AF4BE0 B2873A11 FAEF059C


Key is
                                        D920E7E7 56764052
    FC5BD125 B7B77687 02396659 B28A68C9 6A9F0B0D 5E1DE77C


V is
```

```
                        F5C34D65 24AF4BE0 B2873A11 FAEF059C


rnd_val is
                                              47111E14 6562E9AA
        2FB2A1B0 95D37A81 65AF8FC7 CA611D63 2BE7D4C1 45C83900


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


  additional_input <> NULL, process appropriately
---------------------------

  Block_Cipher_df

    input_str is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    number_of_bits_to_return = 384

    S is
                        00000030 00000030 A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000


    ------------

      BCC

      IV is
```

```
                    00000000 00000000 00000000 00000000


  IV || S is
                                            00000000 00000000
    00000000 00000000 00000030 00000030 A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000


temp is
                    BC61575C 5D4B8037 C9E380B9 3E376057


------------

  BCC

  IV is
                    00000001 00000000 00000000 00000000


  IV || S is
                                            00000001 00000000
    00000000 00000000 00000030 00000030 A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000


temp is
                                            BC61575C 5D4B8037
    C9E380B9 3E376057 2C0B3606 11252C52 85BDEC6C 567C9B5A


------------

  BCC

  IV is
                    00000002 00000000 00000000 00000000


  IV || S is
                                            00000002 00000000
    00000000 00000000 00000030 00000030 A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
```

```
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000


temp is
    BC61575C 5D4B8037 C9E380B9 3E376057 2C0B3606 11252C52
    85BDEC6C 567C9B5A F6259D1D 3848CC93 296E04B5 AD60A97F


------------

Key is
                                        BC61575C 5D4B8037
    C9E380B9 3E376057 2C0B3606 11252C52 85BDEC6C 567C9B5A


X is
                     F6259D1D 3848CC93 296E04B5 AD60A97F


------------

  BlockEncrypt

  Key is
                                        BC61575C 5D4B8037
    C9E380B9 3E376057 2C0B3606 11252C52 85BDEC6C 567C9B5A


  X is
                     F6259D1D 3848CC93 296E04B5 AD60A97F


  X = BlockEncrypt(Key, X) is
                     FBD01F35 7D143F63 0DC0E7F9 B48DAC71


  temp is
                     FBD01F35 7D143F63 0DC0E7F9 B48DAC71


------------

  BlockEncrypt

  Key is
                                        BC61575C 5D4B8037
```

```
        C9E380B9 3E376057 2C0B3606 11252C52 85BDEC6C 567C9B5A


      X is
                           FBD01F35 7D143F63 0DC0E7F9 B48DAC71


      X = BlockEncrypt(Key, X) is
                           440CD750 A626DDB6 7744FD19 DFA9D223


      temp is
                                             FBD01F35 7D143F63
        0DC0E7F9 B48DAC71 440CD750 A626DDB6 7744FD19 DFA9D223


    ------------

      BlockEncrypt

      Key is
                                             BC61575C 5D4B8037
        C9E380B9 3E376057 2C0B3606 11252C52 85BDEC6C 567C9B5A


      X is
                           440CD750 A626DDB6 7744FD19 DFA9D223


      X = BlockEncrypt(Key, X) is
                           FB21DE23 A5E64CE0 712FE847 AF490C39


      temp is
        FBD01F35 7D143F63 0DC0E7F9 B48DAC71 440CD750 A626DDB6
        7744FD19 DFA9D223 FB21DE23 A5E64CE0 712FE847 AF490C39


      requested_bits is
        FBD01F35 7D143F63 0DC0E7F9 B48DAC71 440CD750 A626DDB6
        7744FD19 DFA9D223 FB21DE23 A5E64CE0 712FE847 AF490C39


---------------------------

  Update
```

```
provided_data is
    FBD01F35 7D143F63 0DC0E7F9 B48DAC71 440CD750 A626DDB6
    7744FD19 DFA9D223 FB21DE23 A5E64CE0 712FE847 AF490C39


------------

  While loop

  Key is
                                        D920E7E7 56764052
    FC5BD125 B7B77687 02396659 B28A68C9 6A9F0B0D 5E1DE77C


  V is
                     F5C34D65 24AF4BE0 B2873A11 FAEF059D


  output_block is
                     39AEAB48 6D431EA6 FA729E7B 8DE7EEBC


  temp is
                     39AEAB48 6D431EA6 FA729E7B 8DE7EEBC


------------

  While loop

  Key is
                                        D920E7E7 56764052
    FC5BD125 B7B77687 02396659 B28A68C9 6A9F0B0D 5E1DE77C


  V is
                     F5C34D65 24AF4BE0 B2873A11 FAEF059E


  output_block is
                     2B974223 14E62662 B5292502 EF19F208


  temp is
                                        39AEAB48 6D431EA6
```

```
        FA729E7B 8DE7EEBC 2B974223 14E62662 B5292502 EF19F208


    ------------

      While loop

      Key is
                                              D920E7E7 56764052
        FC5BD125 B7B77687 02396659 B28A68C9 6A9F0B0D 5E1DE77C


      V is
                           F5C34D65 24AF4BE0 B2873A11 FAEF059F


      output_block is
                           5481D794 AEAF9149 3D37E5F4 7344631E


      temp is
        39AEAB48 6D431EA6 FA729E7B 8DE7EEBC 2B974223 14E62662
        B5292502 EF19F208 5481D794 AEAF9149 3D37E5F4 7344631E


    temp XOR provided_data is
        C27EB47D 105721C5 F7B27982 396A42CD 6F9B9573 B2C0FBD4
        C26DD81B 30B0202B AFA009B7 0B49DDA9 4C180DB3 DC0D6F27


    Key is
                                              C27EB47D 105721C5
        F7B27982 396A42CD 6F9B9573 B2C0FBD4 C26DD81B 30B0202B


    V is
                           AFA009B7 0B49DDA9 4C180DB3 DC0D6F27


---------------------------

  Update

    provided_data is
        FBD01F35 7D143F63 0DC0E7F9 B48DAC71 440CD750 A626DDB6
        7744FD19 DFA9D223 FB21DE23 A5E64CE0 712FE847 AF490C39
```

```
------------

  While loop

  Key is
                                          C27EB47D 105721C5
    F7B27982 396A42CD 6F9B9573 B2C0FBD4 C26DD81B 30B0202B


  V is
                      AFA009B7 0B49DDA9 4C180DB3 DC0D6F2A


  output_block is
                      776A18C9 10E930E6 01A81AFA F27A254B


  temp is
                      776A18C9 10E930E6 01A81AFA F27A254B


------------

  While loop

  Key is
                                          C27EB47D 105721C5
    F7B27982 396A42CD 6F9B9573 B2C0FBD4 C26DD81B 30B0202B


  V is
                      AFA009B7 0B49DDA9 4C180DB3 DC0D6F2B


  output_block is
                      6249277E C60F443C CBD11B72 DCB63E6F


  temp is
                                          776A18C9 10E930E6
    01A81AFA F27A254B 6249277E C60F443C CBD11B72 DCB63E6F


------------
```

```
      While loop

      Key is
                                              C27EB47D 105721C5
        F7B27982 396A42CD 6F9B9573 B2C0FBD4 C26DD81B 30B0202B


      V is
                           AFA009B7 0B49DDA9 4C180DB3 DC0D6F2C


      output_block is
                           8FF0B81F D441A1C7 66FFCFD0 EFAFCA4D


      temp is
        776A18C9 10E930E6 01A81AFA F27A254B 6249277E C60F443C
        CBD11B72 DCB63E6F 8FF0B81F D441A1C7 66FFCFD0 EFAFCA4D


    temp XOR provided_data is
        8CBA07FC 6DFD0F85 0C68FD03 46F7893A 2645F02E 6029998A
        BC95E66B 031FEC4C 74D1663C 71A7ED27 17D02797 40E6C674


    Key is
                                              8CBA07FC 6DFD0F85
        0C68FD03 46F7893A 2645F02E 6029998A BC95E66B 031FEC4C


    V is
                           74D1663C 71A7ED27 17D02797 40E6C674


rnd_val is
                                              98A28E3B 1BA363C9
        DAF0F688 7A1CF52B 833D3354 D77A7C10 837DD63D D2E645F8


################################################################

CTR_DRBG

    Requested Security Strength = 256
```

```
    prediction_resistance_flag = "ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    nonce is
                          20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Block_Cipher_df
```

```
input_str is
                     00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
    28292A2B 2C2D2E2F 20212223 24252627 28292A2B 2C2D2E2F


number_of_bits_to_return = 384

S is
                                          00000040 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000


------------

  BCC

  IV is
                     00000000 00000000 00000000 00000000


  IV || S is
    00000000 00000000 00000000 00000000 00000040 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000


temp is
                     4BC4520F E87668A3 A2CE3DCB 5F564BA9


------------

  BCC

  IV is
                     00000001 00000000 00000000 00000000


  IV || S is
    00000001 00000000 00000000 00000000 00000040 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
```

```
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000


temp is
                                        4BC4520F E87668A3
    A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
    00000002 00000000 00000000 00000000 00000040 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000


temp is
    4BC4520F E87668A3 A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB
    9C275423 0F4E6DC4 8283F162 52D8520F D651F481 64D42EC9


------------

Key is
                                        4BC4520F E87668A3
    A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4


X is
                      8283F162 52D8520F D651F481 64D42EC9


------------

  BlockEncrypt

  Key is
                                        4BC4520F E87668A3
```

```
    A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4


  X is
                      8283F162 52D8520F D651F481 64D42EC9


  X = BlockEncrypt(Key, X) is
                      DF1F3CA3 8349478C CDFE738A 222E0645


  temp is
                      DF1F3CA3 8349478C CDFE738A 222E0645


------------

  BlockEncrypt

  Key is
                                          4BC4520F E87668A3
    A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4


  X is
                      DF1F3CA3 8349478C CDFE738A 222E0645


  X = BlockEncrypt(Key, X) is
                      494008AD CEFBE237 13596A7E AE41BBCD


  temp is
                                          DF1F3CA3 8349478C
    CDFE738A 222E0645 494008AD CEFBE237 13596A7E AE41BBCD


------------

  BlockEncrypt

  Key is
                                          4BC4520F E87668A3
    A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4
```

```
      X is
                          494008AD CEFBE237 13596A7E AE41BBCD


      X = BlockEncrypt(Key, X) is
                          C66368D7 8DA21092 840E23C8 995CE6D2


      temp is
        DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
        13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2


      requested_bits is
        DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
        13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2


    seed_material is
        DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
        13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2


---------------------------

  Update

    provided_data is
        DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
        13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2


    ------------

      While loop

      Key is
                                              00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                          00000000 00000000 00000000 00000001


      output_block is
```

```
                    530F8AFB C74536B9 A963B4F1 C4CB738B

  temp is
                    530F8AFB C74536B9 A963B4F1 C4CB738B

------------

  While loop

  Key is
                                          00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000

  V is
                    00000000 00000000 00000000 00000002

  output_block is
                    CEA7403D 4D606B6E 074EC5D3 BAF39D18

  temp is
                                          530F8AFB C74536B9
    A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18

------------

  While loop

  Key is
                                          00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000

  V is
                    00000000 00000000 00000000 00000003

  output_block is
                    726003CA 37A62A74 D1A2F58E 7506358E
```

```
      temp is
        530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
        074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


    temp XOR provided_data is
        8C10B658 440C7135 649DC77B E6E575CE 87E74890 839B8959
        1417AFAD 14B226D5 B4036B1D BA043AE6 55ACD646 EC5AD35C


    Key is
                                            8C10B658 440C7135
        649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5


    V is
                          B4036B1D BA043AE6 55ACD646 EC5AD35C


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

CTR_DRBG_Reseed

    entropy_input is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    additional_input is  <empty>

---------------------------

  Block_Cipher_df
```

```
input_str is
    80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
    98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


number_of_bits_to_return = 384

S is
                     00000030 00000030 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 80000000 00000000


------------

  BCC

  IV is
                     00000000 00000000 00000000 00000000


  IV || S is
                                        00000000 00000000
    00000000 00000000 00000030 00000030 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 80000000 00000000


temp is
                     6808E8C2 37359B53 E4AC883F 8D22A1CA


------------

  BCC

  IV is
                     00000001 00000000 00000000 00000000


  IV || S is
                                        00000001 00000000
    00000000 00000000 00000030 00000030 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 80000000 00000000
```

```
temp is
                                          6808E8C2 37359B53
    E4AC883F 8D22A1CA DC9A2BCF C2C81F7F F712FC22 E18D59F6


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                                          00000002 00000000
    00000000 00000000 00000030 00000030 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 80000000 00000000


temp is
    6808E8C2 37359B53 E4AC883F 8D22A1CA DC9A2BCF C2C81F7F
    F712FC22 E18D59F6 D870D670 2017B3B4 5327BDD3 E5D50B51


------------

Key is
                                          6808E8C2 37359B53
    E4AC883F 8D22A1CA DC9A2BCF C2C81F7F F712FC22 E18D59F6


X is
                      D870D670 2017B3B4 5327BDD3 E5D50B51


------------

  BlockEncrypt

  Key is
                                          6808E8C2 37359B53
    E4AC883F 8D22A1CA DC9A2BCF C2C81F7F F712FC22 E18D59F6
```

```
  X is
                    D870D670 2017B3B4 5327BDD3 E5D50B51


  X = BlockEncrypt(Key, X) is
                    F11E1D8A FE3197D7 A33A494B 9676DBF2


  temp is
                    F11E1D8A FE3197D7 A33A494B 9676DBF2


------------

  BlockEncrypt

  Key is
                                        6808E8C2 37359B53
    E4AC883F 8D22A1CA DC9A2BCF C2C81F7F F712FC22 E18D59F6


  X is
                    F11E1D8A FE3197D7 A33A494B 9676DBF2


  X = BlockEncrypt(Key, X) is
                    27E44756 CA44780C C36E0AA3 895C552E


  temp is
                                        F11E1D8A FE3197D7
    A33A494B 9676DBF2 27E44756 CA44780C C36E0AA3 895C552E


------------

  BlockEncrypt

  Key is
                                        6808E8C2 37359B53
    E4AC883F 8D22A1CA DC9A2BCF C2C81F7F F712FC22 E18D59F6


  X is
                    27E44756 CA44780C C36E0AA3 895C552E
```

```
      X = BlockEncrypt(Key, X) is
                           6301C157 C36F26C4 986874E7 698ECCFD


      temp is
        F11E1D8A FE3197D7 A33A494B 9676DBF2 27E44756 CA44780C
        C36E0AA3 895C552E 6301C157 C36F26C4 986874E7 698ECCFD


      requested_bits is
        F11E1D8A FE3197D7 A33A494B 9676DBF2 27E44756 CA44780C
        C36E0AA3 895C552E 6301C157 C36F26C4 986874E7 698ECCFD


---------------------------

  Update

    provided_data is
        F11E1D8A FE3197D7 A33A494B 9676DBF2 27E44756 CA44780C
        C36E0AA3 895C552E 6301C157 C36F26C4 986874E7 698ECCFD


    ------------

      While loop

      Key is
                                              8C10B658 440C7135
        649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5


      V is
                           B4036B1D BA043AE6 55ACD646 EC5AD35D


      output_block is
                           E686DD55 F758FD91 BA7CB726 FE0B573A


      temp is
                           E686DD55 F758FD91 BA7CB726 FE0B573A
```

```
------------

  While loop

  Key is
                                          8C10B658 440C7135
    649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5


  V is
                      B4036B1D BA043AE6 55ACD646 EC5AD35E


  output_block is
                      180AB674 39FFBDFE 5EC28FB3 7A16A53B


  temp is
                                          E686DD55 F758FD91
    BA7CB726 FE0B573A 180AB674 39FFBDFE 5EC28FB3 7A16A53B


------------

  While loop

  Key is
                                          8C10B658 440C7135
    649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5


  V is
                      B4036B1D BA043AE6 55ACD646 EC5AD35F


  output_block is
                      68F2F51A 364601AF 9533C864 F25DA997


  temp is
    E686DD55 F758FD91 BA7CB726 FE0B573A 180AB674 39FFBDFE
    5EC28FB3 7A16A53B 68F2F51A 364601AF 9533C864 F25DA997


temp XOR provided_data is
    1798C0DF 09696A46 1946FE6D 687D8CC8 3FEEF122 F3BBC5F2
```

```
        9DAC8510 F34AF015 0BF3344D F529276B 0D5BBC83 9BD3656A


    Key is
                                              1798C0DF 09696A46
        1946FE6D 687D8CC8 3FEEF122 F3BBC5F2 9DAC8510 F34AF015


    V is
                         0BF3344D F529276B 0D5BBC83 9BD3656A


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                                              1798C0DF 09696A46
        1946FE6D 687D8CC8 3FEEF122 F3BBC5F2 9DAC8510 F34AF015


      V is
                         0BF3344D F529276B 0D5BBC83 9BD3656D


      output_block is
                         28BC65A8 6AB7C74E DF4BB872 87D34FBB
```

```
  temp is
                      28BC65A8 6AB7C74E DF4BB872 87D34FBB


------------

  While loop

  Key is
                                           1798C0DF 09696A46
    1946FE6D 687D8CC8 3FEEF122 F3BBC5F2 9DAC8510 F34AF015


  V is
                      0BF3344D F529276B 0D5BBC83 9BD3656E


  output_block is
                      8D6F16D7 B91B6ABB EE7B8886 5B0FC7BD


  temp is
                                           28BC65A8 6AB7C74E
    DF4BB872 87D34FBB 8D6F16D7 B91B6ABB EE7B8886 5B0FC7BD


------------

  While loop

  Key is
                                           1798C0DF 09696A46
    1946FE6D 687D8CC8 3FEEF122 F3BBC5F2 9DAC8510 F34AF015


  V is
                      0BF3344D F529276B 0D5BBC83 9BD3656F


  output_block is
                      B74611F3 9295A625 7C39984C 9C099B30


  temp is
    28BC65A8 6AB7C74E DF4BB872 87D34FBB 8D6F16D7 B91B6ABB
    EE7B8886 5B0FC7BD B74611F3 9295A625 7C39984C 9C099B30
```

```
    temp XOR provided_data is
        28BC65A8 6AB7C74E DF4BB872 87D34FBB 8D6F16D7 B91B6ABB
        EE7B8886 5B0FC7BD B74611F3 9295A625 7C39984C 9C099B30


    Key is
                                           28BC65A8 6AB7C74E
        DF4BB872 87D34FBB 8D6F16D7 B91B6ABB EE7B8886 5B0FC7BD


    V is
                          B74611F3 9295A625 7C39984C 9C099B30


rnd_val is
                                           D1E9C737 B6EBAED7
        65A0D4E4 C6EAEBE2 67F5E919 3680FDFF A62F4865 B3F009EC


------------------------------------------------------------

Second call to Generate

************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    additional_input is  <empty>

--------------------------
```

```
Block_Cipher_df

  input_str is
      C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
      D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


  number_of_bits_to_return = 384

  S is
                         00000030 00000030 C0C1C2C3 C4C5C6C7
      C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
      E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF 80000000 00000000


  ------------

    BCC

    IV is
                         00000000 00000000 00000000 00000000


    IV || S is
                                           00000000 00000000
      00000000 00000000 00000030 00000030 C0C1C2C3 C4C5C6C7
      C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
      E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF 80000000 00000000


  temp is
                         F2977267 80DDB539 4AFDD5B8 CCC350C9


  ------------

    BCC

    IV is
                         00000001 00000000 00000000 00000000


    IV || S is
                                           00000001 00000000
      00000000 00000000 00000030 00000030 C0C1C2C3 C4C5C6C7
```

```
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
    E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF 80000000 00000000


temp is
                                        F2977267 80DDB539
    4AFDD5B8 CCC350C9 AA2EF303 87F07708 919EA794 06ADEF9B


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                                        00000002 00000000
    00000000 00000000 00000030 00000030 C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
    E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF 80000000 00000000


temp is
    F2977267 80DDB539 4AFDD5B8 CCC350C9 AA2EF303 87F07708
    919EA794 06ADEF9B 31221A7E 3A0CE21C 54C7074E 0C011CA8


------------

Key is
                                        F2977267 80DDB539
    4AFDD5B8 CCC350C9 AA2EF303 87F07708 919EA794 06ADEF9B


X is
                      31221A7E 3A0CE21C 54C7074E 0C011CA8


------------

  BlockEncrypt

  Key is
                                        F2977267 80DDB539
```

```
    4AFDD5B8 CCC350C9 AA2EF303 87F07708 919EA794 06ADEF9B


  X is
                       31221A7E 3A0CE21C 54C7074E 0C011CA8


  X = BlockEncrypt(Key, X) is
                       AAA32C63 E6A3FED3 B6787677 D5867143


  temp is
                       AAA32C63 E6A3FED3 B6787677 D5867143


------------

  BlockEncrypt

  Key is
                                         F2977267 80DDB539
    4AFDD5B8 CCC350C9 AA2EF303 87F07708 919EA794 06ADEF9B


  X is
                       AAA32C63 E6A3FED3 B6787677 D5867143


  X = BlockEncrypt(Key, X) is
                       F04E8A91 0E0A3F2F A7CDDD9B 8D03090C


  temp is
                                         AAA32C63 E6A3FED3
    B6787677 D5867143 F04E8A91 0E0A3F2F A7CDDD9B 8D03090C


------------

  BlockEncrypt

  Key is
                                         F2977267 80DDB539
    4AFDD5B8 CCC350C9 AA2EF303 87F07708 919EA794 06ADEF9B
```

```
      X is
                          F04E8A91 0E0A3F2F A7CDDD9B 8D03090C


      X = BlockEncrypt(Key, X) is
                          E74B09AD 16BC3C53 457691EE BC770472


      temp is
        AAA32C63 E6A3FED3 B6787677 D5867143 F04E8A91 0E0A3F2F
        A7CDDD9B 8D03090C E74B09AD 16BC3C53 457691EE BC770472


      requested_bits is
        AAA32C63 E6A3FED3 B6787677 D5867143 F04E8A91 0E0A3F2F
        A7CDDD9B 8D03090C E74B09AD 16BC3C53 457691EE BC770472


---------------------------

  Update

    provided_data is
        AAA32C63 E6A3FED3 B6787677 D5867143 F04E8A91 0E0A3F2F
        A7CDDD9B 8D03090C E74B09AD 16BC3C53 457691EE BC770472


    ------------

      While loop

      Key is
                                              28BC65A8 6AB7C74E
        DF4BB872 87D34FBB 8D6F16D7 B91B6ABB EE7B8886 5B0FC7BD


      V is
                          B74611F3 9295A625 7C39984C 9C099B31


      output_block is
                          7ECAD37E 8013E170 208C17FB 03A50642


      temp is
                          7ECAD37E 8013E170 208C17FB 03A50642
```

```
------------

  While loop

  Key is
                                          28BC65A8 6AB7C74E
    DF4BB872 87D34FBB 8D6F16D7 B91B6ABB EE7B8886 5B0FC7BD


  V is
                      B74611F3 9295A625 7C39984C 9C099B32


  output_block is
                      ED31FE00 EE996396 816BAF1B 7071AF4D


  temp is
                                          7ECAD37E 8013E170
    208C17FB 03A50642 ED31FE00 EE996396 816BAF1B 7071AF4D


------------

  While loop

  Key is
                                          28BC65A8 6AB7C74E
    DF4BB872 87D34FBB 8D6F16D7 B91B6ABB EE7B8886 5B0FC7BD


  V is
                      B74611F3 9295A625 7C39984C 9C099B33


  output_block is
                      35C0BF18 C24A77A2 20585DEB 469B94B6


  temp is
    7ECAD37E 8013E170 208C17FB 03A50642 ED31FE00 EE996396
    816BAF1B 7071AF4D 35C0BF18 C24A77A2 20585DEB 469B94B6
```

```
    temp XOR provided_data is
        D469FF1D 66B01FA3 96F4618C D6237701 1D7F7491 E0935CB9
        26A67280 FD72A641 D28BB6B5 D4F64BF1 652ECC05 FAEC90C4


    Key is
                                            D469FF1D 66B01FA3
        96F4618C D6237701 1D7F7491 E0935CB9 26A67280 FD72A641


    V is
                         D28BB6B5 D4F64BF1 652ECC05 FAEC90C4


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                                            D469FF1D 66B01FA3
        96F4618C D6237701 1D7F7491 E0935CB9 26A67280 FD72A641


      V is
                         D28BB6B5 D4F64BF1 652ECC05 FAEC90C7


      output_block is
                         9659D767 B5C6A2BF 0F2D0368 D72322E0
```

```
  temp is
                      9659D767 B5C6A2BF 0F2D0368 D72322E0


------------

  While loop

  Key is
                                          D469FF1D 66B01FA3
    96F4618C D6237701 1D7F7491 E0935CB9 26A67280 FD72A641


  V is
                      D28BB6B5 D4F64BF1 652ECC05 FAEC90C8


  output_block is
                      2B75794A 587DC968 48AB97AE EBA2ED8D


  temp is
                                          9659D767 B5C6A2BF
    0F2D0368 D72322E0 2B75794A 587DC968 48AB97AE EBA2ED8D


------------

  While loop

  Key is
                                          D469FF1D 66B01FA3
    96F4618C D6237701 1D7F7491 E0935CB9 26A67280 FD72A641


  V is
                      D28BB6B5 D4F64BF1 652ECC05 FAEC90C9


  output_block is
                      C7B0D234 2F4275B4 28F8D432 2201BCC7


  temp is
```

```
        9659D767 B5C6A2BF 0F2D0368 D72322E0 2B75794A 587DC968
        48AB97AE EBA2ED8D C7B0D234 2F4275B4 28F8D432 2201BCC7


    temp XOR provided_data is
        9659D767 B5C6A2BF 0F2D0368 D72322E0 2B75794A 587DC968
        48AB97AE EBA2ED8D C7B0D234 2F4275B4 28F8D432 2201BCC7


    Key is
                                            9659D767 B5C6A2BF
        0F2D0368 D72322E0 2B75794A 587DC968 48AB97AE EBA2ED8D


    V is
                          C7B0D234 2F4275B4 28F8D432 2201BCC7


rnd_val is
                                            259DC78C CFAEC421
        0C30AF81 5E4F75A5 662B7DA4 B41013BD C00302DF B6076492


##############################################################

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    Nonce =
```

```
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput1 =
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


    AdditionalInput2 =
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    nonce is
                          20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
        28292A2B 2C2D2E2F 20212223 24252627 28292A2B 2C2D2E2F


    number_of_bits_to_return = 384
```

```
S is
                                          00000040 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000


------------

  BCC

  IV is
                      00000000 00000000 00000000 00000000


  IV || S is
    00000000 00000000 00000000 00000000 00000040 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000


temp is
                      4BC4520F E87668A3 A2CE3DCB 5F564BA9


------------

  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
    00000001 00000000 00000000 00000000 00000040 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000


temp is
                                          4BC4520F E87668A3
    A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4
```

```
------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
    00000002 00000000 00000000 00000000 00000040 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000


temp is
    4BC4520F E87668A3 A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB
    9C275423 0F4E6DC4 8283F162 52D8520F D651F481 64D42EC9


------------

Key is
                                        4BC4520F E87668A3
    A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4


X is
                      8283F162 52D8520F D651F481 64D42EC9


------------

  BlockEncrypt

  Key is
                                        4BC4520F E87668A3
    A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4


  X is
                      8283F162 52D8520F D651F481 64D42EC9


  X = BlockEncrypt(Key, X) is
                      DF1F3CA3 8349478C CDFE738A 222E0645
```

```
  temp is
                      DF1F3CA3 8349478C CDFE738A 222E0645


------------

  BlockEncrypt

  Key is
                                           4BC4520F E87668A3
    A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4


  X is
                      DF1F3CA3 8349478C CDFE738A 222E0645


  X = BlockEncrypt(Key, X) is
                      494008AD CEFBE237 13596A7E AE41BBCD


  temp is
                                           DF1F3CA3 8349478C
    CDFE738A 222E0645 494008AD CEFBE237 13596A7E AE41BBCD


------------

  BlockEncrypt

  Key is
                                           4BC4520F E87668A3
    A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4


  X is
                      494008AD CEFBE237 13596A7E AE41BBCD


  X = BlockEncrypt(Key, X) is
                      C66368D7 8DA21092 840E23C8 995CE6D2


  temp is
```

```
        DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
        13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2


      requested_bits is
        DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
        13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2


    seed_material is
        DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
        13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2


---------------------------

  Update

    provided_data is
        DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
        13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2


    ------------

      While loop

      Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001


      output_block is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


      temp is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


    ------------
```

```
  While loop

  Key is
                                          00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000002


  output_block is
                      CEA7403D 4D606B6E 074EC5D3 BAF39D18


  temp is
                                          530F8AFB C74536B9
    A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18


------------

  While loop

  Key is
                                          00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000003


  output_block is
                      726003CA 37A62A74 D1A2F58E 7506358E


  temp is
    530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
    074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


temp XOR provided_data is
    8C10B658 440C7135 649DC77B E6E575CE 87E74890 839B8959
    1417AFAD 14B226D5 B4036B1D BA043AE6 55ACD646 EC5AD35C
```

```
    Key is
                                            8C10B658 440C7135
        649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5


    V is
                          B4036B1D BA043AE6 55ACD646 EC5AD35C


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


Generate FAILED: Reseed is required
*************************************************************

CTR_DRBG_Reseed

    entropy_input is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


---------------------------

  Block_Cipher_df

    input_str is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
```

```
    98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
    60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
    78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


number_of_bits_to_return = 384

S is
                     00000060 00000030 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000


------------

  BCC

  IV is
                     00000000 00000000 00000000 00000000


  IV || S is
                                        00000000 00000000
    00000000 00000000 00000060 00000030 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000


temp is
                     26006BB7 A0830E15 C03BA4E7 E5D71612


------------

  BCC

  IV is
                     00000001 00000000 00000000 00000000


  IV || S is
                                        00000001 00000000
```

```
    00000000 00000000 00000060 00000030 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000


temp is
                                        26006BB7 A0830E15
    C03BA4E7 E5D71612 8E403592 A555A544 8BB8CCFE B2A3F6D1


------------

  BCC

  IV is
                     00000002 00000000 00000000 00000000


  IV || S is
                                        00000002 00000000
    00000000 00000000 00000060 00000030 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000


temp is
    26006BB7 A0830E15 C03BA4E7 E5D71612 8E403592 A555A544
    8BB8CCFE B2A3F6D1 AEB21276 FE31F327 091B662A E7AEB81E


------------

Key is
                                        26006BB7 A0830E15
    C03BA4E7 E5D71612 8E403592 A555A544 8BB8CCFE B2A3F6D1


X is
                     AEB21276 FE31F327 091B662A E7AEB81E


------------
```

```
  BlockEncrypt

  Key is
                                          26006BB7 A0830E15
    C03BA4E7 E5D71612 8E403592 A555A544 8BB8CCFE B2A3F6D1


  X is
                      AEB21276 FE31F327 091B662A E7AEB81E


  X = BlockEncrypt(Key, X) is
                      D855085C 105ACC7B 757E459C B1895761


  temp is
                      D855085C 105ACC7B 757E459C B1895761


------------

  BlockEncrypt

  Key is
                                          26006BB7 A0830E15
    C03BA4E7 E5D71612 8E403592 A555A544 8BB8CCFE B2A3F6D1


  X is
                      D855085C 105ACC7B 757E459C B1895761


  X = BlockEncrypt(Key, X) is
                      500B0067 10CD4AC5 E966A1E9 3EFF73E0


  temp is
                                          D855085C 105ACC7B
    757E459C B1895761 500B0067 10CD4AC5 E966A1E9 3EFF73E0


------------

  BlockEncrypt
```

```
      Key is
                                              26006BB7 A0830E15
        C03BA4E7 E5D71612 8E403592 A555A544 8BB8CCFE B2A3F6D1


      X is
                           500B0067 10CD4AC5 E966A1E9 3EFF73E0


      X = BlockEncrypt(Key, X) is
                           64E59D80 71CD6888 B6F4DC40 58576A9C


      temp is
        D855085C 105ACC7B 757E459C B1895761 500B0067 10CD4AC5
        E966A1E9 3EFF73E0 64E59D80 71CD6888 B6F4DC40 58576A9C


      requested_bits is
        D855085C 105ACC7B 757E459C B1895761 500B0067 10CD4AC5
        E966A1E9 3EFF73E0 64E59D80 71CD6888 B6F4DC40 58576A9C


----------------------------

  Update

    provided_data is
        D855085C 105ACC7B 757E459C B1895761 500B0067 10CD4AC5
        E966A1E9 3EFF73E0 64E59D80 71CD6888 B6F4DC40 58576A9C


    ------------

      While loop

      Key is
                                              8C10B658 440C7135
        649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5


      V is
                           B4036B1D BA043AE6 55ACD646 EC5AD35D


      output_block is
```

```
                    E686DD55 F758FD91 BA7CB726 FE0B573A

  temp is
                    E686DD55 F758FD91 BA7CB726 FE0B573A

------------

  While loop

  Key is
                                        8C10B658 440C7135
    649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5

  V is
                    B4036B1D BA043AE6 55ACD646 EC5AD35E

  output_block is
                    180AB674 39FFBDFE 5EC28FB3 7A16A53B

  temp is
                                        E686DD55 F758FD91
    BA7CB726 FE0B573A 180AB674 39FFBDFE 5EC28FB3 7A16A53B

------------

  While loop

  Key is
                                        8C10B658 440C7135
    649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5

  V is
                    B4036B1D BA043AE6 55ACD646 EC5AD35F

  output_block is
                    68F2F51A 364601AF 9533C864 F25DA997
```

```
      temp is
        E686DD55 F758FD91 BA7CB726 FE0B573A 180AB674 39FFBDFE
        5EC28FB3 7A16A53B 68F2F51A 364601AF 9533C864 F25DA997


    temp XOR provided_data is
        3ED3D509 E70231EA CF02F2BA 4F82005B 4801B613 2932F73B
        B7A42E5A 44E9D6DB 0C17689A 478B6927 23C71424 AA0AC30B


    Key is
                                            3ED3D509 E70231EA
        CF02F2BA 4F82005B 4801B613 2932F73B B7A42E5A 44E9D6DB


    V is
                           0C17689A 478B6927 23C71424 AA0AC30B


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                                            3ED3D509 E70231EA
        CF02F2BA 4F82005B 4801B613 2932F73B B7A42E5A 44E9D6DB


      V is
```

```
                    0C17689A 478B6927 23C71424 AA0AC30E


  output_block is
                    4CC7BBBC C943D0EB 5B5A21C6 EA95EDD1


  temp is
                    4CC7BBBC C943D0EB 5B5A21C6 EA95EDD1


------------

  While loop

  Key is
                                          3ED3D509 E70231EA
    CF02F2BA 4F82005B 4801B613 2932F73B B7A42E5A 44E9D6DB


  V is
                    0C17689A 478B6927 23C71424 AA0AC30F


  output_block is
                    08DF55C5 8FAF67CD 9E73B72E 01143BCE


  temp is
                                          4CC7BBBC C943D0EB
    5B5A21C6 EA95EDD1 08DF55C5 8FAF67CD 9E73B72E 01143BCE


------------

  While loop

  Key is
                                          3ED3D509 E70231EA
    CF02F2BA 4F82005B 4801B613 2932F73B B7A42E5A 44E9D6DB


  V is
                    0C17689A 478B6927 23C71424 AA0AC310
```

```
      output_block is
                          6A179785 73C8AB48 15DA5329 D1B49C44


      temp is
        4CC7BBBC C943D0EB 5B5A21C6 EA95EDD1 08DF55C5 8FAF67CD
        9E73B72E 01143BCE 6A179785 73C8AB48 15DA5329 D1B49C44


    temp XOR provided_data is
        4CC7BBBC C943D0EB 5B5A21C6 EA95EDD1 08DF55C5 8FAF67CD
        9E73B72E 01143BCE 6A179785 73C8AB48 15DA5329 D1B49C44


    Key is
                                              4CC7BBBC C943D0EB
        5B5A21C6 EA95EDD1 08DF55C5 8FAF67CD 9E73B72E 01143BCE


    V is
                          6A179785 73C8AB48 15DA5329 D1B49C44


rnd_val is
                                              71BB3F9C 9CEAF4E6
        C92A83EB 4C722501 0EE150AC 75E23F5F 77AD5073 EF24D88A


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


Generate FAILED: Reseed is required
***************************************************************
```

CTR_DRBG_Reseed

    entropy_input is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF

  Block_Cipher_df

    input_str is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF

    number_of_bits_to_return = 384

    S is
                          00000060 00000030 C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
        E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000

      BCC

      IV is
                          00000000 00000000 00000000 00000000

      IV || S is
                                                00000000 00000000
        00000000 00000000 00000060 00000030 C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
        E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF A0A1A2A3 A4A5A6A7

```
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000


temp is
                     A77C22F8 F701BD5D F0E36418 04462F38


------------

  BCC

  IV is
                     00000001 00000000 00000000 00000000


  IV || S is
                                          00000001 00000000
    00000000 00000000 00000060 00000030 C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
    E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000


temp is
                                          A77C22F8 F701BD5D
    F0E36418 04462F38 ACB4E9E8 00ABEB0E 18882C37 5360FFB3


------------

  BCC

  IV is
                     00000002 00000000 00000000 00000000


  IV || S is
                                          00000002 00000000
    00000000 00000000 00000060 00000030 C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
    E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000
```

```
temp is
    A77C22F8 F701BD5D F0E36418 04462F38 ACB4E9E8 00ABEB0E
    18882C37 5360FFB3 46C9AE43 4389D41E 050AE515 E7C05BA3


------------

Key is
                                        A77C22F8 F701BD5D
    F0E36418 04462F38 ACB4E9E8 00ABEB0E 18882C37 5360FFB3


X is
                     46C9AE43 4389D41E 050AE515 E7C05BA3


------------

  BlockEncrypt

  Key is
                                        A77C22F8 F701BD5D
    F0E36418 04462F38 ACB4E9E8 00ABEB0E 18882C37 5360FFB3


  X is
                     46C9AE43 4389D41E 050AE515 E7C05BA3


  X = BlockEncrypt(Key, X) is
                     4462618D 4FA2FD6D 5B0312B1 A8BA3E8F


  temp is
                     4462618D 4FA2FD6D 5B0312B1 A8BA3E8F


------------

  BlockEncrypt

  Key is
                                        A77C22F8 F701BD5D
    F0E36418 04462F38 ACB4E9E8 00ABEB0E 18882C37 5360FFB3
```

```
      X is
                          4462618D 4FA2FD6D 5B0312B1 A8BA3E8F


      X = BlockEncrypt(Key, X) is
                          6909E1FF 1DF7D047 788FE17E 615BE531


      temp is
                                            4462618D 4FA2FD6D
        5B0312B1 A8BA3E8F 6909E1FF 1DF7D047 788FE17E 615BE531


    ------------

      BlockEncrypt

      Key is
                                            A77C22F8 F701BD5D
        F0E36418 04462F38 ACB4E9E8 00ABEB0E 18882C37 5360FFB3


      X is
                          6909E1FF 1DF7D047 788FE17E 615BE531


      X = BlockEncrypt(Key, X) is
                          7F99849D D5C2442E BB6CCCC9 4FBAB255


      temp is
        4462618D 4FA2FD6D 5B0312B1 A8BA3E8F 6909E1FF 1DF7D047
        788FE17E 615BE531 7F99849D D5C2442E BB6CCCC9 4FBAB255


      requested_bits is
        4462618D 4FA2FD6D 5B0312B1 A8BA3E8F 6909E1FF 1DF7D047
        788FE17E 615BE531 7F99849D D5C2442E BB6CCCC9 4FBAB255


---------------------------

  Update

    provided_data is
```

```
    4462618D 4FA2FD6D 5B0312B1 A8BA3E8F 6909E1FF 1DF7D047
    788FE17E 615BE531 7F99849D D5C2442E BB6CCCC9 4FBAB255


------------

  While loop

  Key is
                                        4CC7BBBC C943D0EB
    5B5A21C6 EA95EDD1 08DF55C5 8FAF67CD 9E73B72E 01143BCE


  V is
                      6A179785 73C8AB48 15DA5329 D1B49C45


  output_block is
                      24B048EA F05CAFE5 DD6F0FB2 286260F6


  temp is
                      24B048EA F05CAFE5 DD6F0FB2 286260F6


------------

  While loop

  Key is
                                        4CC7BBBC C943D0EB
    5B5A21C6 EA95EDD1 08DF55C5 8FAF67CD 9E73B72E 01143BCE


  V is
                      6A179785 73C8AB48 15DA5329 D1B49C46


  output_block is
                      A70281B2 8D1F015B 274FC493 6887DC9D


  temp is
                                        24B048EA F05CAFE5
    DD6F0FB2 286260F6 A70281B2 8D1F015B 274FC493 6887DC9D
```

```
    ------------

      While loop

      Key is
                                              4CC7BBBC C943D0EB
        5B5A21C6 EA95EDD1 08DF55C5 8FAF67CD 9E73B72E 01143BCE


      V is
                           6A179785 73C8AB48 15DA5329 D1B49C47


      output_block is
                           8086CDC5 A0997070 A038BD76 1C2627A6


      temp is
        24B048EA F05CAFE5 DD6F0FB2 286260F6 A70281B2 8D1F015B
        274FC493 6887DC9D 8086CDC5 A0997070 A038BD76 1C2627A6


    temp XOR provided_data is
        60D22967 BFFE5288 866C1D03 80D85E79 CE0B604D 90E8D11C
        5FC025ED 09DC39AC FF1F4958 755B345E 1B5471BF 539C95F3


    Key is
                                              60D22967 BFFE5288
        866C1D03 80D85E79 CE0B604D 90E8D11C 5FC025ED 09DC39AC


    V is
                           FF1F4958 755B345E 1B5471BF 539C95F3

**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------
```

```
Update

  provided_data is
      00000000 00000000 00000000 00000000 00000000 00000000
      00000000 00000000 00000000 00000000 00000000 00000000


  ------------

    While loop

    Key is
                                              60D22967 BFFE5288
      866C1D03 80D85E79 CE0B604D 90E8D11C 5FC025ED 09DC39AC


    V is
                         FF1F4958 755B345E 1B5471BF 539C95F6


    output_block is
                         9E56500A 6898B16D 6265BC60 CAF2705E


    temp is
                         9E56500A 6898B16D 6265BC60 CAF2705E


  ------------

    While loop

    Key is
                                              60D22967 BFFE5288
      866C1D03 80D85E79 CE0B604D 90E8D11C 5FC025ED 09DC39AC


    V is
                         FF1F4958 755B345E 1B5471BF 539C95F7


    output_block is
                         1453470E D44D2883 B421447D 71F6176B
```

```
      temp is
                                                9E56500A 6898B16D
        6265BC60 CAF2705E 1453470E D44D2883 B421447D 71F6176B


    ------------

      While loop

      Key is
                                                60D22967 BFFE5288
        866C1D03 80D85E79 CE0B604D 90E8D11C 5FC025ED 09DC39AC


      V is
                           FF1F4958 755B345E 1B5471BF 539C95F8


      output_block is
                           4D0DC726 445D0DEC C1CD0D7C 41016C9B


      temp is
        9E56500A 6898B16D 6265BC60 CAF2705E 1453470E D44D2883
        B421447D 71F6176B 4D0DC726 445D0DEC C1CD0D7C 41016C9B


    temp XOR provided_data is
        9E56500A 6898B16D 6265BC60 CAF2705E 1453470E D44D2883
        B421447D 71F6176B 4D0DC726 445D0DEC C1CD0D7C 41016C9B


    Key is
                                                9E56500A 6898B16D
        6265BC60 CAF2705E 1453470E D44D2883 B421447D 71F6176B


    V is
                           4D0DC726 445D0DEC C1CD0D7C 41016C9B


rnd_val is
                                                386DEBBB F091BBF0
        502957B0 329938FB 836B82E5 94A2F5FD D5EB28D4 E35528F4
```

```
###############################################################

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    Nonce =
                            20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString =
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    AdditionalInput = <empty>

###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    nonce is
                            20212223 24252627 28292A2B 2C2D2E2F
```

```
    personal_str is
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
        28292A2B 2C2D2E2F 20212223 24252627 28292A2B 2C2D2E2F
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    number_of_bits_to_return = 384

    S is
                                               00000070 00000030
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
        20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
        60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000


    ------------

      BCC

      IV is
                          00000000 00000000 00000000 00000000


      IV || S is
        00000000 00000000 00000000 00000000 00000070 00000030
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
        20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
```

```
    60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000


temp is
                     8A0B0FB5 AA3FA8FD 4B9E8708 FACD2A08


------------

  BCC

  IV is
                     00000001 00000000 00000000 00000000


  IV || S is
    00000001 00000000 00000000 00000070 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
    48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
    60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000


temp is
                                        8A0B0FB5 AA3FA8FD
    4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718


------------

  BCC

  IV is
                     00000002 00000000 00000000 00000000


  IV || S is
    00000002 00000000 00000000 00000070 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
    48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
    60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000
```

```
temp is
    8A0B0FB5 AA3FA8FD 4B9E8708 FACD2A08 A13B6B8D A420CCBC
    43CF57C7 F3A7C718 2B4B429F EDFD2D2D 937CA4B4 71B86606


------------

Key is
                                        8A0B0FB5 AA3FA8FD
    4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718


X is
                     2B4B429F EDFD2D2D 937CA4B4 71B86606


------------

  BlockEncrypt

  Key is
                                        8A0B0FB5 AA3FA8FD
    4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718


  X is
                     2B4B429F EDFD2D2D 937CA4B4 71B86606


  X = BlockEncrypt(Key, X) is
                     31D82952 CBF4754A 1354F1A9 184841B4


  temp is
                     31D82952 CBF4754A 1354F1A9 184841B4


------------

  BlockEncrypt

  Key is
                                        8A0B0FB5 AA3FA8FD
    4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718
```

```
      X is
                          31D82952 CBF4754A 1354F1A9 184841B4


      X = BlockEncrypt(Key, X) is
                          C0812181 C179FD79 547E5367 AB8C9FA4


      temp is
                                            31D82952 CBF4754A
        1354F1A9 184841B4 C0812181 C179FD79 547E5367 AB8C9FA4


    ------------

      BlockEncrypt

      Key is
                                            8A0B0FB5 AA3FA8FD
        4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718


      X is
                          C0812181 C179FD79 547E5367 AB8C9FA4


      X = BlockEncrypt(Key, X) is
                          51223D14 E89B833F 62FC5EF8 0034A200


      temp is
        31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
        547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200


      requested_bits is
        31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
        547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200


    seed_material is
        31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
        547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200


--------------------------
```

```
Update

  provided_data is
      31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
      547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200


  ------------

    While loop

    Key is
                                                00000000 00000000
      00000000 00000000 00000000 00000000 00000000 00000000


    V is
                         00000000 00000000 00000000 00000001


    output_block is
                         530F8AFB C74536B9 A963B4F1 C4CB738B


    temp is
                         530F8AFB C74536B9 A963B4F1 C4CB738B


  ------------

    While loop

    Key is
                                                00000000 00000000
      00000000 00000000 00000000 00000000 00000000 00000000


    V is
                         00000000 00000000 00000000 00000002


    output_block is
                         CEA7403D 4D606B6E 074EC5D3 BAF39D18
```

```
      temp is
                                                530F8AFB C74536B9
        A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18


    ------------

      While loop

      Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000003


      output_block is
                           726003CA 37A62A74 D1A2F58E 7506358E


      temp is
        530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
        074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


    temp XOR provided_data is
        62D7A3A9 0CB143F3 BA374558 DC83323F 0E2661BC 8C199617
        533096B4 117F02BC 23423EDE DF3DA94B B35EAB76 7532978E


    Key is
                                                62D7A3A9 0CB143F3
        BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC


    V is
                           23423EDE DF3DA94B B35EAB76 7532978E


------------------------------------------------------------

First call to Generate

************************************************************
```

```
CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
************************************************************

CTR_DRBG_Reseed

    entropy_input is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    additional_input is  <empty>

---------------------------

  Block_Cipher_df

    input_str is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    number_of_bits_to_return = 384

    S is
                          00000030 00000030 80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 80000000 00000000


    ------------

      BCC

      IV is
                          00000000 00000000 00000000 00000000


      IV || S is
                                             00000000 00000000
```

```
    00000000 00000000 00000030 00000030 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 80000000 00000000


temp is
                     6808E8C2 37359B53 E4AC883F 8D22A1CA


------------

  BCC

  IV is
                     00000001 00000000 00000000 00000000


  IV || S is
                                       00000001 00000000
    00000000 00000000 00000030 00000030 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 80000000 00000000


temp is
                                       6808E8C2 37359B53
    E4AC883F 8D22A1CA DC9A2BCF C2C81F7F F712FC22 E18D59F6


------------

  BCC

  IV is
                     00000002 00000000 00000000 00000000


  IV || S is
                                       00000002 00000000
    00000000 00000000 00000030 00000030 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 80000000 00000000


temp is
    6808E8C2 37359B53 E4AC883F 8D22A1CA DC9A2BCF C2C81F7F
```

```
    F712FC22 E18D59F6 D870D670 2017B3B4 5327BDD3 E5D50B51


------------

Key is
                                        6808E8C2 37359B53
    E4AC883F 8D22A1CA DC9A2BCF C2C81F7F F712FC22 E18D59F6


X is
                     D870D670 2017B3B4 5327BDD3 E5D50B51


------------

  BlockEncrypt

  Key is
                                        6808E8C2 37359B53
    E4AC883F 8D22A1CA DC9A2BCF C2C81F7F F712FC22 E18D59F6


  X is
                     D870D670 2017B3B4 5327BDD3 E5D50B51


  X = BlockEncrypt(Key, X) is
                     F11E1D8A FE3197D7 A33A494B 9676DBF2


  temp is
                     F11E1D8A FE3197D7 A33A494B 9676DBF2


------------

  BlockEncrypt

  Key is
                                        6808E8C2 37359B53
    E4AC883F 8D22A1CA DC9A2BCF C2C81F7F F712FC22 E18D59F6


  X is
                     F11E1D8A FE3197D7 A33A494B 9676DBF2
```

```
      X = BlockEncrypt(Key, X) is
                          27E44756 CA44780C C36E0AA3 895C552E


      temp is
                                                F11E1D8A FE3197D7
        A33A494B 9676DBF2 27E44756 CA44780C C36E0AA3 895C552E


    ------------

      BlockEncrypt

      Key is
                                                6808E8C2 37359B53
        E4AC883F 8D22A1CA DC9A2BCF C2C81F7F F712FC22 E18D59F6


      X is
                          27E44756 CA44780C C36E0AA3 895C552E


      X = BlockEncrypt(Key, X) is
                          6301C157 C36F26C4 986874E7 698ECCFD


      temp is
        F11E1D8A FE3197D7 A33A494B 9676DBF2 27E44756 CA44780C
        C36E0AA3 895C552E 6301C157 C36F26C4 986874E7 698ECCFD


      requested_bits is
        F11E1D8A FE3197D7 A33A494B 9676DBF2 27E44756 CA44780C
        C36E0AA3 895C552E 6301C157 C36F26C4 986874E7 698ECCFD


---------------------------

  Update

    provided_data is
        F11E1D8A FE3197D7 A33A494B 9676DBF2 27E44756 CA44780C
        C36E0AA3 895C552E 6301C157 C36F26C4 986874E7 698ECCFD
```

```
------------

  While loop

  Key is
                                          62D7A3A9 0CB143F3
    BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC


  V is
                      23423EDE DF3DA94B B35EAB76 7532978F


  output_block is
                      99BB703C DD820609 903F1241 EA856E27


  temp is
                      99BB703C DD820609 903F1241 EA856E27


------------

  While loop

  Key is
                                          62D7A3A9 0CB143F3
    BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC


  V is
                      23423EDE DF3DA94B B35EAB76 75329790


  output_block is
                      A54C2B75 EEA7775B 68093FCD 47B52E7F


  temp is
                                          99BB703C DD820609
    903F1241 EA856E27 A54C2B75 EEA7775B 68093FCD 47B52E7F


------------
```

```
      While loop

      Key is
                                              62D7A3A9 0CB143F3
        BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC


      V is
                           23423EDE DF3DA94B B35EAB76 75329791


      output_block is
                           40A4397E 72F15782 98F8B8FB 54A8BAD1


      temp is
        99BB703C DD820609 903F1241 EA856E27 A54C2B75 EEA7775B
        68093FCD 47B52E7F 40A4397E 72F15782 98F8B8FB 54A8BAD1


    temp XOR provided_data is
        68A56DB6 23B391DE 33055B0A 7CF3B5D5 82A86C23 24E30F57
        AB67356E CEE97B51 23A5F829 B19E7146 0090CC1C 3D26762C


    Key is
                                              68A56DB6 23B391DE
        33055B0A 7CF3B5D5 82A86C23 24E30F57 AB67356E CEE97B51


    V is
                           23A5F829 B19E7146 0090CC1C 3D26762C


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update
```

```
provided_data is
    00000000 00000000 00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


------------

  While loop

  Key is
                                          68A56DB6 23B391DE
    33055B0A 7CF3B5D5 82A86C23 24E30F57 AB67356E CEE97B51


  V is
                      23A5F829 B19E7146 0090CC1C 3D26762F


  output_block is
                      0C47A82D 2442216E A904EC72 E3BDF875


  temp is
                      0C47A82D 2442216E A904EC72 E3BDF875


------------

  While loop

  Key is
                                          68A56DB6 23B391DE
    33055B0A 7CF3B5D5 82A86C23 24E30F57 AB67356E CEE97B51


  V is
                      23A5F829 B19E7146 0090CC1C 3D267630


  output_block is
                      6ABE26CD 74DC1CD3 EC6084B1 C60B49E8


  temp is
                                          0C47A82D 2442216E
    A904EC72 E3BDF875 6ABE26CD 74DC1CD3 EC6084B1 C60B49E8
```

```
    ------------

      While loop

      Key is
                                              68A56DB6 23B391DE
        33055B0A 7CF3B5D5 82A86C23 24E30F57 AB67356E CEE97B51


      V is
                           23A5F829 B19E7146 0090CC1C 3D267631


      output_block is
                           5BF18BBA A9D36E9D A7C1A6B4 FB4ABC9D


      temp is
        0C47A82D 2442216E A904EC72 E3BDF875 6ABE26CD 74DC1CD3
        EC6084B1 C60B49E8 5BF18BBA A9D36E9D A7C1A6B4 FB4ABC9D


    temp XOR provided_data is
        0C47A82D 2442216E A904EC72 E3BDF875 6ABE26CD 74DC1CD3
        EC6084B1 C60B49E8 5BF18BBA A9D36E9D A7C1A6B4 FB4ABC9D


    Key is
                                              0C47A82D 2442216E
        A904EC72 E3BDF875 6ABE26CD 74DC1CD3 EC6084B1 C60B49E8


    V is
                           5BF18BBA A9D36E9D A7C1A6B4 FB4ABC9D


rnd_val is
                                              1A2E3FEE 9056E98D
        375525FD C2B63B95 B47CE51F CF594D80 4BD5A17F 2E01139B


------------------------------------------------------------

Second call to Generate
```

```
***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    additional_input is  <empty>

---------------------------

  Block_Cipher_df

    input_str is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    number_of_bits_to_return = 384

    S is
                          00000030 00000030 C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
        E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF 80000000 00000000


    ------------

      BCC

      IV is
                          00000000 00000000 00000000 00000000
```

```
  IV || S is
                                                00000000 00000000
    00000000 00000000 00000030 00000030 C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
    E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF 80000000 00000000


temp is
                     F2977267 80DDB539 4AFDD5B8 CCC350C9


------------

  BCC

  IV is
                     00000001 00000000 00000000 00000000


  IV || S is
                                                00000001 00000000
    00000000 00000000 00000030 00000030 C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
    E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF 80000000 00000000


temp is
                                                F2977267 80DDB539
    4AFDD5B8 CCC350C9 AA2EF303 87F07708 919EA794 06ADEF9B


------------

  BCC

  IV is
                     00000002 00000000 00000000 00000000


  IV || S is
                                                00000002 00000000
    00000000 00000000 00000030 00000030 C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
    E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF 80000000 00000000
```

```
temp is
    F2977267 80DDB539 4AFDD5B8 CCC350C9 AA2EF303 87F07708
    919EA794 06ADEF9B 31221A7E 3A0CE21C 54C7074E 0C011CA8


------------

Key is
                                        F2977267 80DDB539
    4AFDD5B8 CCC350C9 AA2EF303 87F07708 919EA794 06ADEF9B


X is
                     31221A7E 3A0CE21C 54C7074E 0C011CA8


------------

  BlockEncrypt

  Key is
                                        F2977267 80DDB539
    4AFDD5B8 CCC350C9 AA2EF303 87F07708 919EA794 06ADEF9B


  X is
                     31221A7E 3A0CE21C 54C7074E 0C011CA8


  X = BlockEncrypt(Key, X) is
                     AAA32C63 E6A3FED3 B6787677 D5867143


  temp is
                     AAA32C63 E6A3FED3 B6787677 D5867143


------------

  BlockEncrypt

  Key is
                                        F2977267 80DDB539
    4AFDD5B8 CCC350C9 AA2EF303 87F07708 919EA794 06ADEF9B
```

```
      X is
                          AAA32C63 E6A3FED3 B6787677 D5867143

      X = BlockEncrypt(Key, X) is
                          F04E8A91 0E0A3F2F A7CDDD9B 8D03090C

      temp is
                                             AAA32C63 E6A3FED3
        B6787677 D5867143 F04E8A91 0E0A3F2F A7CDDD9B 8D03090C

    ------------

      BlockEncrypt

      Key is
                                             F2977267 80DDB539
        4AFDD5B8 CCC350C9 AA2EF303 87F07708 919EA794 06ADEF9B

      X is
                          F04E8A91 0E0A3F2F A7CDDD9B 8D03090C

      X = BlockEncrypt(Key, X) is
                          E74B09AD 16BC3C53 457691EE BC770472

      temp is
        AAA32C63 E6A3FED3 B6787677 D5867143 F04E8A91 0E0A3F2F
        A7CDDD9B 8D03090C E74B09AD 16BC3C53 457691EE BC770472

      requested_bits is
        AAA32C63 E6A3FED3 B6787677 D5867143 F04E8A91 0E0A3F2F
        A7CDDD9B 8D03090C E74B09AD 16BC3C53 457691EE BC770472

---------------------------

  Update

    provided_data is
        AAA32C63 E6A3FED3 B6787677 D5867143 F04E8A91 0E0A3F2F
```

```
    A7CDDD9B 8D03090C E74B09AD 16BC3C53 457691EE BC770472


------------

  While loop

  Key is
                                          0C47A82D 2442216E
    A904EC72 E3BDF875 6ABE26CD 74DC1CD3 EC6084B1 C60B49E8


  V is
                      5BF18BBA A9D36E9D A7C1A6B4 FB4ABC9E


  output_block is
                      AB18E1F1 ABEF409E 52DCDE30 3D02FC54


  temp is
                      AB18E1F1 ABEF409E 52DCDE30 3D02FC54


------------

  While loop

  Key is
                                          0C47A82D 2442216E
    A904EC72 E3BDF875 6ABE26CD 74DC1CD3 EC6084B1 C60B49E8


  V is
                      5BF18BBA A9D36E9D A7C1A6B4 FB4ABC9F


  output_block is
                      DE988F57 31C380F9 B32BA7C3 4C794DDB


  temp is
                                          AB18E1F1 ABEF409E
    52DCDE30 3D02FC54 DE988F57 31C380F9 B32BA7C3 4C794DDB
```

```
    ------------

      While loop

      Key is
                                              0C47A82D 2442216E
        A904EC72 E3BDF875 6ABE26CD 74DC1CD3 EC6084B1 C60B49E8


      V is
                           5BF18BBA A9D36E9D A7C1A6B4 FB4ABCA0


      output_block is
                           88DBB237 E58E23BF E34A6BF4 592480D9


      temp is
        AB18E1F1 ABEF409E 52DCDE30 3D02FC54 DE988F57 31C380F9
        B32BA7C3 4C794DDB 88DBB237 E58E23BF E34A6BF4 592480D9


    temp XOR provided_data is
        01BBCD92 4D4CBE4D E4A4A847 E8848D17 2ED605C6 3FC9BFD6
        14E67A58 C17A44D7 6F90BB9A F3321FEC A63CFA1A E55384AB


    Key is
                                              01BBCD92 4D4CBE4D
        E4A4A847 E8848D17 2ED605C6 3FC9BFD6 14E67A58 C17A44D7


    V is
                           6F90BB9A F3321FEC A63CFA1A E55384AB


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------
```

```
Update

  provided_data is
      00000000 00000000 00000000 00000000 00000000 00000000
      00000000 00000000 00000000 00000000 00000000 00000000


  ------------

    While loop

    Key is
                                             01BBCD92 4D4CBE4D
      E4A4A847 E8848D17 2ED605C6 3FC9BFD6 14E67A58 C17A44D7


    V is
                       6F90BB9A F3321FEC A63CFA1A E55384AE


    output_block is
                       A36C785C 712E59D1 2FDE205C 9A10BAE5


    temp is
                       A36C785C 712E59D1 2FDE205C 9A10BAE5


  ------------

    While loop

    Key is
                                             01BBCD92 4D4CBE4D
      E4A4A847 E8848D17 2ED605C6 3FC9BFD6 14E67A58 C17A44D7


    V is
                       6F90BB9A F3321FEC A63CFA1A E55384AF


    output_block is
                       C0A4CA2F 0282977F 44D0F4A1 EC889D62


    temp is
```

```
                                            A36C785C 712E59D1
        2FDE205C 9A10BAE5 C0A4CA2F 0282977F 44D0F4A1 EC889D62


    ------------

      While loop

      Key is
                                            01BBCD92 4D4CBE4D
        E4A4A847 E8848D17 2ED605C6 3FC9BFD6 14E67A58 C17A44D7


      V is
                           6F90BB9A F3321FEC A63CFA1A E55384B0


      output_block is
                           CEC24BC1 DABE2F6E 459F14FD 869349FB


      temp is
        A36C785C 712E59D1 2FDE205C 9A10BAE5 C0A4CA2F 0282977F
        44D0F4A1 EC889D62 CEC24BC1 DABE2F6E 459F14FD 869349FB


    temp XOR provided_data is
        A36C785C 712E59D1 2FDE205C 9A10BAE5 C0A4CA2F 0282977F
        44D0F4A1 EC889D62 CEC24BC1 DABE2F6E 459F14FD 869349FB


    Key is
                                            A36C785C 712E59D1
        2FDE205C 9A10BAE5 C0A4CA2F 0282977F 44D0F4A1 EC889D62


    V is
                           CEC24BC1 DABE2F6E 459F14FD 869349FB


rnd_val is
                                            601F9538 4F0D8594
        6301D1EA CE8F645A 825CE38F 1E2565B0 C0C43944 8E9CA8AC


################################################################
```

```
CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString =
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    AdditionalInput1 =
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


    AdditionalInput2 =
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - with derivation function
```

```
    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    nonce is
                         20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Block_Cipher_df

    input_str is
                         00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
        28292A2B 2C2D2E2F 20212223 24252627 28292A2B 2C2D2E2F
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    number_of_bits_to_return = 384

    S is
                                               00000070 00000030
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
        20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
        60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000


    ------------

      BCC

      IV is
                         00000000 00000000 00000000 00000000
```

```
  IV || S is
    00000000 00000000 00000000 00000000 00000070 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
    48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
    60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000


temp is
                     8A0B0FB5 AA3FA8FD 4B9E8708 FACD2A08


------------

  BCC

  IV is
                     00000001 00000000 00000000 00000000


  IV || S is
    00000001 00000000 00000000 00000000 00000070 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
    48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
    60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000


temp is
                                        8A0B0FB5 AA3FA8FD
    4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718


------------

  BCC

  IV is
                     00000002 00000000 00000000 00000000


  IV || S is
    00000002 00000000 00000000 00000000 00000070 00000030
```

```
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
    48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
    60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000


temp is
    8A0B0FB5 AA3FA8FD 4B9E8708 FACD2A08 A13B6B8D A420CCBC
    43CF57C7 F3A7C718 2B4B429F EDFD2D2D 937CA4B4 71B86606


------------

Key is
                                        8A0B0FB5 AA3FA8FD
    4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718


X is
                     2B4B429F EDFD2D2D 937CA4B4 71B86606


------------

  BlockEncrypt

  Key is
                                        8A0B0FB5 AA3FA8FD
    4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718


  X is
                     2B4B429F EDFD2D2D 937CA4B4 71B86606


  X = BlockEncrypt(Key, X) is
                     31D82952 CBF4754A 1354F1A9 184841B4


  temp is
                     31D82952 CBF4754A 1354F1A9 184841B4


------------
```

```
  BlockEncrypt

  Key is
                                          8A0B0FB5 AA3FA8FD
    4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718


  X is
                      31D82952 CBF4754A 1354F1A9 184841B4


  X = BlockEncrypt(Key, X) is
                      C0812181 C179FD79 547E5367 AB8C9FA4


  temp is
                                          31D82952 CBF4754A
    1354F1A9 184841B4 C0812181 C179FD79 547E5367 AB8C9FA4


------------

  BlockEncrypt

  Key is
                                          8A0B0FB5 AA3FA8FD
    4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718


  X is
                      C0812181 C179FD79 547E5367 AB8C9FA4


  X = BlockEncrypt(Key, X) is
                      51223D14 E89B833F 62FC5EF8 0034A200


  temp is
    31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
    547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200


  requested_bits is
    31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
    547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200
```

```
    seed_material is
        31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
        547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200


---------------------------

  Update

    provided_data is
        31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
        547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200


    ------------

      While loop

      Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001


      output_block is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


      temp is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


    ------------

      While loop

      Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
```

```
                      00000000 00000000 00000000 00000002

  output_block is
                      CEA7403D 4D606B6E 074EC5D3 BAF39D18

  temp is
                                        530F8AFB C74536B9
    A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18

------------

  While loop

  Key is
                                        00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000003

  output_block is
                      726003CA 37A62A74 D1A2F58E 7506358E

  temp is
    530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
    074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E

temp XOR provided_data is
    62D7A3A9 0CB143F3 BA374558 DC83323F 0E2661BC 8C199617
    533096B4 117F02BC 23423EDE DF3DA94B B35EAB76 7532978E

Key is
                                        62D7A3A9 0CB143F3
    BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC

V is
                      23423EDE DF3DA94B B35EAB76 7532978E
```

```
-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


Generate FAILED: Reseed is required
*************************************************************

CTR_DRBG_Reseed

    entropy_input is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


---------------------------

  Block_Cipher_df

    input_str is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


    number_of_bits_to_return = 384

    S is
```

```
                    00000060 00000030 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000


------------

  BCC

  IV is
                    00000000 00000000 00000000 00000000


  IV || S is
                                       00000000 00000000
    00000000 00000000 00000060 00000030 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000


temp is
                    26006BB7 A0830E15 C03BA4E7 E5D71612


------------

  BCC

  IV is
                    00000001 00000000 00000000 00000000


  IV || S is
                                       00000001 00000000
    00000000 00000000 00000060 00000030 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000


temp is
```

```
                                          26006BB7 A0830E15
    C03BA4E7 E5D71612 8E403592 A555A544 8BB8CCFE B2A3F6D1


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                                          00000002 00000000
    00000000 00000000 00000060 00000030 80818283 84858687
    88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
    80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000


temp is
    26006BB7 A0830E15 C03BA4E7 E5D71612 8E403592 A555A544
    8BB8CCFE B2A3F6D1 AEB21276 FE31F327 091B662A E7AEB81E


------------

Key is
                                          26006BB7 A0830E15
    C03BA4E7 E5D71612 8E403592 A555A544 8BB8CCFE B2A3F6D1


X is
                      AEB21276 FE31F327 091B662A E7AEB81E


------------

  BlockEncrypt

  Key is
                                          26006BB7 A0830E15
    C03BA4E7 E5D71612 8E403592 A555A544 8BB8CCFE B2A3F6D1
```

```
  X is
                      AEB21276 FE31F327 091B662A E7AEB81E


  X = BlockEncrypt(Key, X) is
                      D855085C 105ACC7B 757E459C B1895761


  temp is
                      D855085C 105ACC7B 757E459C B1895761


------------

  BlockEncrypt

  Key is
                                          26006BB7 A0830E15
    C03BA4E7 E5D71612 8E403592 A555A544 8BB8CCFE B2A3F6D1


  X is
                      D855085C 105ACC7B 757E459C B1895761


  X = BlockEncrypt(Key, X) is
                      500B0067 10CD4AC5 E966A1E9 3EFF73E0


  temp is
                                          D855085C 105ACC7B
    757E459C B1895761 500B0067 10CD4AC5 E966A1E9 3EFF73E0


------------

  BlockEncrypt

  Key is
                                          26006BB7 A0830E15
    C03BA4E7 E5D71612 8E403592 A555A544 8BB8CCFE B2A3F6D1


  X is
                      500B0067 10CD4AC5 E966A1E9 3EFF73E0
```

```
      X = BlockEncrypt(Key, X) is
                          64E59D80 71CD6888 B6F4DC40 58576A9C


      temp is
        D855085C 105ACC7B 757E459C B1895761 500B0067 10CD4AC5
        E966A1E9 3EFF73E0 64E59D80 71CD6888 B6F4DC40 58576A9C


      requested_bits is
        D855085C 105ACC7B 757E459C B1895761 500B0067 10CD4AC5
        E966A1E9 3EFF73E0 64E59D80 71CD6888 B6F4DC40 58576A9C


---------------------------

  Update

    provided_data is
        D855085C 105ACC7B 757E459C B1895761 500B0067 10CD4AC5
        E966A1E9 3EFF73E0 64E59D80 71CD6888 B6F4DC40 58576A9C


    ------------

      While loop

      Key is
                                             62D7A3A9 0CB143F3
        BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC


      V is
                          23423EDE DF3DA94B B35EAB76 7532978F


      output_block is
                          99BB703C DD820609 903F1241 EA856E27


      temp is
                          99BB703C DD820609 903F1241 EA856E27


    ------------
```

```
  While loop

  Key is
                                          62D7A3A9 0CB143F3
    BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC


  V is
                     23423EDE DF3DA94B B35EAB76 75329790


  output_block is
                     A54C2B75 EEA7775B 68093FCD 47B52E7F


  temp is
                                          99BB703C DD820609
    903F1241 EA856E27 A54C2B75 EEA7775B 68093FCD 47B52E7F


------------

  While loop

  Key is
                                          62D7A3A9 0CB143F3
    BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC


  V is
                     23423EDE DF3DA94B B35EAB76 75329791


  output_block is
                     40A4397E 72F15782 98F8B8FB 54A8BAD1


  temp is
    99BB703C DD820609 903F1241 EA856E27 A54C2B75 EEA7775B
    68093FCD 47B52E7F 40A4397E 72F15782 98F8B8FB 54A8BAD1


temp XOR provided_data is
    41EE7860 CDD8CA72 E54157DD 5B0C3946 F5472B12 FE6A3D9E
    816F9E24 794A5D9F 2441A4FE 033C3F0A 2E0C64BB 0CFFD04D
```

```
    Key is
                                            41EE7860 CDD8CA72
        E54157DD 5B0C3946 F5472B12 FE6A3D9E 816F9E24 794A5D9F


    V is
                         2441A4FE 033C3F0A 2E0C64BB 0CFFD04D


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                                            41EE7860 CDD8CA72
        E54157DD 5B0C3946 F5472B12 FE6A3D9E 816F9E24 794A5D9F


      V is
                         2441A4FE 033C3F0A 2E0C64BB 0CFFD050


      output_block is
                         30B27377 DE24BD94 8F2037BC BA1BB65B


      temp is
```

```
                    30B27377 DE24BD94 8F2037BC BA1BB65B


------------

  While loop

  Key is
                                        41EE7860 CDD8CA72
    E54157DD 5B0C3946 F5472B12 FE6A3D9E 816F9E24 794A5D9F


  V is
                    2441A4FE 033C3F0A 2E0C64BB 0CFFD051


  output_block is
                    EAF4E2D2 46CFE777 0F27D16B 89069C3A


  temp is
                                        30B27377 DE24BD94
    8F2037BC BA1BB65B EAF4E2D2 46CFE777 0F27D16B 89069C3A


------------

  While loop

  Key is
                                        41EE7860 CDD8CA72
    E54157DD 5B0C3946 F5472B12 FE6A3D9E 816F9E24 794A5D9F


  V is
                    2441A4FE 033C3F0A 2E0C64BB 0CFFD052


  output_block is
                    0592090E A1D6CB56 93F23B12 1BB07AC2


  temp is
    30B27377 DE24BD94 8F2037BC BA1BB65B EAF4E2D2 46CFE777
    0F27D16B 89069C3A 0592090E A1D6CB56 93F23B12 1BB07AC2
```

```
    temp XOR provided_data is
        30B27377 DE24BD94 8F2037BC BA1BB65B EAF4E2D2 46CFE777
        0F27D16B 89069C3A 0592090E A1D6CB56 93F23B12 1BB07AC2


    Key is
                                            30B27377 DE24BD94
        8F2037BC BA1BB65B EAF4E2D2 46CFE777 0F27D16B 89069C3A


    V is
                          0592090E A1D6CB56 93F23B12 1BB07AC2


rnd_val is
                                            EAE6BCE7 81807E52
        4D26605E A1980779 32D01EEB 445B9AC6 C5D99C10 1D29F46E


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


Generate FAILED: Reseed is required
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    additional_input is
```

```
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


----------------------------

  Block_Cipher_df

    input_str is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    number_of_bits_to_return = 384

    S is
                         00000060 00000030 C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
        E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000


    ------------

      BCC

      IV is
                         00000000 00000000 00000000 00000000


      IV || S is
                                                  00000000 00000000
        00000000 00000000 00000060 00000030 C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
        E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000


    temp is
                         A77C22F8 F701BD5D F0E36418 04462F38
```

```
------------

  BCC

  IV is
                      00000001 00000000 00000000 00000000


  IV || S is
                                           00000001 00000000
    00000000 00000000 00000060 00000030 C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
    E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000


temp is
                                           A77C22F8 F701BD5D
    F0E36418 04462F38 ACB4E9E8 00ABEB0E 18882C37 5360FFB3


------------

  BCC

  IV is
                      00000002 00000000 00000000 00000000


  IV || S is
                                           00000002 00000000
    00000000 00000000 00000060 00000030 C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
    E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000


temp is
    A77C22F8 F701BD5D F0E36418 04462F38 ACB4E9E8 00ABEB0E
    18882C37 5360FFB3 46C9AE43 4389D41E 050AE515 E7C05BA3


------------
```

```
Key is
                                          A77C22F8 F701BD5D
    F0E36418 04462F38 ACB4E9E8 00ABEB0E 18882C37 5360FFB3


X is
                     46C9AE43 4389D41E 050AE515 E7C05BA3


------------

  BlockEncrypt

  Key is
                                          A77C22F8 F701BD5D
    F0E36418 04462F38 ACB4E9E8 00ABEB0E 18882C37 5360FFB3


  X is
                     46C9AE43 4389D41E 050AE515 E7C05BA3


  X = BlockEncrypt(Key, X) is
                     4462618D 4FA2FD6D 5B0312B1 A8BA3E8F


  temp is
                     4462618D 4FA2FD6D 5B0312B1 A8BA3E8F


------------

  BlockEncrypt

  Key is
                                          A77C22F8 F701BD5D
    F0E36418 04462F38 ACB4E9E8 00ABEB0E 18882C37 5360FFB3


  X is
                     4462618D 4FA2FD6D 5B0312B1 A8BA3E8F


  X = BlockEncrypt(Key, X) is
                     6909E1FF 1DF7D047 788FE17E 615BE531
```

```
      temp is
                                              4462618D 4FA2FD6D
        5B0312B1 A8BA3E8F 6909E1FF 1DF7D047 788FE17E 615BE531


    ------------

      BlockEncrypt

      Key is
                                              A77C22F8 F701BD5D
        F0E36418 04462F38 ACB4E9E8 00ABEB0E 18882C37 5360FFB3


      X is
                           6909E1FF 1DF7D047 788FE17E 615BE531


      X = BlockEncrypt(Key, X) is
                           7F99849D D5C2442E BB6CCCC9 4FBAB255


      temp is
        4462618D 4FA2FD6D 5B0312B1 A8BA3E8F 6909E1FF 1DF7D047
        788FE17E 615BE531 7F99849D D5C2442E BB6CCCC9 4FBAB255


      requested_bits is
        4462618D 4FA2FD6D 5B0312B1 A8BA3E8F 6909E1FF 1DF7D047
        788FE17E 615BE531 7F99849D D5C2442E BB6CCCC9 4FBAB255


---------------------------

  Update

    provided_data is
        4462618D 4FA2FD6D 5B0312B1 A8BA3E8F 6909E1FF 1DF7D047
        788FE17E 615BE531 7F99849D D5C2442E BB6CCCC9 4FBAB255


    ------------

      While loop
```

```
  Key is
                                          30B27377 DE24BD94
    8F2037BC BA1BB65B EAF4E2D2 46CFE777 0F27D16B 89069C3A


  V is
                      0592090E A1D6CB56 93F23B12 1BB07AC3


  output_block is
                      49724416 6965665C E658C814 AE95122A


  temp is
                      49724416 6965665C E658C814 AE95122A


------------

  While loop

  Key is
                                          30B27377 DE24BD94
    8F2037BC BA1BB65B EAF4E2D2 46CFE777 0F27D16B 89069C3A


  V is
                      0592090E A1D6CB56 93F23B12 1BB07AC4


  output_block is
                      DE01CB7F A3BD14EF 0F00EEFA 7DCA0699


  temp is
                                          49724416 6965665C
    E658C814 AE95122A DE01CB7F A3BD14EF 0F00EEFA 7DCA0699


------------

  While loop

  Key is
                                          30B27377 DE24BD94
    8F2037BC BA1BB65B EAF4E2D2 46CFE777 0F27D16B 89069C3A
```

```
      V is
                          0592090E A1D6CB56 93F23B12 1BB07AC5


      output_block is
                          21AFEF12 119A1B34 E5DF1581 62CC7F6E


      temp is
        49724416 6965665C E658C814 AE95122A DE01CB7F A3BD14EF
        0F00EEFA 7DCA0699 21AFEF12 119A1B34 E5DF1581 62CC7F6E


    temp XOR provided_data is
        0D10259B 26C79B31 BD5BDAA5 062F2CA5 B7082A80 BE4AC4A8
        778F0F84 1C91E3A8 5E366B8F C4585F1A 5EB3D948 2D76CD3B


    Key is
                                           0D10259B 26C79B31
        BD5BDAA5 062F2CA5 B7082A80 BE4AC4A8 778F0F84 1C91E3A8


    V is
                          5E366B8F C4585F1A 5EB3D948 2D76CD3B


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
```

```
------------

  While loop

  Key is
                                          0D10259B 26C79B31
    BD5BDAA5 062F2CA5 B7082A80 BE4AC4A8 778F0F84 1C91E3A8


  V is
                      5E366B8F C4585F1A 5EB3D948 2D76CD3E


  output_block is
                      A12D1656 186D2BC2 AF8837A1 F5F41C75


  temp is
                      A12D1656 186D2BC2 AF8837A1 F5F41C75


------------

  While loop

  Key is
                                          0D10259B 26C79B31
    BD5BDAA5 062F2CA5 B7082A80 BE4AC4A8 778F0F84 1C91E3A8


  V is
                      5E366B8F C4585F1A 5EB3D948 2D76CD3F


  output_block is
                      6832B24D 2F4EEB19 EFBD0618 14F0B45D


  temp is
                                          A12D1656 186D2BC2
    AF8837A1 F5F41C75 6832B24D 2F4EEB19 EFBD0618 14F0B45D


------------

  While loop
```

```
      Key is
                                              0D10259B 26C79B31
        BD5BDAA5 062F2CA5 B7082A80 BE4AC4A8 778F0F84 1C91E3A8


      V is
                           5E366B8F C4585F1A 5EB3D948 2D76CD40


      output_block is
                           DB10B248 786AD0CA EB9C1B03 60D2DF4C


      temp is
        A12D1656 186D2BC2 AF8837A1 F5F41C75 6832B24D 2F4EEB19
        EFBD0618 14F0B45D DB10B248 786AD0CA EB9C1B03 60D2DF4C


    temp XOR provided_data is
        A12D1656 186D2BC2 AF8837A1 F5F41C75 6832B24D 2F4EEB19
        EFBD0618 14F0B45D DB10B248 786AD0CA EB9C1B03 60D2DF4C


    Key is
                                              A12D1656 186D2BC2
        AF8837A1 F5F41C75 6832B24D 2F4EEB19 EFBD0618 14F0B45D


    V is
                           DB10B248 786AD0CA EB9C1B03 60D2DF4C


rnd_val is
                                              738E99C9 5AF59519
        AAD37FF3 D5180986 ADEBAB6E 95836725 097E50A8 D1D0BD28
```

```
###############################################################

DualEC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    Nonce =
                                           20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F


    nonce is
                                           20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"
```

```
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                      01 00000100
        00010203 04050607 08090A0B 0C0D0E0F 20212223 24252627


    Hash(counter||no_of_bits_to_return||input_string) is
                                             F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


    temp =
                                             F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


s is
                                             F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


------------------------------------------------------------

First call to Generate

************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
  ------------
  i=0
  t is
                                             F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A
```

```
s is
                                              5FFEFE90 005C75B2
      CBEF01A9 A3887F7A 80430A4F 6FF0A196 28CE1610 96350C75


r is
                                              C0CCFF51 63C388F7
      91E96F10 52D5C8F0 BD6FBF71 44839C48 90FF8548 7C5C1270


------------
tmp is
                                                  FF51 63C388F7
      91E96F10 52D5C8F0 BD6FBF71 44839C48 90FF8548 7C5C1270


------------
i=1
t is
                                              5FFEFE90 005C75B2
      CBEF01A9 A3887F7A 80430A4F 6FF0A196 28CE1610 96350C75


s is
                                              11C42D2D 4A98B054
      AE25746E DA4E147A 9308E68B B91B7788 BA140B8B E18CEA1A


r is
                                              DDE82E4C 9849AF51
      8AE68DEB 14D3A627 02BBDE4B 98AB2117 65FD87AC A12FC2A6


------------
tmp is
                                  FF5163C3 88F791E9 6F1052D5
      C8F0BD6F BF714483 9C4890FF 85487C5C 12702E4C 9849AF51
      8AE68DEB 14D3A627 02BBDE4B 98AB2117 65FD87AC A12FC2A6


------------
s is
                                              DDBD9639 34E3E942
      8CCC5C84 175C70D6 4D31CF0B E3CE141D 61F3D297 D87CF0B4
```

```
------------------------------------------------------------

Second call to Generate

************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
  ------------
  i=0
  t is
                                              DDBD9639 34E3E942
        8CCC5C84 175C70D6 4D31CF0B E3CE141D 61F3D297 D87CF0B4


  s is
                                              2B79FE2B F483248C
        E845B587 11469A0B 01A4B263 F1565570 34D2B409 B6CEDA66


  r is
                                              6F0B9A0A 11F2DFB8
        8F726055 9DD8DA61 34EB2B34 CC0415FA 8FD0474D B6B85E1A


  ------------
  tmp is
                                                  9A0A 11F2DFB8
        8F726055 9DD8DA61 34EB2B34 CC0415FA 8FD0474D B6B85E1A


  ------------
  i=1
  t is
                                              2B79FE2B F483248C
        E845B587 11469A0B 01A4B263 F1565570 34D2B409 B6CEDA66


  s is
                                              38BB1AF3 9E3826B2
        EE6BAA80 93ADD16E 4035E2B1 A843CCF8 9DA4D5B4 29B2E571
```

```
  r is
                                              307E0838 5F41B435
        DF81296B 1B4EDF66 E0107C08 44E3D28A 89B05046 B89177F2


  ------------
  tmp is
                                    9A0A11F2 DFB88F72 60559DD8
        DA6134EB 2B34CC04 15FA8FD0 474DB6B8 5E1A0838 5F41B435
        DF81296B 1B4EDF66 E0107C08 44E3D28A 89B05046 B89177F2


  ------------
  s is
                                              73722037 B3B07CE9
        0A55ADB8 612AB20E 0525F499 7D0207C7 813A2B31 9E7A2DA6


rnd_val is
                                    9A0A11F2 DFB88F72 60559DD8
        DA6134EB 2B34CC04 15FA8FD0 474DB6B8 5E1A0838 5F41B435
        DF81296B 1B4EDF66 E0107C08 44E3D28A 89B05046 B89177F2


################################################################

DualEC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
```

```
    Nonce =
                                            20212223 24252627

    PersonalizationString = <empty>

    AdditionalInput1  =
                          60616263 64656667 68696A6B 6C6D6E6F

    AdditionalInput2  =
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF

##################################################################

******************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F

    nonce is
                                            20212223 24252627

    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Hash_df()
  --------------------------
    no_of_bits_to_return = 256

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                    01 00000100
        00010203 04050607 08090A0B 0C0D0E0F 20212223 24252627

    Hash(counter||no_of_bits_to_return||input_string) is
```

```
                                                F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


    temp =
                                                F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


s is
                                                F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


-------------------------------------------------------------

First call to Generate

*************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F


    requested_number_of_bits is 480
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000100 60616263 64656667 68696A6B 6C6D6E6F


    Hash(counter||no_of_bits_to_return||input_string) is
                                                1971EF06 D6518B33
        336E7701 1D9E34D9 ECE74E43 EC2BE92C 053526A8 B8807FCA


    temp =
                                                1971EF06 D6518B33
```

```
      336E7701 1D9E34D9 ECE74E43 EC2BE92C 053526A8 B8807FCA


------------
i=0
t is
                                          EC8C589E 6484D9BB
      D1B2C4DC 11289A89 9759475A A1931D5E 35B026DB AA30E380


s is
                                          5F064198 5EA2043C
      DEBD8380 852676B3 8BAA49B2 C85B6821 7C746DE2 4F03E627


r is
                                          2B1FC08E 954FCD48
      6D0B0934 A0236692 AC705A83 5D1A3C94 D2ACD468 4AB26E97


------------
tmp is
                                              C08E 954FCD48
      6D0B0934 A0236692 AC705A83 5D1A3C94 D2ACD468 4AB26E97


------------
i=1
t is
                                          5F064198 5EA2043C
      DEBD8380 852676B3 8BAA49B2 C85B6821 7C746DE2 4F03E627


s is
                                          5BE1CB12 82E9CDC9
      3DD30A8A F23ECD4F 36591ADA 96DF76A8 1314226D BFA18A92


r is
                                          90108D7D 42E73CC0
      6D6EC147 2C63E51B ED7F7151 8395836E 2052BBD7 3A20CABB


------------
tmp is
                                C08E954F CD486D0B 0934A023
```

```
        6692AC70 5A835D1A 3C94D2AC D4684AB2 6E978D7D 42E73CC0
        6D6EC147 2C63E51B ED7F7151 8395836E 2052BBD7 3A20CABB


  ------------
  s is
                                              31406B18 A2764288
        6EC67852 835838D9 FC9FD279 1F9960B9 809DF42B B52BAC5C


---------------------------------------------------------------

Second call to Generate

***************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    requested_number_of_bits is 480
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000100 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    Hash(counter||no_of_bits_to_return||input_string) is
                                              27881CBD D6B3C655
        5FE3EF70 59B5FEFC E86DF84C 255D832A A1E1091C 79D9FFF9


    temp =
                                              27881CBD D6B3C655
        5FE3EF70 59B5FEFC E86DF84C 255D832A A1E1091C 79D9FFF9


  ------------
```

```
i=0
t is
                                          16C877A5 74C584DD
      31259722 DAEDC625 14F22A35 3AC4E393 217CFD37 CCF253A5


s is
                                          36C76642 BD5B0F60
      73FD4784 18C48BD4 ABB6AC5D 252C9649 6DAEEA58 48060F9D


r is
                                          31081D76 DEE36FCC
      5F9478C1 12EAFA1C 4CCD0635 435A6F3A 247A3BA3 849790B5


------------
tmp is
                                              1D76 DEE36FCC
      5F9478C1 12EAFA1C 4CCD0635 435A6F3A 247A3BA3 849790B5


------------
i=1
t is
                                          36C76642 BD5B0F60
      73FD4784 18C48BD4 ABB6AC5D 252C9649 6DAEEA58 48060F9D


s is
                                          D76BD5B5 4F2B26EB
      2EE4A79C 53AF57C4 E73B3F2B CD9E2430 C82DD251 8125B46B


r is
                                          15CA2450 70E95C1A
      67BE7A39 BFB213F2 C0EFCC17 1A3253DA 6D54DA43 62EA2099


------------
tmp is
                                1D76DEE3 6FCC5F94 78C112EA
      FA1C4CCD 0635435A 6F3A247A 3BA38497 90B52450 70E95C1A
      67BE7A39 BFB213F2 C0EFCC17 1A3253DA 6D54DA43 62EA2099
```

```
  ------------
  s is
                                              6CB3B3D3 09120EEB
        251C808B A104D660 99C8B794 B9ED537F B79BEC24 F935BCB3


rnd_val is
                                    1D76DEE3 6FCC5F94 78C112EA
        FA1C4CCD 0635435A 6F3A247A 3BA38497 90B52450 70E95C1A
        67BE7A39 BFB213F2 C0EFCC17 1A3253DA 6D54DA43 62EA2099


################################################################

DualEC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    Nonce =
                                              20212223 24252627


    PersonalizationString =
                          40414243 44454647 48494A4B 4C4D4E4F


    AdditionalInput = <empty>

################################################################

****************************************************************
```

```
DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                           00010203 04050607 08090A0B 0C0D0E0F


    nonce is
                                               20212223 24252627


    personal_str is
                           40414243 44454647 48494A4B 4C4D4E4F


    prediction_resistance_flag = "No PredictionResistance"

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000100 00010203 04050607 08090A0B 0C0D0E0F
          20212223 24252627 40414243 44454647 48494A4B 4C4D4E4F


    Hash(counter||no_of_bits_to_return||input_string) is
                                               48306692 AF00A3F6
          1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


    temp =
                                               48306692 AF00A3F6
          1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


s is
                                               48306692 AF00A3F6
          1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


-------------------------------------------------------------
```

```
First call to Generate

****************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
  ------------
  i=0
  t is
                                                48306692 AF00A3F6
        1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


  s is
                                                07220A43 46B8BDCB
        FF430F10 82A022FA 98C76EF1 4CB72ABB AED09239 8979075C


  r is
                                                E3413AB0 95CC493A
        8730D70D E923108B 2E471079 9044FFC2 7D0A1156 250DDF97


  ------------
  tmp is
                                                    3AB0 95CC493A
        8730D70D E923108B 2E471079 9044FFC2 7D0A1156 250DDF97


  ------------
  i=1
  t is
                                                07220A43 46B8BDCB
        FF430F10 82A022FA 98C76EF1 4CB72ABB AED09239 8979075C


  s is
                                                DBFB35E7 65853122
        DBC73725 0E8CA258 2EE963BF 558623F3 FE296EB2 58D2B212


  r is
```

```
                                              8821E8B0 5ACE055E
      49F3E3F5 B928CCD1 8317A3E6 8FCB0B6F 0459ADF9 ECF79C87


  ------------
  tmp is
                                    3AB095CC 493A8730 D70DE923
      108B2E47 10799044 FFC27D0A 1156250D DF97E8B0 5ACE055E
      49F3E3F5 B928CCD1 8317A3E6 8FCB0B6F 0459ADF9 ECF79C87


  ------------
  s is
                                              51338CAF 4ACC90DB
      2AB01EFA 386BCD9A A3D218AF 38A5F953 87606B24 75E70E3A


----------------------------------------------------------------

Second call to Generate

****************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
  ------------
  i=0
  t is
                                              51338CAF 4ACC90DB
      2AB01EFA 386BCD9A A3D218AF 38A5F953 87606B24 75E70E3A


  s is
                                              9519EAFE 8981CE23
      1073C826 1BCCD88B 69E75951 F2AF69D6 629B4541 01D8BFAD


  r is
                                              A83D7B90 2FC35B0A
      F50F57F8 822936D0 8A96E41B 16967C6B 1AA0BC05 032F0D53


  ------------
```

```
  tmp is
                                                    7B90 2FC35B0A
        F50F57F8 822936D0 8A96E41B 16967C6B 1AA0BC05 032F0D53


  ------------
  i=1
  t is
                                                9519EAFE 8981CE23
        1073C826 1BCCD88B 69E75951 F2AF69D6 629B4541 01D8BFAD


  s is
                                                FD5E645A 56976F29
        75742607 B18FA7E1 30192BCD E1DE9430 CB0BA656 1B41A231


  r is
                                                2789919D C587B664
        C883E2FE 8F394800 2FCD8BCB FC4706BC AA2075EF 6BF41167


  ------------
  tmp is
                                   7B902FC3 5B0AF50F 57F88229
        36D08A96 E41B1696 7C6B1AA0 BC05032F 0D53919D C587B664
        C883E2FE 8F394800 2FCD8BCB FC4706BC AA2075EF 6BF41167


  ------------
  s is
                                                5C4B76D2 04F17E37
        C01EA94A D09DE5A4 6BE71997 328E1C7E 85FC290B CF435505


rnd_val is
                                   7B902FC3 5B0AF50F 57F88229
        36D08A96 E41B1696 7C6B1AA0 BC05032F 0D53919D C587B664
        C883E2FE 8F394800 2FCD8BCB FC4706BC AA2075EF 6BF41167


##############################################################

DualEC_DRBG

    Requested Security Strength = 128
```

```
    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    Nonce =
                                            20212223 24252627


    PersonalizationString =
                          40414243 44454647 48494A4B 4C4D4E4F


    AdditionalInput1  =
                          60616263 64656667 68696A6B 6C6D6E6F


    AdditionalInput2  =
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


##################################################################

******************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F


    nonce is
                                            20212223 24252627
```

```
    personal_str is
                          40414243 44454647 48494A4B 4C4D4E4F


    prediction_resistance_flag = "No PredictionResistance"

  Hash_df()
  ----------------------------
    no_of_bits_to_return = 256

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000100 00010203 04050607 08090A0B 0C0D0E0F
          20212223 24252627 40414243 44454647 48494A4B 4C4D4E4F


    Hash(counter||no_of_bits_to_return||input_string) is
                                              48306692 AF00A3F6
          1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


    temp =
                                              48306692 AF00A3F6
          1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


s is
                                              48306692 AF00A3F6
          1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


---------------------------------------------------------------

First call to Generate

***************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F
```

```
  requested_number_of_bits is 480
Hash_df()
----------------------------
  no_of_bits_to_return = 256

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
           01 00000100 60616263 64656667 68696A6B 6C6D6E6F


  Hash(counter||no_of_bits_to_return||input_string) is
                                              1971EF06 D6518B33
      336E7701 1D9E34D9 ECE74E43 EC2BE92C 053526A8 B8807FCA


  temp =
                                              1971EF06 D6518B33
      336E7701 1D9E34D9 ECE74E43 EC2BE92C 053526A8 B8807FCA


------------
i=0
t is
                                              51418994 795128C5
      22EAF14C FC1DCE68 0A8B490A 70E67165 BA4DDEDB C0DEA379


s is
                                              28C1806A FCF56F49
      08362DB4 0FA1245B 9E998CE3 0AE2A5DA F57E4D3C 2C44ECEE


r is
                                              27423B68 A1D95ED0
      312150AC 19911897 80F37EC5 0E75249F 915CD806 BBA0C44F


------------
tmp is
                                                  3B68 A1D95ED0
      312150AC 19911897 80F37EC5 0E75249F 915CD806 BBA0C44F
```

```
  ------------
  i=1
  t is
                                              28C1806A FCF56F49
        08362DB4 0FA1245B 9E998CE3 0AE2A5DA F57E4D3C 2C44ECEE


  s is
                                              7B37CB05 75C300B3
        4928C5F9 FD1237E6 FCEE99FC 0D4FD7D6 071DB5DD 93D20B31


  r is
                                              E9259E3A 919B2390
        805E1E90 C1D2D1C8 23B17B96 DB44535B 72E0CFB6 2723529D


  ------------
  tmp is
                                    3B68A1D9 5ED03121 50AC1991
        189780F3 7EC50E75 249F915C D806BBA0 C44F9E3A 919B2390
        805E1E90 C1D2D1C8 23B17B96 DB44535B 72E0CFB6 2723529D


  ------------
  s is
                                              8E0D63D9 788C13A4
        5615F270 2D9DA602 D8BA211E 6E5E8586 CB3822BB ABBCC7DD


------------------------------------------------------------

Second call to Generate

************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
                           A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    requested_number_of_bits is 480
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256
```

```
  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
           01 00000100 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


  Hash(counter||no_of_bits_to_return||input_string) is
                                              27881CBD D6B3C655
      5FE3EF70 59B5FEFC E86DF84C 255D832A A1E1091C 79D9FFF9


  temp =
                                              27881CBD D6B3C655
      5FE3EF70 59B5FEFC E86DF84C 255D832A A1E1091C 79D9FFF9


------------
i=0
t is
                                              A9857F64 AE3FD5F1
      09F61D00 742858FE 30D7D952 4B0306AC 6AD92BA7 D2653824


s is
                                              C5EF4CF0 C33DD22F
      204FD138 282533DD 3B9D7812 167899C8 8E71B22C 78602C57


r is
                                              A676250B 933475E3
      BD4FC85D 97FD7978 34B599DE DEDF8B6F 15474E1F 31B4AF21


------------
tmp is
                                                  250B 933475E3
      BD4FC85D 97FD7978 34B599DE DEDF8B6F 15474E1F 31B4AF21


------------
i=1
t is
                                              C5EF4CF0 C33DD22F
```

```
        204FD138 282533DD 3B9D7812 167899C8 8E71B22C 78602C57


  s is
                                                DA9644BD 977A1508
        7F58F877 1A886253 A32E8B5D 9855DC48 460AF031 BAC3896C


  r is
                                                8D0F5CFA 7A8C0A02
        96A2E374 B3886BB0 CC7E49DB B1932456 4B451E64 F12864F9


  ------------
  tmp is
                                   250B9334 75E3BD4F C85D97FD
        797834B5 99DEDEDF 8B6F1547 4E1F31B4 AF215CFA 7A8C0A02
        96A2E374 B3886BB0 CC7E49DB B1932456 4B451E64 F12864F9


  ------------
  s is
                                                A2F2449A CA6D389C
        D8DAD909 D8AF9818 0F9D97B1 9EC14FF8 03076E87 3D1C9115


rnd_val is
                                   250B9334 75E3BD4F C85D97FD
        797834B5 99DEDEDF 8B6F1547 4E1F31B4 AF215CFA 7A8C0A02
        96A2E374 B3886BB0 CC7E49DB B1932456 4B451E64 F12864F9


##############################################################

DualEC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                           00010203 04050607 08090A0B 0C0D0E0F


    EntropyInput1 (for Reseed1) =
```

```
                          80818283 84858687 88898A8B 8C8D8E8F

    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF

    Nonce =
                                               20212223 24252627

    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F

    nonce is
                                               20212223 24252627

    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Hash_df()
  ----------------------------
    no_of_bits_to_return = 256

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                        01 00000100
        00010203 04050607 08090A0B 0C0D0E0F 20212223 24252627
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                                                F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


    temp =
                                                F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


s is
                                                F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


------------------------------------------------------------

First call to Generate

************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
Generate FAILED: Reseed is required
************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                           80818283 84858687 88898A8B 8C8D8E8F


    additional_input is  <empty>

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
```

```
                                                    01 00000100
        F5FDB798 B2D55288 E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472
        30850073 12B09C4A 80818283 84858687 88898A8B 8C8D8E8F


    Hash(counter||no_of_bits_to_return||input_string) is
                                                5B1DEA76 192287BB
        9C8157EA 5260A02D F4EFD5AB 0DF0948D 63780564 5554479E


    temp =
                                                5B1DEA76 192287BB
        9C8157EA 5260A02D F4EFD5AB 0DF0948D 63780564 5554479E


s is
                                                5B1DEA76 192287BB
        9C8157EA 5260A02D F4EFD5AB 0DF0948D 63780564 5554479E


**************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
  ------------
  i=0
  t is
                                                5B1DEA76 192287BB
        9C8157EA 5260A02D F4EFD5AB 0DF0948D 63780564 5554479E


  s is
                                                47F46DB7 B18F1D4C
        041140C3 BC8767AD B9103687 3FB275D2 77FE728B BAE1F584


  r is
                                                A5438C77 288EDBEA
        9A742464 F78D55E3 3593C1BF 5F9D8CD8 609D6D53 BAC4E4B4


  ------------
  tmp is
```

```
                                                    8C77 288EDBEA
        9A742464 F78D55E3 3593C1BF 5F9D8CD8 609D6D53 BAC4E4B4


  ------------
  i=1
  t is
                                                47F46DB7 B18F1D4C
        041140C3 BC8767AD B9103687 3FB275D2 77FE728B BAE1F584


  s is
                                                DF51738B BB438BF6
        B1FAA44D 1E561ACD A0B7EF6B 36C402CD 03CE82C0 77CE330F


  r is
                                                25F22252 A227A99B
        AD0F2358 B05955CD 35723B54 9401C71C 9C1F32F8 A2018E24


  ------------
  tmp is
                                    8C77288E DBEA9A74 2464F78D
        55E33593 C1BF5F9D 8CD8609D 6D53BAC4 E4B42252 A227A99B
        AD0F2358 B05955CD 35723B54 9401C71C 9C1F32F8 A2018E24


  ------------
  s is
                                                B2142494 19F0F84A
        F4D54B42 9509CBA8 F5835661 70A3710B 1FF7EAE5 64504A63


------------------------------------------------------------

Second call to Generate

************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
Generate FAILED: Reseed is required
```

```
***************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                           C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    additional_input is  <empty>

  Hash_df()
  ----------------------------
    no_of_bits_to_return = 256

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                      01 00000100
        B2142494 19F0F84A F4D54B42 9509CBA8 F5835661 70A3710B
        1FF7EAE5 64504A63 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    Hash(counter||no_of_bits_to_return||input_string) is
                                               6BA22FDD 08909D88
        5A6A3B1D 6D1632C0 7AF24024 2935D4D9 55103EB1 5BB92E04


    temp =
                                               6BA22FDD 08909D88
        5A6A3B1D 6D1632C0 7AF24024 2935D4D9 55103EB1 5BB92E04


s is
                                               6BA22FDD 08909D88
        5A6A3B1D 6D1632C0 7AF24024 2935D4D9 55103EB1 5BB92E04


***************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
```

```
------------
i=0
t is
                                          6BA22FDD 08909D88
      5A6A3B1D 6D1632C0 7AF24024 2935D4D9 55103EB1 5BB92E04


s is
                                          B22FAD78 8AF6890F
      D4322A2B BC14A063 91F983AD DD3C56CA 7C04799D D99A18F0


r is
                                          3BA856EC A61C64F6
      9C1C232E 992623C7 1418BD0B 96D78311 8FAAD94A 09E3A9DB


------------
tmp is
                                             56EC A61C64F6
      9C1C232E 992623C7 1418BD0B 96D78311 8FAAD94A 09E3A9DB


------------
i=1
t is
                                          B22FAD78 8AF6890F
      D4322A2B BC14A063 91F983AD DD3C56CA 7C04799D D99A18F0


s is
                                          5DCD988F 0DC87671
      E4907A4A 52E0A024 B2F88A3F ADEC28B4 28DD2B57 ACD478E1


r is
                                          16E974D1 5E805BA7
      F1462599 5CA77612 B2EF7A05 863699EC BABF70D3 D422C014


------------
tmp is
                                56ECA61C 64F69C1C 232E9926
      23C71418 BD0B96D7 83118FAA D94A09E3 A9DB74D1 5E805BA7
      F1462599 5CA77612 B2EF7A05 863699EC BABF70D3 D422C014
```

```
  ------------
  s is
                                          A4E6B504 E112C915
        DEF15EB4 EB78EB3E 722E248E 82B9F810 C666C984 E43F0FCF


rnd_val is
                                  56ECA61C 64F69C1C 232E9926
        23C71418 BD0B96D7 83118FAA D94A09E3 A9DB74D1 5E805BA7
        F1462599 5CA77612 B2EF7A05 863699EC BABF70D3 D422C014


################################################################

DualEC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    Nonce =
                                          20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput1  =
                          60616263 64656667 68696A6B 6C6D6E6F


    AdditionalInput2  =
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
```

```
################################################################

****************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                           00010203 04050607 08090A0B 0C0D0E0F


    nonce is
                                             20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Hash_df()
  --------------------------
    no_of_bits_to_return = 256

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                      01 00000100
        00010203 04050607 08090A0B 0C0D0E0F 20212223 24252627


    Hash(counter||no_of_bits_to_return||input_string) is
                                             F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


    temp =
                                             F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


s is
                                             F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A
```

```
------------------------------------------------------------

First call to Generate

************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F


    requested_number_of_bits is 480
Generate FAILED: Reseed is required
************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                          80818283 84858687 88898A8B 8C8D8E8F


    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F


  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000100 F5FDB798 B2D55288 E2DCB3DD 0CB6AE50
        7BBE0919 4DB8F472 30850073 12B09C4A 80818283 84858687
        88898A8B 8C8D8E8F 60616263 64656667 68696A6B 6C6D6E6F


    Hash(counter||no_of_bits_to_return||input_string) is
                                              8100942E F294225C
        24D0CCF5 5840770F 814EC45C F6A0BB36 28263FE8 099B1D1F
```

```
    temp =
                                                8100942E F294225C
        24D0CCF5 5840770F 814EC45C F6A0BB36 28263FE8 099B1D1F


s is
                                                8100942E F294225C
        24D0CCF5 5840770F 814EC45C F6A0BB36 28263FE8 099B1D1F


****************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
  ------------
  i=0
  t is
                                                8100942E F294225C
        24D0CCF5 5840770F 814EC45C F6A0BB36 28263FE8 099B1D1F


  s is
                                                60D7E8F7 CB33C5A5
        2D090E43 BD26A3EA 5764CFB2 E6CF4743 0AF74DF5 A28AAC59


  r is
                                                5B1FA5C3 97DFEB54
        0E86F047 0E9625D5 C5AC2D50 016FB201 E8DF574F 2201DFBB


  ------------
  tmp is
                                                    A5C3 97DFEB54
        0E86F047 0E9625D5 C5AC2D50 016FB201 E8DF574F 2201DFBB


  ------------
  i=1
  t is
                                                60D7E8F7 CB33C5A5
        2D090E43 BD26A3EA 5764CFB2 E6CF4743 0AF74DF5 A28AAC59
```

```
  s is
                                              06288C70 188402B0
        14887772 4B477EBD 40E62110 6270CBA6 5792C2D2 847C86AD


  r is
                                              B38242A7 99FEB9E2
        38AAD301 A4933822 50EEE60D 2E2927E5 00E848E5 7535ABD1


  ------------
  tmp is
                                    A5C397DF EB540E86 F0470E96
        25D5C5AC 2D50016F B201E8DF 574F2201 DFBB42A7 99FEB9E2
        38AAD301 A4933822 50EEE60D 2E2927E5 00E848E5 7535ABD1


  ------------
  s is
                                              93EF7B5F 358590E4
        E6DF5A98 94678FEE 009123B7 88483A68 7EE6D629 2928B3DD


----------------------------------------------------------------

Second call to Generate

****************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    requested_number_of_bits is 480
Generate FAILED: Reseed is required
****************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
```

```
    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


  Hash_df()
  --------------------------
    no_of_bits_to_return = 256

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000100 93EF7B5F 358590E4 E6DF5A98 94678FEE
          009123B7 88483A68 7EE6D629 2928B3DD C0C1C2C3 C4C5C6C7
          C8C9CACB CCCDCECF A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    Hash(counter||no_of_bits_to_return||input_string) is
                                                 186A98AB 693C65C1
          D5196A10 703A89C9 5D1E25C8 B21849D2 8D09D987 C2C6BA44


    temp =
                                                 186A98AB 693C65C1
          D5196A10 703A89C9 5D1E25C8 B21849D2 8D09D987 C2C6BA44


s is
                                                 186A98AB 693C65C1
          D5196A10 703A89C9 5D1E25C8 B21849D2 8D09D987 C2C6BA44


**************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
  ------------
  i=0
  t is
                                                 186A98AB 693C65C1
          D5196A10 703A89C9 5D1E25C8 B21849D2 8D09D987 C2C6BA44
```

```
s is
                                          3980714F B4C5ED77
      5AF5E80E 5B1D3EB2 D8018EDE 95222FAD 2C203151 D7E2CC8F


r is
                                          222ABF98 94630BEB
      AF0A0EDF E726285E B055FD2E D678B766 73803DD3 27F49DBE


------------
tmp is
                                              BF98 94630BEB
      AF0A0EDF E726285E B055FD2E D678B766 73803DD3 27F49DBE


------------
i=1
t is
                                          3980714F B4C5ED77
      5AF5E80E 5B1D3EB2 D8018EDE 95222FAD 2C203151 D7E2CC8F


s is
                                          A99DFD75 FEA1F1EA
      03A4937F A040781B 06568FA5 46B0C859 F246C3BE 02910AE0


r is
                                          AE6BDE87 D3E447A6
      EB73B5D5 C52A4007 8132677F 412E9E7D E32B9B1C B32421B9


------------
tmp is
                                 BF989463 0BEBAF0A 0EDFE726
      285EB055 FD2ED678 B7667380 3DD327F4 9DBEDE87 D3E447A6
      EB73B5D5 C52A4007 8132677F 412E9E7D E32B9B1C B32421B9


------------
s is
                                          CE70C30B ECC61502
      548EE461 F9A4F714 433B4A07 541F6823 44FBEF3A 9E1A9827
```

```
rnd_val is
                                  BF989463 0BEBAF0A 0EDFE726
        285EB055 FD2ED678 B7667380 3DD327F4 9DBEDE87 D3E447A6
        EB73B5D5 C52A4007 8132677F 412E9E7D E32B9B1C B32421B9


################################################################

DualEC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    Nonce =
                                           20212223 24252627


    PersonalizationString =
                          40414243 44454647 48494A4B 4C4D4E4F


    AdditionalInput = <empty>

################################################################

****************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
```

```
                          00010203 04050607 08090A0B 0C0D0E0F

    nonce is
                                            20212223 24252627

    personal_str is
                          40414243 44454647 48494A4B 4C4D4E4F

    prediction_resistance_flag = "PredictionResistance"

  Hash_df()
  ----------------------------
    no_of_bits_to_return = 256

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000100 00010203 04050607 08090A0B 0C0D0E0F
          20212223 24252627 40414243 44454647 48494A4B 4C4D4E4F


    Hash(counter||no_of_bits_to_return||input_string) is
                                            48306692 AF00A3F6
          1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


    temp =
                                            48306692 AF00A3F6
          1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


s is
                                            48306692 AF00A3F6
          1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


---------------------------------------------------------------

First call to Generate

***************************************************************
```

```
DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
Generate FAILED: Reseed is required
************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                          80818283 84858687 88898A8B 8C8D8E8F


    additional_input is  <empty>

  Hash_df()
  --------------------------
    no_of_bits_to_return = 256

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                    01 00000100
        48306692 AF00A3F6 1184864D E183FAB1 E66C0749 9CCD9849
        BF78F873 785EDCB3 80818283 84858687 88898A8B 8C8D8E8F


    Hash(counter||no_of_bits_to_return||input_string) is
                                             B8F6A9DD 0AB21123
        FCC40457 1E90FECF AD3F2412 41C15577 DBA50C9F A888E37B


    temp =
                                             B8F6A9DD 0AB21123
        FCC40457 1E90FECF AD3F2412 41C15577 DBA50C9F A888E37B


s is
                                             B8F6A9DD 0AB21123
        FCC40457 1E90FECF AD3F2412 41C15577 DBA50C9F A888E37B
```

```
**************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
  ------------
  i=0
  t is
                                                B8F6A9DD 0AB21123
        FCC40457 1E90FECF AD3F2412 41C15577 DBA50C9F A888E37B


  s is
                                                1C8D0AC6 6A850666
        4E70CC42 23F109BC D3B1DA1F 531D9E50 92D9C5A0 40781E73


  r is
                                                FCF84A5C 82ADD86A
        FFB9F9FD 7597BC59 532F767E ED26547E EB072586 BBF9D540


  ------------
  tmp is
                                                    4A5C 82ADD86A
        FFB9F9FD 7597BC59 532F767E ED26547E EB072586 BBF9D540


  ------------
  i=1
  t is
                                                1C8D0AC6 6A850666
        4E70CC42 23F109BC D3B1DA1F 531D9E50 92D9C5A0 40781E73


  s is
                                                32F03EEE 59A6862A
        88FC0490 49F2695B F6DD969D 10758C41 79DC8269 5EE19749


  r is
                                                6D18F5AC 80C2F1D9
        167CA3AD A2ABFF91 96501175 9F68581C B49F3DD9 01D9B16F
```

```
  ------------
  tmp is
                                  4A5C82AD D86AFFB9 F9FD7597
        BC59532F 767EED26 547EEB07 2586BBF9 D540F5AC 80C2F1D9
        167CA3AD A2ABFF91 96501175 9F68581C B49F3DD9 01D9B16F


  ------------
  s is
                                              B9B256D0 F088A9D2
        CDE0CD8D C50D3F2E D5BDC632 14352901 2FF690C6 36797F58


----------------------------------------------------------------

Second call to Generate

****************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
Generate FAILED: Reseed is required
****************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                           C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    additional_input is  <empty>

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                    01 00000100
```

```
        B9B256D0 F088A9D2 CDE0CD8D C50D3F2E D5BDC632 14352901
        2FF690C6 36797F58 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    Hash(counter||no_of_bits_to_return||input_string) is
                                              03D8AA3A 8D6D46E7
        2E5AE8CB E0BB2835 76DD4669 FABEA280 31F69B38 2699E320


    temp =
                                              03D8AA3A 8D6D46E7
        2E5AE8CB E0BB2835 76DD4669 FABEA280 31F69B38 2699E320


s is
                                              03D8AA3A 8D6D46E7
        2E5AE8CB E0BB2835 76DD4669 FABEA280 31F69B38 2699E320


**************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
  ------------
  i=0
  t is
                                              03D8AA3A 8D6D46E7
        2E5AE8CB E0BB2835 76DD4669 FABEA280 31F69B38 2699E320


  s is
                                              32207F17 5B02FA3E
        BCC9F293 B3FE074D DEDA6D7E AC481615 B8A1C460 CE1B41A8


  r is
                                              D01B37AA 3C613D8A
        E18A3F78 09F8C702 03E93952 7C70A559 434FE57C 4D62C3FC


  ------------
  tmp is
                                                  37AA 3C613D8A
```

```
        E18A3F78 09F8C702 03E93952 7C70A559 434FE57C 4D62C3FC


  ------------
  i=1
  t is
                                              32207F17 5B02FA3E
        BCC9F293 B3FE074D DEDA6D7E AC481615 B8A1C460 CE1B41A8


  s is
                                              C4944CAF F5F32BF2
        D004209A 66482C57 D3345F67 C01F647F 5C249681 F66FA94F


  r is
                                              E28442FD 4F6F3479
        97B563EE E9AE1163 AC05022F 5A12CF16 E22680BF E53CAD8C


  ------------
  tmp is
                                    37AA3C61 3D8AE18A 3F7809F8
        C70203E9 39527C70 A559434F E57C4D62 C3FC42FD 4F6F3479
        97B563EE E9AE1163 AC05022F 5A12CF16 E22680BF E53CAD8C


  ------------
  s is
                                              FD9CECE2 7535A492
        0232C4AA F84D4474 D36A93C5 186F71C4 E2997909 3F8471E9


rnd_val is
                                    37AA3C61 3D8AE18A 3F7809F8
        C70203E9 39527C70 A559434F E57C4D62 C3FC42FD 4F6F3479
        97B563EE E9AE1163 AC05022F 5A12CF16 E22680BF E53CAD8C


################################################################

DualEC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256
```

```
    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F

    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F

    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF

    Nonce =
                                            20212223 24252627

    PersonalizationString =
                          40414243 44454647 48494A4B 4C4D4E4F

    AdditionalInput1  =
                          60616263 64656667 68696A6B 6C6D6E6F

    AdditionalInput2  =
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF

##################################################################

******************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F

    nonce is
                                            20212223 24252627

    personal_str is
                          40414243 44454647 48494A4B 4C4D4E4F
```

```
    prediction_resistance_flag = "PredictionResistance"

  Hash_df()
  ----------------------------
    no_of_bits_to_return = 256

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000100 00010203 04050607 08090A0B 0C0D0E0F
          20212223 24252627 40414243 44454647 48494A4B 4C4D4E4F


    Hash(counter||no_of_bits_to_return||input_string) is
                                              48306692 AF00A3F6
          1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


    temp =
                                              48306692 AF00A3F6
          1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


s is
                                              48306692 AF00A3F6
          1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


---------------------------------------------------------------

First call to Generate

***************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
                           60616263 64656667 68696A6B 6C6D6E6F


    requested_number_of_bits is 480
Generate FAILED: Reseed is required
```

```
***************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                           80818283 84858687 88898A8B 8C8D8E8F


    additional_input is
                           60616263 64656667 68696A6B 6C6D6E6F


  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000100 48306692 AF00A3F6 1184864D E183FAB1
        E66C0749 9CCD9849 BF78F873 785EDCB3 80818283 84858687
        88898A8B 8C8D8E8F 60616263 64656667 68696A6B 6C6D6E6F


    Hash(counter||no_of_bits_to_return||input_string) is
                                               5D43947D 5BD466C7
        53E20C75 14AA8A14 3CE6D37F 5ED751D2 0797BAB3 56BB2B51


    temp =
                                               5D43947D 5BD466C7
        53E20C75 14AA8A14 3CE6D37F 5ED751D2 0797BAB3 56BB2B51


s is
                                               5D43947D 5BD466C7
        53E20C75 14AA8A14 3CE6D37F 5ED751D2 0797BAB3 56BB2B51


***************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>
```

```
  requested_number_of_bits is 480
------------
i=0
t is
                                          5D43947D 5BD466C7
      53E20C75 14AA8A14 3CE6D37F 5ED751D2 0797BAB3 56BB2B51


s is
                                          EC1BBA64 B4505E98
      D12175B6 A4083728 35373206 BB3BFD35 CAEC666F 4666CDDF


r is
                                          0B9FBA81 AD8C5F06
      ED4A785D E6CD736D 65E554EB E620033F 6F0E5488 140D064D


------------
tmp is
                                              BA81 AD8C5F06
      ED4A785D E6CD736D 65E554EB E620033F 6F0E5488 140D064D


------------
i=1
t is
                                          EC1BBA64 B4505E98
      D12175B6 A4083728 35373206 BB3BFD35 CAEC666F 4666CDDF


s is
                                          1AE0ECE9 63EF66BC
      84E9DB9E 71DB018A E898F1AD 3E23D1AD B1EC7F25 F2D29115


r is
                                          8805351C AA3EAB50
      306CA8CF D682472D D3EEEFD5 DD7E7742 C9EAB9AE 0BEDF69D


------------
tmp is
                                 BA81AD8C 5F06ED4A 785DE6CD
      736D65E5 54EBE620 033F6F0E 5488140D 064D351C AA3EAB50
```

306CA8CF D682472D D3EEEFD5 DD7E7742 C9EAB9AE 0BEDF69D

  ----
  s is
                                          42751559 C0AB1C14
       6C572FCD C3759E34 82EF69EB E632DFA8 6256E0B9 915ED67F

Second call to Generate

****

DualEC_DRBG_Generate_algorithm

    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF

    requested_number_of_bits is 480
Generate FAILED: Reseed is required
****

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF

    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF

  Hash_df()
  ----
    no_of_bits_to_return = 256

    ----

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000100 42751559 C0AB1C14 6C572FCD C3759E34
        82EF69EB E632DFA8 6256E0B9 915ED67F C0C1C2C3 C4C5C6C7

```
        C8C9CACB CCCDCECF A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    Hash(counter||no_of_bits_to_return||input_string) is
                                                A1BDA7BF 75E06332
        6F58AFFD 08370308 B74A7FEB 41236318 A7F7525D FA858B4F


    temp =
                                                A1BDA7BF 75E06332
        6F58AFFD 08370308 B74A7FEB 41236318 A7F7525D FA858B4F


s is
                                                A1BDA7BF 75E06332
        6F58AFFD 08370308 B74A7FEB 41236318 A7F7525D FA858B4F


****************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
  ------------
  i=0
  t is
                                                A1BDA7BF 75E06332
        6F58AFFD 08370308 B74A7FEB 41236318 A7F7525D FA858B4F


  s is
                                                49D25672 4DCFA4D8
        4FD10072 AEC159C9 B8EFAC1D 9068784F 1ED562D4 84BA81FF


  r is
                                                4AA4BB9C 38A24410
        25BEBD6C 20EC630B D26F8AF5 E92D5B10 1F9F3609 F2AD30D7


  ------------
  tmp is
                                                    BB9C 38A24410
        25BEBD6C 20EC630B D26F8AF5 E92D5B10 1F9F3609 F2AD30D7
```

```
  ------------
  i=1
  t is
                                              49D25672 4DCFA4D8
        4FD10072 AEC159C9 B8EFAC1D 9068784F 1ED562D4 84BA81FF


  s is
                                              361AEC57 BD228951
        E38E5D67 F9A43BFB 1D79389E 88C1394E A33DF322 8C27D415


  r is
                                              1751F982 A78DFA43
        DAAB53ED B2C14F41 2BB5DD2D B7FB2123 B313A40D 934F775C


  ------------
  tmp is
                                   BB9C38A2 441025BE BD6C20EC
        630BD26F 8AF5E92D 5B101F9F 3609F2AD 30D7F982 A78DFA43
        DAAB53ED B2C14F41 2BB5DD2D B7FB2123 B313A40D 934F775C


  ------------
  s is
                                              70E9DD58 60AB91BF
        92E743C3 FAFC74A3 8D39FD77 04091EE9 B0F6C5F1 F4B26B71


rnd_val is
                                   BB9C38A2 441025BE BD6C20EC
        630BD26F 8AF5E92D 5B101F9F 3609F2AD 30D7F982 A78DFA43
        DAAB53ED B2C14F41 2BB5DD2D B7FB2123 B313A40D 934F775C
```

```
################################################################

DualEC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7


    Nonce =
                                    20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    nonce is
                                    20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"
```

```
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                        01 00000180 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 20212223 24252627 28292A2B


    Hash(counter||no_of_bits_to_return||input_string) is
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


    temp =
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


s is
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


-------------------------------------------------------------

First call to Generate

*************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916
```

```
s is
      F2FC3FD8 D0AA88D4 72FB707A 21BE6746 3E2DE7DF 74064A88
      C8164CAE FE7C8610 843DFCC6 FE485BF4 6B9E4EDF A27F5DCC


r is
      8A671F85 8858B653 57D6360E 1ED8F847 5767B08D AB30718C
      CA01C6FA E77A4BDC E2702C76 D0FB4758 EA1ED6AA 587CFD26


------------
tmp is
          1F85 8858B653 57D6360E 1ED8F847 5767B08D AB30718C
      CA01C6FA E77A4BDC E2702C76 D0FB4758 EA1ED6AA 587CFD26


------------
i=1
t is
      F2FC3FD8 D0AA88D4 72FB707A 21BE6746 3E2DE7DF 74064A88
      C8164CAE FE7C8610 843DFCC6 FE485BF4 6B9E4EDF A27F5DCC


s is
      8207B70B 4C1E9251 0BB3A9B0 1B6AA417 B13C9209 9DF08249
      72E8E211 53A3C3A4 C5A9F26C A1534212 5325C40F BE945C2C


r is
      7D59B901 1DC8A75D 0B415419 3BB2C179 8FFA52BC AB208310
      3CD2AAD4 4BEED56D 042FC2B8 915D7D9B ED6437EF EB1582EE


------------
tmp is
               1F858858 B65357D6 360E1ED8 F8475767 B08DAB30
      718CCA01 C6FAE77A 4BDCE270 2C76D0FB 4758EA1E D6AA587C
      FD26B901 1DC8A75D 0B415419 3BB2C179 8FFA52BC AB208310
      3CD2AAD4 4BEED56D 042FC2B8 915D7D9B ED6437EF EB1582EE


------------
s is
      44BF1783 A6B7894D C897B34B 3BC6EDD7 413A1F6C 7E88D519
      D9ED2E36 A425BF36 E198FBC6 9B648DA9 D963E3B9 FAE2C447
```

```
---------------------------------------------------------------

Second call to Generate

***************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
        44BF1783 A6B7894D C897B34B 3BC6EDD7 413A1F6C 7E88D519
        D9ED2E36 A425BF36 E198FBC6 9B648DA9 D963E3B9 FAE2C447


  s is
        70053ED7 AA7B499D AE7C42C1 165EF827 CDA13E2B C0D168C2
        A7DB64B1 681135C9 0A5CFB5A 8323AF2B 7B3FE552 7ABE627D


  r is
        A3486E4A AB639382 12C870F2 4BB067A3 2CA9E7FC 23435D41
        1729268C 8BA6F90E 87074D04 888CE2CC 5A916B7A C93FEDE8


  ------------
  tmp is
             6E4A AB639382 12C870F2 4BB067A3 2CA9E7FC 23435D41
        1729268C 8BA6F90E 87074D04 888CE2CC 5A916B7A C93FEDE8


  ------------
  i=1
  t is
        70053ED7 AA7B499D AE7C42C1 165EF827 CDA13E2B C0D168C2
        A7DB64B1 681135C9 0A5CFB5A 8323AF2B 7B3FE552 7ABE627D


  s is
        806E73C1 4153EEA2 4956B2DD CB071E7A 3EC380AF 7B0B58D3
        E628559E 93A0CB03 7D7AFF79 14E4FE5F BAB17979 F2B1EADA
```

```
  r is
        0FE65E29 95645DFC C4CE44B9 FB41F1BF CC5E9F59 EE3A8E1B
        8F85247F 741B7C48 0521EE6B F8BA319B 59048E65 F08FAA76


  ------------
  tmp is
                 6E4AAB63 938212C8 70F24BB0 67A32CA9 E7FC2343
        5D411729 268C8BA6 F90E8707 4D04888C E2CC5A91 6B7AC93F
        EDE85E29 95645DFC C4CE44B9 FB41F1BF CC5E9F59 EE3A8E1B
        8F85247F 741B7C48 0521EE6B F8BA319B 59048E65 F08FAA76


  ------------
  s is
        40199D10 CB37B6DA 8430A41D 0453374C 1E961A2C 5BB7941A
        007CAE18 B0E9B553 603D85BC 18FBEA1C CD108F85 F7B94BDC


rnd_val is
                 6E4AAB63 938212C8 70F24BB0 67A32CA9 E7FC2343
        5D411729 268C8BA6 F90E8707 4D04888C E2CC5A91 6B7AC93F
        EDE85E29 95645DFC C4CE44B9 FB41F1BF CC5E9F59 EE3A8E1B
        8F85247F 741B7C48 0521EE6B F8BA319B 59048E65 F08FAA76


################################################################

DualEC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


    EntropyInput2 (for Reseed2) =
```

```
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7


    Nonce =
                                  20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput1  =
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    AdditionalInput2  =
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


###############################################################

***************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    nonce is
                                  20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Hash_df()
  --------------------------
    no_of_bits_to_return = 384

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                      01 00000180 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 20212223 24252627 28292A2B
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


    temp =
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


s is
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


---------------------------------------------------------------

First call to Generate

***************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    requested_number_of_bits is 736
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                  01 00000180
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    Hash(counter||no_of_bits_to_return||input_string) is
        1DF233C6 2DC2E629 D1255A25 0E87BED1 B26E6ADA D1DE4DE7
        0D84A331 AE09EA46 4A626E6A 3EE7E31F B2E9D581 60C62506
```

```
  temp =
      1DF233C6 2DC2E629 D1255A25 0E87BED1 B26E6ADA D1DE4DE7
      0D84A331 AE09EA46 4A626E6A 3EE7E31F B2E9D581 60C62506


------------
i=0
t is
      EE101B0B 1F2D06C8 DE9E66A1 687EB4B1 932C985A 23FB87A2
      75086936 30431DB3 067DC37A 866FFCA0 57E552C9 66256C10


s is
      87B2F560 6E29B0FB BE43F68C CB66808C 55BFFE7C 67E8D6DF
      D011E9A3 9172614F 25F2DDCD 18F3BB4B 0EFB359C FDC05D18


r is
      E513F534 620C9FAC A8B7A7D5 0285FAF4 C29128EC 622A4B49
      EA3AB8C9 056F5019 42534953 4B00B72E 1D870CF7 8B4ACF53


------------
tmp is
          F534 620C9FAC A8B7A7D5 0285FAF4 C29128EC 622A4B49
      EA3AB8C9 056F5019 42534953 4B00B72E 1D870CF7 8B4ACF53


------------
i=1
t is
      87B2F560 6E29B0FB BE43F68C CB66808C 55BFFE7C 67E8D6DF
      D011E9A3 9172614F 25F2DDCD 18F3BB4B 0EFB359C FDC05D18


s is
      00769F7D 31700CBE D808128B 02C74C06 B5F92312 289EAF03
      E96AAFDF CDF9D248 0CAE4ED5 682E8C5E D2BCFB9B A49C096A


r is
      806D75C2 FEF7E440 92697D96 9AE3C3DB 909AF09D 1D87587B
      30AADF5D F9B9F14F 549A0871 00A0137C 16DFB4A6 12C2AA0E
```

```
  ------------
  tmp is
                F534620C 9FACA8B7 A7D50285 FAF4C291 28EC622A
        4B49EA3A B8C9056F 50194253 49534B00 B72E1D87 0CF78B4A
        CF5375C2 FEF7E440 92697D96 9AE3C3DB 909AF09D 1D87587B
        30AADF5D F9B9F14F 549A0871 00A0137C 16DFB4A6 12C2AA0E


  ------------
  s is
        258B2AC7 FC3CDBC9 74089A54 2B1FF289 13B97D01 8253BDF3
        BE28A9A8 85801E9A 66387D12 4F0ADCA5 B3631A44 B48AAC5F


------------------------------------------------------------

Second call to Generate

************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


    requested_number_of_bits is 736
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                    01 00000180
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


    Hash(counter||no_of_bits_to_return||input_string) is
        46EE6038 F6F0DC33 FBF6BA3D 19141D5A 2DBF240D 7D9D85F6
        0DB6BC42 6ABCFC8F D5171DFD A919A2FA 3100054B 9B0B4CC1
```

```
  temp =
      46EE6038 F6F0DC33 FBF6BA3D 19141D5A 2DBF240D 7D9D85F6
      0DB6BC42 6ABCFC8F D5171DFD A919A2FA 3100054B 9B0B4CC1


------------
i=0
t is
      63654AFF 0ACC07FA 8FFE2069 320BEFD3 3E06590C FFCE3805
      B39E15EA EF3CE215 B32F60EF E6137E5F 82631F0F 2F81E09E


s is
      0FDAB8E7 D5D67674 E92EF0DA B3EA6E7F 9CA8AE18 8922A917
      18BE1476 B0097C2D 5A546D47 F7888B32 383F1219 68811459


r is
      386F8018 59605617 F9B9CC4D 484E85F5 FD7DEF0A 6E0AECA4
      1D6E523C E4985928 C60D5E1C 41DF06BA 64987967 1A98AB43


------------
tmp is
          8018 59605617 F9B9CC4D 484E85F5 FD7DEF0A 6E0AECA4
      1D6E523C E4985928 C60D5E1C 41DF06BA 64987967 1A98AB43


------------
i=1
t is
      0FDAB8E7 D5D67674 E92EF0DA B3EA6E7F 9CA8AE18 8922A917
      18BE1476 B0097C2D 5A546D47 F7888B32 383F1219 68811459


s is
      CE5F019A F577B9A1 B9FC7444 BE896F31 DCA8C513 48376D40
      6CA03A30 6F3C6507 F4B2F020 B2E10A20 957D352F 8F158416


r is
      3D36843F 80BFDFC6 8F614439 5D1698D6 8FCDA6C0 800345DB
      DBA6689C 33BA050A 1F1EA52F EB649A62 9328CC53 6F711B7C


------------
```

```
  tmp is
                80185960 5617F9B9 CC4D484E 85F5FD7D EF0A6E0A
        ECA41D6E 523CE498 5928C60D 5E1C41DF 06BA6498 79671A98
        AB43843F 80BFDFC6 8F614439 5D1698D6 8FCDA6C0 800345DB
        DBA6689C 33BA050A 1F1EA52F EB649A62 9328CC53 6F711B7C


  ------------
  s is
        64508503 BCF8F875 F5D5E5D4 B66E9377 D631405D 5AAD357E
        062EE7D3 384E5FE5 E4BCB1A6 630A0353 003A3320 E1ABBAA6


rnd_val is
                80185960 5617F9B9 CC4D484E 85F5FD7D EF0A6E0A
        ECA41D6E 523CE498 5928C60D 5E1C41DF 06BA6498 79671A98
        AB43843F 80BFDFC6 8F614439 5D1698D6 8FCDA6C0 800345DB
        DBA6689C 33BA050A 1F1EA52F EB649A62 9328CC53 6F711B7C


##############################################################

DualEC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7


    Nonce =
                                  20212223 24252627 28292A2B


    PersonalizationString =
```

```
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    AdditionalInput = <empty>

################################################################

****************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    nonce is
                                    20212223 24252627 28292A2B


    personal_str is
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    prediction_resistance_flag = "No PredictionResistance"

  Hash_df()
  ----------------------------
    no_of_bits_to_return = 384

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                        01 00000180 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 20212223 24252627 28292A2B
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    Hash(counter||no_of_bits_to_return||input_string) is
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


    temp =
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
```

```
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


s is
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


------------------------------------------------------------

First call to Generate

************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


  s is
        A2E1B617 1D631A2E A0363469 64A650F1 A7748CEE 97D5F3DD
        767CACD2 03A40682 FE5DF995 611FFEBF E1A48917 14850D3A


  r is
        5A30E6A3 0AB0C9AF CBA673E4 F1C94B3D B1F0C7D7 8B3D87B9
        67281BE1 E7B3CAF5 200AED50 2C26B84F C169FE83 36BD2327


  ------------
  tmp is
             E6A3 0AB0C9AF CBA673E4 F1C94B3D B1F0C7D7 8B3D87B9
        67281BE1 E7B3CAF5 200AED50 2C26B84F C169FE83 36BD2327


  ------------
  i=1
  t is
        A2E1B617 1D631A2E A0363469 64A650F1 A7748CEE 97D5F3DD
```

```
        767CACD2 03A40682 FE5DF995 611FFEBF E1A48917 14850D3A


  s is
        029B765D EFF6471C FCB50530 1F748D1F 11EBE53C B56900A4
        9D3C6F8C 3F196E53 1C7B9640 7005D201 956DCC57 0EFC0195


  r is
        21F81CB2 99812F2C F1955AA6 3FC36204 4ABA246E F1610F9E
        DC613924 A84A00F8 DB3FC65C 13373F31 71EB2084 8FA9A70E


  ------------
  tmp is
                 E6A30AB0 C9AFCBA6 73E4F1C9 4B3DB1F0 C7D78B3D
        87B96728 1BE1E7B3 CAF5200A ED502C26 B84FC169 FE8336BD
        23271CB2 99812F2C F1955AA6 3FC36204 4ABA246E F1610F9E
        DC613924 A84A00F8 DB3FC65C 13373F31 71EB2084 8FA9A70E


  ------------
  s is
        6D96C3E9 B559B30B 765BF521 DB141F82 AF8092EE DD2A8052
        6069A452 D623ABAE 3696A224 8F509BB0 738885F2 6F0DC48A


----------------------------------------------------------------

Second call to Generate

****************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
        6D96C3E9 B559B30B 765BF521 DB141F82 AF8092EE DD2A8052
        6069A452 D623ABAE 3696A224 8F509BB0 738885F2 6F0DC48A


  s is
```

```
      3B5154FD FE0EEB95 401DF1A4 81528DE5 1E3B02D7 2C9EBB24
      EB0037FA 149F11BD F7AB93FE 21D32977 3EA8B3A4 BD9CADE4


r is
      64458585 764DF1C8 6EA12ACC B882525B F6217B44 74865EBF
      DA367B86 57FA8047 1139BAC6 26172B9F 219DF2CE 9099F658


------------
tmp is
          8585 764DF1C8 6EA12ACC B882525B F6217B44 74865EBF
      DA367B86 57FA8047 1139BAC6 26172B9F 219DF2CE 9099F658


------------
i=1
t is
      3B5154FD FE0EEB95 401DF1A4 81528DE5 1E3B02D7 2C9EBB24
      EB0037FA 149F11BD F7AB93FE 21D32977 3EA8B3A4 BD9CADE4


s is
      724C35C6 80ED0254 7B8F134F 7083B917 E1D5F9C1 A0AC5D3A
      692E7AC3 E1BC3300 4C521576 095E230F 04ABE2D4 CDD55CAE


r is
      5CE433E0 7CD1A8DD 80468779 EA3C2662 0A2C9C9F 5C7EFCDD
      C036E6F6 C8BF7031 6D3C37FC 246A4CC7 9B3F1DB9 71D72ED0


------------
tmp is
               8585764D F1C86EA1 2ACCB882 525BF621 7B447486
      5EBFDA36 7B8657FA 80471139 BAC62617 2B9F219D F2CE9099
      F65833E0 7CD1A8DD 80468779 EA3C2662 0A2C9C9F 5C7EFCDD
      C036E6F6 C8BF7031 6D3C37FC 246A4CC7 9B3F1DB9 71D72ED0


------------
s is
      56A02C8F E41C3B1A 9F2D6B6F 418F2F8C 83216C5B 52712185
      38B66E54 D2479749 D22CFE83 5EEF4FC8 3E680A45 4249A567
```

```
rnd_val is
                8585764D F1C86EA1 2ACCB882 525BF621 7B447486
        5EBFDA36 7B8657FA 80471139 BAC62617 2B9F219D F2CE9099
        F65833E0 7CD1A8DD 80468779 EA3C2662 0A2C9C9F 5C7EFCDD
        C036E6F6 C8BF7031 6D3C37FC 246A4CC7 9B3F1DB9 71D72ED0


##############################################################

DualEC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7


    Nonce =
                                  20212223 24252627 28292A2B


    PersonalizationString =
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    AdditionalInput1  =
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    AdditionalInput2  =
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


##############################################################
```

```
***************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    nonce is
                                    20212223 24252627 28292A2B


    personal_str is
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    prediction_resistance_flag = "No PredictionResistance"

  Hash_df()
  ----------------------------
    no_of_bits_to_return = 384

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                        01 00000180 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 20212223 24252627 28292A2B
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    Hash(counter||no_of_bits_to_return||input_string) is
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


    temp =
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


s is
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F
```

```
------------------------------------------------------------

First call to Generate

************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    requested_number_of_bits is 736
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                    01 00000180
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    Hash(counter||no_of_bits_to_return||input_string) is
        1DF233C6 2DC2E629 D1255A25 0E87BED1 B26E6ADA D1DE4DE7
        0D84A331 AE09EA46 4A626E6A 3EE7E31F B2E9D581 60C62506


    temp =
        1DF233C6 2DC2E629 D1255A25 0E87BED1 B26E6ADA D1DE4DE7
        0D84A331 AE09EA46 4A626E6A 3EE7E31F B2E9D581 60C62506


  ------------
  i=0
  t is
        2747E904 F2CAA5D1 37E5382C 5138CC92 ECD8C298 DEF2700F
        BE87BB43 7AC58E4A 425CE7BD CC79864B FB3C3A48 54D39C59


  s is
        70636843 2A0D70BF 00244A45 E4FEA8C4 28E7D778 344EF939
```

```
      FEE7C4BC D0E50906 BBE5437A AA537741 A5EF3C6E C623E5D0


 r is
      D22413F6 EA9BBA7B ABDC2A52 A3B9FD73 D65ECAA6 38A04C74
      BCCA2ACD E6FD29FE A4B5D884 E095E87D 1B7C0DEB 9D377AD8


 ------------
 tmp is
          13F6 EA9BBA7B ABDC2A52 A3B9FD73 D65ECAA6 38A04C74
      BCCA2ACD E6FD29FE A4B5D884 E095E87D 1B7C0DEB 9D377AD8


 ------------
 i=1
 t is
      70636843 2A0D70BF 00244A45 E4FEA8C4 28E7D778 344EF939
      FEE7C4BC D0E50906 BBE5437A AA537741 A5EF3C6E C623E5D0


 s is
      B2BD4448 6B311865 14EB9217 A0B8C120 9C84F045 2FB4537D
      7C15CD34 875B5FE3 0AB3F82F 2D4FB274 3159BDEC 4FA73C20


 r is
      12551FBF EEA2D5EF 82C0F6F5 2B9FCC35 9E769AC9 DF2A876C
      58BAF216 57814F3E 66D1680B 1D4EBD65 581E4253 4F85197D


 ------------
 tmp is
               13F6EA9B BA7BABDC 2A52A3B9 FD73D65E CAA638A0
      4C74BCCA 2ACDE6FD 29FEA4B5 D884E095 E87D1B7C 0DEB9D37
      7AD81FBF EEA2D5EF 82C0F6F5 2B9FCC35 9E769AC9 DF2A876C
      58BAF216 57814F3E 66D1680B 1D4EBD65 581E4253 4F85197D


 ------------
 s is
      17EACDB6 7EC46403 6741189C BFA507A9 57279F54 B089160D
      29D42AB5 19759164 07506EDF EA8BA231 461E73A7 EBAFB1DE


-------------------------------------------------------------
```

```
Second call to Generate

************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


    requested_number_of_bits is 736
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                  01 00000180
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


    Hash(counter||no_of_bits_to_return||input_string) is
        46EE6038 F6F0DC33 FBF6BA3D 19141D5A 2DBF240D 7D9D85F6
        0DB6BC42 6ABCFC8F D5171DFD A919A2FA 3100054B 9B0B4CC1


    temp =
        46EE6038 F6F0DC33 FBF6BA3D 19141D5A 2DBF240D 7D9D85F6
        0DB6BC42 6ABCFC8F D5171DFD A919A2FA 3100054B 9B0B4CC1


  ------------
  i=0
  t is
        5104AD8E 8834B830 9CB7A2A1 A6B11AF3 7A98BB59 CD1493FB
        246296F7 73C96DEB D2477322 439200CB 771E76EC 70A4FD1F


  s is
        3FD8CA8C BE1597E1 2DC5A32E 35F22DE1 2791DA06 DEC6BB92
        EB6476FE EEDEF970 2601C0E6 FF663F99 8311CFB0 A4C15BE6
```

```
  r is
        2402FC0A 36F4D20F 8F83BE34 30AA3C36 A4919182 1A82072B
        BC3D5AFF 8D7EC394 84D64627 7CE87599 B6FE8CCA 98625597


  ------------
  tmp is
            FC0A 36F4D20F 8F83BE34 30AA3C36 A4919182 1A82072B
        BC3D5AFF 8D7EC394 84D64627 7CE87599 B6FE8CCA 98625597


  ------------
  i=1
  t is
        3FD8CA8C BE1597E1 2DC5A32E 35F22DE1 2791DA06 DEC6BB92
        EB6476FE EEDEF970 2601C0E6 FF663F99 8311CFB0 A4C15BE6


  s is
        80FA1CF8 26484C63 453011FE A35D2396 EA90C79B 59102132
        C03E1CD5 C69AF0CF 19A7F583 9D3DD13A 3D5B7EF2 83E2C69A


  r is
        2E8D03A1 0F4DE106 6BFD30B8 0C325E77 4B512525 BC6D3734
        4C939063 68243D31 F89E99C4 D2A6E9BE B24D5F72 67360DCA


  ------------
  tmp is
                  FC0A36F4 D20F8F83 BE3430AA 3C36A491 91821A82
        072BBC3D 5AFF8D7E C39484D6 46277CE8 7599B6FE 8CCA9862
        559703A1 0F4DE106 6BFD30B8 0C325E77 4B512525 BC6D3734
        4C939063 68243D31 F89E99C4 D2A6E9BE B24D5F72 67360DCA


  ------------
  s is
        39EB1BA2 6F6F487F E07FD5B8 A8A40287 5DB93D9F 6BB0797D
        BC38A71D 68B0CA41 6199DF43 134B881E 6048885B 3C44B5A9


rnd_val is
                  FC0A36F4 D20F8F83 BE3430AA 3C36A491 91821A82
        072BBC3D 5AFF8D7E C39484D6 46277CE8 7599B6FE 8CCA9862
```

559703A1 0F4DE106 6BFD30B8 0C325E77 4B512525 BC6D3734
4C939063 68243D31 F89E99C4 D2A6E9BE B24D5F72 67360DCA

##

DualEC_DRBG

Requested Security Strength = 192

Requested Hash Algorithm = SHA-384

prediction_resistance_flag = "ENABLED"
EntropyInput =
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617

EntropyInput1 (for Reseed1) =
80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697

EntropyInput2 (for Reseed2) =
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7

Nonce =
20212223 24252627 28292A2B

PersonalizationString = <empty>

AdditionalInput = <empty>

##

****

DualEC_DRBG_Instantiate_algorithm

entropy_input is
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617

nonce is
20212223 24252627 28292A2B

```
    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Hash_df()
  --------------------------
    no_of_bits_to_return = 384

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                        01 00000180 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 20212223 24252627 28292A2B


    Hash(counter||no_of_bits_to_return||input_string) is
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


    temp =
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


s is
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


-------------------------------------------------------------

First call to Generate

*************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
Generate FAILED: Reseed is required
*************************************************************
```

```
DualEC_DRBG_Reseed_algorithm

    entropy_input is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


    additional_input is  <empty>

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                    01 00000180
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


    Hash(counter||no_of_bits_to_return||input_string) is
        32FC492B 99BAB8A8 BC3EFEEF F7955E4D 81788F69 1D18801D
        3EA1AD48 17133B8C C0AC41D5 A13C60F2 5D0A8061 6A9D3D81


    temp =
        32FC492B 99BAB8A8 BC3EFEEF F7955E4D 81788F69 1D18801D
        3EA1AD48 17133B8C C0AC41D5 A13C60F2 5D0A8061 6A9D3D81


s is
        32FC492B 99BAB8A8 BC3EFEEF F7955E4D 81788F69 1D18801D
        3EA1AD48 17133B8C C0AC41D5 A13C60F2 5D0A8061 6A9D3D81


**************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
```

```
------------
i=0
t is
      32FC492B 99BAB8A8 BC3EFEEF F7955E4D 81788F69 1D18801D
      3EA1AD48 17133B8C C0AC41D5 A13C60F2 5D0A8061 6A9D3D81


s is
      CE1E095D 226B5C74 BF3E2ED2 E271DF6C 98214823 D12C9D11
      6DC1E21A 839D7000 3646B810 058ADBAF E3992B68 A713265F


r is
      F6C5CC78 8F70FB08 F256D960 4333630D 85936D40 0F45718D
      C3F939A8 B9F6F75D 3E4EC17D 68FBB924 AEACB702 129548FA


------------
tmp is
          CC78 8F70FB08 F256D960 4333630D 85936D40 0F45718D
      C3F939A8 B9F6F75D 3E4EC17D 68FBB924 AEACB702 129548FA


------------
i=1
t is
      CE1E095D 226B5C74 BF3E2ED2 E271DF6C 98214823 D12C9D11
      6DC1E21A 839D7000 3646B810 058ADBAF E3992B68 A713265F


s is
      4D15B54C F35F02E1 6FFD87A2 7CFA8CDD F663CFD6 EF61087F
      14904E07 E4427164 99937058 5B1388DA 282EF95F 9094A42C


r is
      BFD263CE 9BCB8217 6639B64D E890A470 25B55823 12FE934E
      F0D0A126 97C0F05D 2DA108CC ADB511BA 0EB62F40 51BB2354


------------
tmp is
               CC788F70 FB08F256 D9604333 630D8593 6D400F45
      718DC3F9 39A8B9F6 F75D3E4E C17D68FB B924AEAC B7021295
      48FA63CE 9BCB8217 6639B64D E890A470 25B55823 12FE934E
      F0D0A126 97C0F05D 2DA108CC ADB511BA 0EB62F40 51BB2354
```

```
  ------------
  s is
        51B364B8 88A04C1C 0F03B49E E2936F07 33646485 1330CB1E
        4B3F40EE 4F3C04AC 017D393F 1C571FD0 1028AB62 30ECDA6C


--------------------------------------------------------------

Second call to Generate

**************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
Generate FAILED: Reseed is required
**************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7


    additional_input is  <empty>

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                    01 00000180
        51B364B8 88A04C1C 0F03B49E E2936F07 33646485 1330CB1E
        4B3F40EE 4F3C04AC 017D393F 1C571FD0 1028AB62 30ECDA6C
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
        A981E9D6 AC1C712A 69ED13B6 14E252CC BB65CD75 0C3C66F7
        40613F19 96F2C244 FC301679 449D440C 7D605111 1FE9AC42


    temp =
        A981E9D6 AC1C712A 69ED13B6 14E252CC BB65CD75 0C3C66F7
        40613F19 96F2C244 FC301679 449D440C 7D605111 1FE9AC42


s is
        A981E9D6 AC1C712A 69ED13B6 14E252CC BB65CD75 0C3C66F7
        40613F19 96F2C244 FC301679 449D440C 7D605111 1FE9AC42


************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
        A981E9D6 AC1C712A 69ED13B6 14E252CC BB65CD75 0C3C66F7
        40613F19 96F2C244 FC301679 449D440C 7D605111 1FE9AC42


  s is
        63AD9407 333FDE6F 1BC287E3 C481A78E 34AD4BE9 EC2F0ACC
        7CDB1D01 87BC6C72 5470BF03 41F2BF72 145B01C2 3ECB7232


  r is
        21C22C92 2EA620D7 6E4137B3 15EBC29E 518F8095 1B3F0E61
        73FA2BFD 94A230EE 513EE2E4 EB330D80 2F620DD2 4911534E


  ------------
  tmp is
            2C92 2EA620D7 6E4137B3 15EBC29E 518F8095 1B3F0E61
        73FA2BFD 94A230EE 513EE2E4 EB330D80 2F620DD2 4911534E


  ------------
  i=1
```

```
  t is
        63AD9407 333FDE6F 1BC287E3 C481A78E 34AD4BE9 EC2F0ACC
        7CDB1D01 87BC6C72 5470BF03 41F2BF72 145B01C2 3ECB7232


  s is
        F0664F09 A819C032 7174D687 859509EF C82AFE96 AD132D70
        7F528B39 AB54103C CC8414E6 E9EE91D9 DD2D5135 08EC7B18


  r is
        9930C0F9 5A1F1D44 A2125F5D 57476A66 6FC37209 2B55D0D6
        8B49738F 5BC466EC 206AB3CF 6A972B38 BCFAE5FC D53C7E21


  ------------
  tmp is
                  2C922EA6 20D76E41 37B315EB C29E518F 80951B3F
        0E6173FA 2BFD94A2 30EE513E E2E4EB33 0D802F62 0DD24911
        534EC0F9 5A1F1D44 A2125F5D 57476A66 6FC37209 2B55D0D6
        8B49738F 5BC466EC 206AB3CF 6A972B38 BCFAE5FC D53C7E21


  ------------
  s is
        62154AE1 587BB30F 09ACF488 9ED4B44C 42C1EEB7 49631CBC
        79BC4F15 6E3A0778 83A6AB20 BEE81B90 787E7696 F1A59CF7


rnd_val is
                  2C922EA6 20D76E41 37B315EB C29E518F 80951B3F
        0E6173FA 2BFD94A2 30EE513E E2E4EB33 0D802F62 0DD24911
        534EC0F9 5A1F1D44 A2125F5D 57476A66 6FC37209 2B55D0D6
        8B49738F 5BC466EC 206AB3CF 6A972B38 BCFAE5FC D53C7E21


##############################################################

DualEC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
```

```
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7


    Nonce =
                                  20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput1  =
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    AdditionalInput2  =
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


###############################################################

***************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    nonce is
                                  20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384
```

```
    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                       01 00000180 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 20212223 24252627 28292A2B


    Hash(counter||no_of_bits_to_return||input_string) is
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


    temp =
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


s is
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


------------------------------------------------------------

First call to Generate

**************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    requested_number_of_bits is 736
Generate FAILED: Reseed is required
**************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
```

```
    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


  Hash_df()
  --------------------------
    no_of_bits_to_return = 384

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                    01 00000180
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    Hash(counter||no_of_bits_to_return||input_string) is
        6F0CF28C 7B226E42 698B1ACF 1FE859B1 9E585D8A CCE91C27
        101AFF9F E6E860EA ED22DEFD 26D9F43D 70EC620B DAA870E3


    temp =
        6F0CF28C 7B226E42 698B1ACF 1FE859B1 9E585D8A CCE91C27
        101AFF9F E6E860EA ED22DEFD 26D9F43D 70EC620B DAA870E3


s is
        6F0CF28C 7B226E42 698B1ACF 1FE859B1 9E585D8A CCE91C27
        101AFF9F E6E860EA ED22DEFD 26D9F43D 70EC620B DAA870E3


**************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
```

```
      6F0CF28C 7B226E42 698B1ACF 1FE859B1 9E585D8A CCE91C27
      101AFF9F E6E860EA ED22DEFD 26D9F43D 70EC620B DAA870E3


s is
      04184A7A DE35DE09 06BC174C 1DA79FBA FE6AB1E8 5631910D
      38665DD4 08F751E3 3C6A75BB 6AC7E52F 31BA716D B3FBDD67


r is
      7A88FE55 601BF734 49301370 5CCEB76E 44AAD483 73F742E7
      2B83D470 1FA65492 55F1CDE6 21795352 2FF973BA 4F6EC96D


------------
tmp is
          FE55 601BF734 49301370 5CCEB76E 44AAD483 73F742E7
      2B83D470 1FA65492 55F1CDE6 21795352 2FF973BA 4F6EC96D


------------
i=1
t is
      04184A7A DE35DE09 06BC174C 1DA79FBA FE6AB1E8 5631910D
      38665DD4 08F751E3 3C6A75BB 6AC7E52F 31BA716D B3FBDD67


s is
      AC57A08B EDD6099E 1D473001 AD5FE71E 8FB91D2C D851DAF0
      07C078FB B66C5498 20B51779 424742B2 AF3A2F33 B903D91E


r is
      8F6B2BDC F14A76BE 7DEB6178 1E34B993 35BD714F 17C91739
      B4E2AB57 E36E9C31 16E215D3 D94FCFAD 53263687 4875CAC7


------------
tmp is
               FE55601B F7344930 13705CCE B76E44AA D48373F7
      42E72B83 D4701FA6 549255F1 CDE62179 53522FF9 73BA4F6E
      C96D2BDC F14A76BE 7DEB6178 1E34B993 35BD714F 17C91739
      B4E2AB57 E36E9C31 16E215D3 D94FCFAD 53263687 4875CAC7


------------
```

```
  s is
        94110169 CEA534FB B7FE6B2A 5ED5A998 D5E2A707 3D1BD763
        7676242A 8E8B64C5 E49E049B B070B2A4 4CDEDE76 D9E6DA60


---------------------------------------------------------------

Second call to Generate

***************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


    requested_number_of_bits is 736
Generate FAILED: Reseed is required
***************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7


    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                    01 00000180
        94110169 CEA534FB B7FE6B2A 5ED5A998 D5E2A707 3D1BD763
        7676242A 8E8B64C5 E49E049B B070B2A4 4CDEDE76 D9E6DA60
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
        48D959C7 AB3F44CA BB50A056 C5947261 B34EC266 DACE1029
        18A6AFB1 0978C407 9B3C9866 A431182D 0F7415DA D510D1F0


    temp =
        48D959C7 AB3F44CA BB50A056 C5947261 B34EC266 DACE1029
        18A6AFB1 0978C407 9B3C9866 A431182D 0F7415DA D510D1F0


s is
        48D959C7 AB3F44CA BB50A056 C5947261 B34EC266 DACE1029
        18A6AFB1 0978C407 9B3C9866 A431182D 0F7415DA D510D1F0


************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
        48D959C7 AB3F44CA BB50A056 C5947261 B34EC266 DACE1029
        18A6AFB1 0978C407 9B3C9866 A431182D 0F7415DA D510D1F0


  s is
        F086349E 5D200ACD 3821E708 164EE368 81175E1A 4EA66CF7
        E8C96B8D 8B7E67A0 96533ECD A1D0892E B5FB019D 2091E7A8


  r is
        4B05F5E5 9D0ABADE 81F62FFA B9D4A6A2 6FF20001 6608A721
        5E389858 FFED83FB C75CFD33 DBA6688C 89AA32AD 22E480EA


  ------------
  tmp is
            F5E5 9D0ABADE 81F62FFA B9D4A6A2 6FF20001 6608A721
        5E389858 FFED83FB C75CFD33 DBA6688C 89AA32AD 22E480EA
```

```
  ------------
  i=1
  t is
        F086349E 5D200ACD 3821E708 164EE368 81175E1A 4EA66CF7
        E8C96B8D 8B7E67A0 96533ECD A1D0892E B5FB019D 2091E7A8


  s is
        F0E8044F DB6805D8 6D95CCF3 E00A14D6 EB583EA4 9168F666
        8BE21578 9D7FD0DD F866B894 AFDC9A36 EF8BE64D 3F62996A


  r is
        27563D04 EADFB355 67B67564 207E64B7 7844E8E4 A87502D5
        02DBBB6D 8277F1CA CDB7CF8D 293D09DB 7DD59A95 0821507A


  ------------
  tmp is
                 F5E59D0A BADE81F6 2FFAB9D4 A6A26FF2 00016608
        A7215E38 9858FFED 83FBC75C FD33DBA6 688C89AA 32AD22E4
        80EA3D04 EADFB355 67B67564 207E64B7 7844E8E4 A87502D5
        02DBBB6D 8277F1CA CDB7CF8D 293D09DB 7DD59A95 0821507A


  ------------
  s is
        63B09B71 7CEE9988 D4C20A67 2EF7A070 43114545 49BD6BDA
        008BD303 A227F3E7 4AC2EF83 14B2A36E 5AB44DB7 ED5765FD


rnd_val is
                 F5E59D0A BADE81F6 2FFAB9D4 A6A26FF2 00016608
        A7215E38 9858FFED 83FBC75C FD33DBA6 688C89AA 32AD22E4
        80EA3D04 EADFB355 67B67564 207E64B7 7844E8E4 A87502D5
        02DBBB6D 8277F1CA CDB7CF8D 293D09DB 7DD59A95 0821507A


#############################################################

DualEC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384
```

```
    prediction_resistance_flag = "ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7


    Nonce =
                                  20212223 24252627 28292A2B


    PersonalizationString =
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    AdditionalInput = <empty>

################################################################

****************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    nonce is
                                  20212223 24252627 28292A2B


    personal_str is
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    prediction_resistance_flag = "PredictionResistance"

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384
```

```
    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                      01 00000180 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 20212223 24252627 28292A2B
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    Hash(counter||no_of_bits_to_return||input_string) is
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


    temp =
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


s is
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


---------------------------------------------------------------

First call to Generate

***************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
Generate FAILED: Reseed is required
***************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
```

```
    additional_input is  <empty>

  Hash_df()
  --------------------------
    no_of_bits_to_return = 384

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                    01 00000180
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


    Hash(counter||no_of_bits_to_return||input_string) is
        DC6F1374 8FEEECE2 3E20DFB3 3F6FD202 6526BF56 506D21AE
        5EBCE30F C3676D44 4DB0324B F6F1326F DA6D1095 C08BE9F5


    temp =
        DC6F1374 8FEEECE2 3E20DFB3 3F6FD202 6526BF56 506D21AE
        5EBCE30F C3676D44 4DB0324B F6F1326F DA6D1095 C08BE9F5


s is
        DC6F1374 8FEEECE2 3E20DFB3 3F6FD202 6526BF56 506D21AE
        5EBCE30F C3676D44 4DB0324B F6F1326F DA6D1095 C08BE9F5


**************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
        DC6F1374 8FEEECE2 3E20DFB3 3F6FD202 6526BF56 506D21AE
        5EBCE30F C3676D44 4DB0324B F6F1326F DA6D1095 C08BE9F5
```

```
s is
      7A5716FE 96AD1AE2 7579A5DC E9446D90 9F04FF26 0E4F719F
      3D7F0EDF C164AEC3 F5074788 DA07A9B6 3BF3149B 239A486C


r is
      97DE7103 B98CEB33 C6199267 23A49B0F E8E80A9E DE9D433A
      519080E6 2344386C 3DCAD93F 72BBAA25 DE7857C1 63AA3669


------------
tmp is
          7103 B98CEB33 C6199267 23A49B0F E8E80A9E DE9D433A
      519080E6 2344386C 3DCAD93F 72BBAA25 DE7857C1 63AA3669


------------
i=1
t is
      7A5716FE 96AD1AE2 7579A5DC E9446D90 9F04FF26 0E4F719F
      3D7F0EDF C164AEC3 F5074788 DA07A9B6 3BF3149B 239A486C


s is
      314CF789 29E60365 7D212745 C19F1BD2 E058506A CF8FDE7D
      E72EFE12 04FE0BA6 9040E57B 5E1E0723 B82272D3 D1B55C02


r is
      095C8643 FEE94B62 610D34B0 6D753350 9D072FB3 3F83F0AD
      CD91CE33 FE65D273 A4515684 DA401FE0 005F44E4 4EB090B0


------------
tmp is
               7103B98C EB33C619 926723A4 9B0FE8E8 0A9EDE9D
      433A5190 80E62344 386C3DCA D93F72BB AA25DE78 57C163AA
      36698643 FEE94B62 610D34B0 6D753350 9D072FB3 3F83F0AD
      CD91CE33 FE65D273 A4515684 DA401FE0 005F44E4 4EB090B0


------------
s is
      1E501974 59C49108 A6542E1F F84A34A1 4918CAB4 F3E623C0
      609C174A 4CDF8E99 E19A3DBD 4735AC17 A5ECF846 E2D620A0
```

```
---------------------------------------------------------------

Second call to Generate

***************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
Generate FAILED: Reseed is required
***************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7


    additional_input is  <empty>

  Hash_df()
  --------------------------
    no_of_bits_to_return = 384

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                    01 00000180
        1E501974 59C49108 A6542E1F F84A34A1 4918CAB4 F3E623C0
        609C174A 4CDF8E99 E19A3DBD 4735AC17 A5ECF846 E2D620A0
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7


    Hash(counter||no_of_bits_to_return||input_string) is
        0A20975D E8D09863 134DDC5C 005C8F9C 4011D107 BAF39BBB
        B297BBC3 74484713 8E714B3E D2AF559D 294C6C53 EF714313


    temp =
        0A20975D E8D09863 134DDC5C 005C8F9C 4011D107 BAF39BBB
        B297BBC3 74484713 8E714B3E D2AF559D 294C6C53 EF714313
```

```
s is
        0A20975D E8D09863 134DDC5C 005C8F9C 4011D107 BAF39BBB
        B297BBC3 74484713 8E714B3E D2AF559D 294C6C53 EF714313


**************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
        0A20975D E8D09863 134DDC5C 005C8F9C 4011D107 BAF39BBB
        B297BBC3 74484713 8E714B3E D2AF559D 294C6C53 EF714313


  s is
        A83687F0 1C8C2CD0 B10ED7DF 7E13F0EF C400CB4C 53526AB5
        2F752202 C7371876 DA247179 9759F3E4 82A5863A 49ECA73A


  r is
        C779FA07 A143E761 F3EB103B D499CB9D FDAFA38D 3EF0BB5E
        976BEC85 B5C99230 809FCEB8 F1CAC958 284E603A F32549B2


  ------------
  tmp is
            FA07 A143E761 F3EB103B D499CB9D FDAFA38D 3EF0BB5E
        976BEC85 B5C99230 809FCEB8 F1CAC958 284E603A F32549B2


  ------------
  i=1
  t is
        A83687F0 1C8C2CD0 B10ED7DF 7E13F0EF C400CB4C 53526AB5
        2F752202 C7371876 DA247179 9759F3E4 82A5863A 49ECA73A


  s is
        608EFF3D E73BB7E5 7082495C 6A8DF173 1B73EA1E 606D95E8
```

```
        4DEA5BFD 033255C0 82E615B6 021F5B8B 4D2A2402 D767F601


  r is
        64214F65 38534E26 3F1AB60C FB2D7C68 E573C69C C89B413D
        E5C82713 AE09431C BFE9F234 6F46A72F E5B95685 0A3C9AB1


  ------------
  tmp is
                 FA07A143 E761F3EB 103BD499 CB9DFDAF A38D3EF0
        BB5E976B EC85B5C9 9230809F CEB8F1CA C958284E 603AF325
        49B24F65 38534E26 3F1AB60C FB2D7C68 E573C69C C89B413D
        E5C82713 AE09431C BFE9F234 6F46A72F E5B95685 0A3C9AB1


  ------------
  s is
        E1AC17AF 5A333A4B 7AB0FF6C 1C8A3062 165778AF 8809B3FC
        3F382E08 5BFF098C 8C85546C 2E7056F3 7517BB95 13FC87C0


rnd_val is
                 FA07A143 E761F3EB 103BD499 CB9DFDAF A38D3EF0
        BB5E976B EC85B5C9 9230809F CEB8F1CA C958284E 603AF325
        49B24F65 38534E26 3F1AB60C FB2D7C68 E573C69C C89B413D
        E5C82713 AE09431C BFE9F234 6F46A72F E5B95685 0A3C9AB1


##############################################################

DualEC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
```

```
    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7


    Nonce =
                                  20212223 24252627 28292A2B


    PersonalizationString =
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    AdditionalInput1  =
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    AdditionalInput2  =
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


################################################################

****************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    nonce is
                                  20212223 24252627 28292A2B


    personal_str is
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    prediction_resistance_flag = "PredictionResistance"

  Hash_df()
  ----------------------------
    no_of_bits_to_return = 384

    ------------
```

```
    i = 1

    counter||no_of_bits_to_return||input_string is
                      01 00000180 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 20212223 24252627 28292A2B
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    Hash(counter||no_of_bits_to_return||input_string) is
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


    temp =
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


s is
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


-------------------------------------------------------------

First call to Generate

*************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    requested_number_of_bits is 736
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


    additional_input is
```

```
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                    01 00000180
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    Hash(counter||no_of_bits_to_return||input_string) is
        028A28E0 392066C1 C704C425 8A9BB572 6EADB894 6E744A00
        FC69EFEC D4B4C43B 86EE0B0F 661D6820 E9E9BE06 1AFCF90B


    temp =
        028A28E0 392066C1 C704C425 8A9BB572 6EADB894 6E744A00
        FC69EFEC D4B4C43B 86EE0B0F 661D6820 E9E9BE06 1AFCF90B


s is
        028A28E0 392066C1 C704C425 8A9BB572 6EADB894 6E744A00
        FC69EFEC D4B4C43B 86EE0B0F 661D6820 E9E9BE06 1AFCF90B


************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
        028A28E0 392066C1 C704C425 8A9BB572 6EADB894 6E744A00
        FC69EFEC D4B4C43B 86EE0B0F 661D6820 E9E9BE06 1AFCF90B
```

```
s is
      0D315A80 5EA251EB 10DB2488 2F72A7C5 9586987B 26F4DF57
      25382F25 55689022 A4DBB37D 09573EAF 62FDA1AD 1B522A61


r is
      30289F27 C6E67022 B9B11D86 420CB8A3 DDF58CB2 48CBF202
      1CEC9E02 23B117D7 DB380E7B 79EF871D 0EB6EC7D A1D7DBB7


------------
tmp is
          9F27 C6E67022 B9B11D86 420CB8A3 DDF58CB2 48CBF202
      1CEC9E02 23B117D7 DB380E7B 79EF871D 0EB6EC7D A1D7DBB7


------------
i=1
t is
      0D315A80 5EA251EB 10DB2488 2F72A7C5 9586987B 26F4DF57
      25382F25 55689022 A4DBB37D 09573EAF 62FDA1AD 1B522A61


s is
      147E494E 2408CA55 32EFA7BE 16DA7999 370835A7 D69C8A7A
      DC30EA97 AA03FA57 302EC436 0C697569 8BAA7CA6 03272BD8


r is
      0033CECE 60301506 E0CE12EC 7295620D 3641BE27 BFE2AACA
      E5C02F51 8AAB6B69 AAB3B4FA 95AF8D22 8F81E66E 226FD5C8


------------
tmp is
               9F27C6E6 7022B9B1 1D86420C B8A3DDF5 8CB248CB
      F2021CEC 9E0223B1 17D7DB38 0E7B79EF 871D0EB6 EC7DA1D7
      DBB7CECE 60301506 E0CE12EC 7295620D 3641BE27 BFE2AACA
      E5C02F51 8AAB6B69 AAB3B4FA 95AF8D22 8F81E66E 226FD5C8


------------
s is
      1C3B30AE 6F28022D 658AA75C AE4B533A 6863A914 C136122C
```

```
        C34CA3B3 0ACBE79E E10A2A1C 9D140B49 5C104E9B 4B65F15D


-------------------------------------------------------------

Second call to Generate

*************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


    requested_number_of_bits is 736
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7


    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


  Hash_df()
  --------------------------
    no_of_bits_to_return = 384

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                    01 00000180
        1C3B30AE 6F28022D 658AA75C AE4B533A 6863A914 C136122C
        C34CA3B3 0ACBE79E E10A2A1C 9D140B49 5C104E9B 4B65F15D
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
        DBFB441D 9C174B30 30B002C6 8E04D6C0 46BE866E 7FA2D980
        6DB64B62 344878F4 7C264158 565011A3 792B4DDE 119474FD


    temp =
        DBFB441D 9C174B30 30B002C6 8E04D6C0 46BE866E 7FA2D980
        6DB64B62 344878F4 7C264158 565011A3 792B4DDE 119474FD


s is
        DBFB441D 9C174B30 30B002C6 8E04D6C0 46BE866E 7FA2D980
        6DB64B62 344878F4 7C264158 565011A3 792B4DDE 119474FD


**************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
        DBFB441D 9C174B30 30B002C6 8E04D6C0 46BE866E 7FA2D980
        6DB64B62 344878F4 7C264158 565011A3 792B4DDE 119474FD


  s is
        1A94EC0E 06333F8C 73285506 0716E5C3 A7B87C64 18D52462
        4E8920D7 7C49B122 7D9F7514 59384FCE 30BF19AC EDABBE0F


  r is
        BBFF821B 7F5B7334 4B4CA9BA EE05AE2B 68280DE4 F6BE2764
        C4337423 0B7C1CAA 22AF5C37 F0350871 B23B1DE3 F36BA487


  ------------
  tmp is
            821B 7F5B7334 4B4CA9BA EE05AE2B 68280DE4 F6BE2764
        C4337423 0B7C1CAA 22AF5C37 F0350871 B23B1DE3 F36BA487


  ------------
  i=1
```

```
  t is
        1A94EC0E 06333F8C 73285506 0716E5C3 A7B87C64 18D52462
        4E8920D7 7C49B122 7D9F7514 59384FCE 30BF19AC EDABBE0F


  s is
        D9D28A06 CCF032B7 615DCBDA CDC61464 F63A9902 AC414A8C
        BA1DE90F 2DC8CE3B 00A65425 24350049 EF92E299 101F5E59


  r is
        B44733D6 039F7482 3B5B1570 23303B6D 5D008392 58345DC8
        9EC3B223 B2992557 823DDA40 DF90436E A1FB45F9 64260014


  ------------
  tmp is
                 821B7F5B 73344B4C A9BAEE05 AE2B6828 0DE4F6BE
        2764C433 74230B7C 1CAA22AF 5C37F035 0871B23B 1DE3F36B
        A48733D6 039F7482 3B5B1570 23303B6D 5D008392 58345DC8
        9EC3B223 B2992557 823DDA40 DF90436E A1FB45F9 64260014


  ------------
  s is
        D102E664 BD76234F D34D8E9D AA3101C5 F69DE66E D97CF85A
        2B27FDB3 28232303 E043E118 46C737CD 9F67C68D D1F693B7


rnd_val is
                 821B7F5B 73344B4C A9BAEE05 AE2B6828 0DE4F6BE
        2764C433 74230B7C 1CAA22AF 5C37F035 0871B23B 1DE3F36B
        A48733D6 039F7482 3B5B1570 23303B6D 5D008392 58345DC8
        9EC3B223 B2992557 823DDA40 DF90436E A1FB45F9 64260014
```

```
################################################################

DualEC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    Nonce =
                           20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    nonce is
                           20212223 24252627 28292A2B 2C2D2E2F
```

```
  personal_str is  <empty>

  prediction_resistance_flag = "No PredictionResistance"

Hash_df()
----------------------------
  no_of_bits__to_return = 521

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                                                    01 00000209
      00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
      18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


  Hash(counter||no_of_bits_to_return||input_string) is
                       E4CD803E 82C6D10E 8D8F3E5A 2A80F4A4
      9F5C3DE4 E5946995 FBE2131F 6A3DAC66 DB4DEE1A AC0C37DA
      BBB31BB5 F6885BF6 E94BFB19 BD1CD4FC E1D96840 7E2AD9FA


  temp =
                       E4CD803E 82C6D10E 8D8F3E5A 2A80F4A4
      9F5C3DE4 E5946995 FBE2131F 6A3DAC66 DB4DEE1A AC0C37DA
      BBB31BB5 F6885BF6 E94BFB19 BD1CD4FC E1D96840 7E2AD9FA


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                                                    02 00000209
      00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
      18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


  Hash(counter||no_of_bits_to_return||input_string) is
                       0BF4E84E 26C435F1 A8C9DDAF B866D3E9
      C7556662 F08A12DA AE1B2239 3FDBEE40 5525C9EB 5A450CF2
      909A7569 FC96F424 56BD7D86 65B70B4D EB24620D FD48A7BF
```

```
    temp =
                    E4CD 803E82C6 D10E8D8F 3E5A2A80 F4A49F5C
         3DE4E594 6995FBE2 131F6A3D AC66DB4D EE1AAC0C 37DABBB3
         1BB5F688 5BF6E94B FB19BD1C D4FCE1D9 68407E2A D9FA0BF4


s is
                      01 C99B007D 058DA21D 1B1E7CB4 5501E949
         3EB87BC9 CB28D32B F7C4263E D47B58CD B69BDC35 58186FB5
         7766376B ED10B7ED D297F633 7A39A9F9 C3B2D080 FC55B3F4


------------------------------------------------------------

First call to Generate

************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
  ------------
  i=0
  t is
                    01C9 9B007D05 8DA21D1B 1E7CB455 01E9493E
         B87BC9CB 28D32BF7 C4263ED4 7B58CDB6 9BDC3558 186FB577
         66376BED 10B7EDD2 97F6337A 39A9F9C3 B2D080FC 55B3F417


  s is
                    0184 DFADEDF9 52E25461 BB4AA1BE 30E71E61
         78684D7F E6B3780F FF07BA03 F6DF20C3 AED0F51B C87AF6EC
         BBE2B5B5 5C655A45 9E025132 56DBE4A6 C49D6030 7C083F80


  r is
                    006A 697A8313 798EE1D1 89871268 3F2D0B0D
         EE580414 6ABA64FD A8DB4E53 9CC8D1E5 9C74EE5A A48E73E9
         58C8EC85 DD529D42 E68B4F7E 02FFAF3E 3EF8312A EA68BC08


  ------------
  tmp is
```

```
                          7A8313 798EE1D1 89871268 3F2D0B0D
       EE580414 6ABA64FD A8DB4E53 9CC8D1E5 9C74EE5A A48E73E9
       58C8EC85 DD529D42 E68B4F7E 02FFAF3E 3EF8312A EA68BC08


  ------------
  i=1
  t is
                    0184 DFADEDF9 52E25461 BB4AA1BE 30E71E61
       78684D7F E6B3780F FF07BA03 F6DF20C3 AED0F51B C87AF6EC
       BBE2B5B5 5C655A45 9E025132 56DBE4A6 C49D6030 7C083F80


  s is
                    018C 12DF4800 2EACB926 2FF30ED4 602163F6
       DDAB9311 2D7B4DCE EAD88297 D3CFE0CF D90945EE F01945BE
       D9BDC506 907B28E8 7B999F72 1F739A6E F745BD2A A5BAD725


  r is
                    019C F8A41488 5E60A7DF 0B55F9D9 0210B319
       E9B8FD23 E078A415 3636F29A A3CAC819 8CB1D5D8 46151653
       ECE275A5 91089261 238014E5 05841006 5AB8229E B9115E8E


  ------------
  tmp is
                                              7A83 13798EE1
       D1898712 683F2D0B 0DEE5804 146ABA64 FDA8DB4E 539CC8D1
       E59C74EE 5AA48E73 E958C8EC 85DD529D 42E68B4F 7E02FFAF
       3E3EF831 2AEA68BC 08A41488 5E60A7DF 0B55F9D9 0210B319
       E9B8FD23 E078A415 3636F29A A3CAC819 8CB1D5D8 46151653
       ECE275A5 91089261 238014E5 05841006 5AB8229E B9115E8E


  ------------
  s is
                    00D7 29C6A475 1C7D84A8 D3E87130 520B9A2B
       BAF45403 4BDD399F CFB17E68 4CA699E1 23F5DB62 662800F4
       75A9968C 5B6ADD38 BB881123 82F60261 1129C3A0 337EF399


------------------------------------------------------------

Second call to Generate
```

```
************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
  ------------
  i=0
  t is
                    00D7 29C6A475 1C7D84A8 D3E87130 520B9A2B
        BAF45403 4BDD399F CFB17E68 4CA699E1 23F5DB62 662800F4
        75A9968C 5B6ADD38 BB881123 82F60261 1129C3A0 337EF399


  s is
                    01AB 2E84F361 48B8F19E 32CDC76A DA4B89CF
        4CB51665 03EA392A 694C42D4 EBC5EC40 4002F74F 147310C0
        F19C202B 0B8C723A A80EBE3D 856B9BFC 575CF0CE 4636FE40


  r is
                    0187 19918B5D 79E64664 966D954B C5E2946B
        F48F061B F0C2701C 3C2D1F75 EA821E1D A05D5B3C 2C4EEA24
        6E806B53 BF6BDB3F 3D53A3AE 756C2A45 C7260397 3A3DE1BC


  ------------
  tmp is
                          918B5D 79E64664 966D954B C5E2946B
        F48F061B F0C2701C 3C2D1F75 EA821E1D A05D5B3C 2C4EEA24
        6E806B53 BF6BDB3F 3D53A3AE 756C2A45 C7260397 3A3DE1BC


  ------------
  i=1
  t is
                    01AB 2E84F361 48B8F19E 32CDC76A DA4B89CF
        4CB51665 03EA392A 694C42D4 EBC5EC40 4002F74F 147310C0
        F19C202B 0B8C723A A80EBE3D 856B9BFC 575CF0CE 4636FE40


  s is
                    00F0 1FEAFD93 DE04000C 2A462427 46D650CD
        17630E80 E0C328FB A8B83509 345BBC18 2B3398F5 AC3E08AD
        F104E177 9C7B14D6 9FCC879E DD521C42 0223C48C 0D1D04E1
```

```
  r is
                    01A2 BB367C28 3CA124A5 589CEAB3 0E5D2D74
        8A40DD87 4FF15B03 2CF4F4B2 AAD590B0 DB91A0D3 8FCE93C5
        AAD4E55A C482F86F F06FAE66 B7C7CCA7 E45557E1 A5A3B85D


  ------------
  tmp is
                                                 918B 5D79E646
        64966D95 4BC5E294 6BF48F06 1BF0C270 1C3C2D1F 75EA821E
        1DA05D5B 3C2C4EEA 246E806B 53BF6BDB 3F3D53A3 AE756C2A
        45C72603 973A3DE1 BC367C28 3CA124A5 589CEAB3 0E5D2D74
        8A40DD87 4FF15B03 2CF4F4B2 AAD590B0 DB91A0D3 8FCE93C5
        AAD4E55A C482F86F F06FAE66 B7C7CCA7 E45557E1 A5A3B85D


  ------------
  s is
                    0178 3BF15984 3C3128B6 5859F3FE 386C7626
        17D41636 10290433 2108DC6C 316FAA03 6A07AA57 EE0E1B9B
        F764E118 0F3A2BA1 A6AC29E1 D6A302A0 85508337 38555EE8


rnd_val is
                                                 918B 5D79E646
        64966D95 4BC5E294 6BF48F06 1BF0C270 1C3C2D1F 75EA821E
        1DA05D5B 3C2C4EEA 246E806B 53BF6BDB 3F3D53A3 AE756C2A
        45C72603 973A3DE1 BC367C28 3CA124A5 589CEAB3 0E5D2D74
        8A40DD87 4FF15B03 2CF4F4B2 AAD590B0 DB91A0D3 8FCE93C5
        AAD4E55A C482F86F F06FAE66 B7C7CCA7 E45557E1 A5A3B85D


################################################################

DualEC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                             00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
```

```
    EntropyInput1 (for Reseed1) =
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    Nonce =
                           20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput1  =
                                                60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    AdditionalInput2  =
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


##################################################################

******************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    nonce is
                           20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"
```

```
Hash_df()
----------------------------
  no_of_bits_to_return = 521

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                                                    01 00000209
      00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
      18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


  Hash(counter||no_of_bits_to_return||input_string) is
                         E4CD803E 82C6D10E 8D8F3E5A 2A80F4A4
      9F5C3DE4 E5946995 FBE2131F 6A3DAC66 DB4DEE1A AC0C37DA
      BBB31BB5 F6885BF6 E94BFB19 BD1CD4FC E1D96840 7E2AD9FA


  temp =
                         E4CD803E 82C6D10E 8D8F3E5A 2A80F4A4
      9F5C3DE4 E5946995 FBE2131F 6A3DAC66 DB4DEE1A AC0C37DA
      BBB31BB5 F6885BF6 E94BFB19 BD1CD4FC E1D96840 7E2AD9FA


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                                                    02 00000209
      00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
      18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


  Hash(counter||no_of_bits_to_return||input_string) is
                         0BF4E84E 26C435F1 A8C9DDAF B866D3E9
      C7556662 F08A12DA AE1B2239 3FDBEE40 5525C9EB 5A450CF2
      909A7569 FC96F424 56BD7D86 65B70B4D EB24620D FD48A7BF


  temp =
                    E4CD 803E82C6 D10E8D8F 3E5A2A80 F4A49F5C
      3DE4E594 6995FBE2 131F6A3D AC66DB4D EE1AAC0C 37DABBB3
```

```
        1BB5F688 5BF6E94B FB19BD1C D4FCE1D9 68407E2A D9FA0BF4


s is
                      01 C99B007D 058DA21D 1B1E7CB4 5501E949
        3EB87BC9 CB28D32B F7C4263E D47B58CD B69BDC35 58186FB5
        7766376B ED10B7ED D297F633 7A39A9F9 C3B2D080 FC55B3F4


------------------------------------------------------------

First call to Generate

************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
                                            60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    requested_number_of_bits is 1008
  Hash_df()
  --------------------------
    no_of_bits_to_return = 521

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 00000209 60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    Hash(counter||no_of_bits_to_return||input_string) is
                          DD40BFFA 030E77F8 FA7D9879 56C20710
        375466E8 3CB744D8 C0446A19 281AC290 6B67BD14 F2D61258
        FABDD1B3 26CE70C3 A1598A72 68CCBAA0 8C8A2627 3214342D


    temp =
                          DD40BFFA 030E77F8 FA7D9879 56C20710
        375466E8 3CB744D8 C0446A19 281AC290 6B67BD14 F2D61258
        FABDD1B3 26CE70C3 A1598A72 68CCBAA0 8C8A2627 3214342D
```

```
  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                               02 00000209 60616263 64656667
      68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


  Hash(counter||no_of_bits_to_return||input_string) is
                        65976B23 DEBAE6F7 53B1ACC6 F0D9ADCF
      CB60A084 FA65AC58 81966BB9 8CD2EBCD 65575220 B97738B9
      5E3E883D B4078A79 F792E81E D23C19A1 8625F9B2 D681A407


  temp =
                    DD40 BFFA030E 77F8FA7D 987956C2 07103754
      66E83CB7 44D8C044 6A19281A C2906B67 BD14F2D6 1258FABD
      D1B326CE 70C3A159 8A7268CC BAA08C8A 26273214 342D6597


------------
i=0
t is
                    0073 1A7F8903 914DECEF E54C46F8 85E76950
      10B619B2 465A9A77 4CF20C84 4EDDED60 54A61CBD B44B0482
      1D940DA0 8C566A90 24E2D7AB A0DCB8DA A69CCE98 7DDBAEDC


s is
                    0123 1265E5A0 1AC55186 49AF0A53 7B9F1E7F
      CB0068CD 6B8BE36C D18FC8CE 194C5EEC FCEBA029 B45DC1F0
      3438D2F1 5B75E1EF 2C03BB3E EE7B25EF 875D25B5 47D71582


r is
                    012F A2C12142 4391C2D8 C9C494BA 80BB4C14
      CC7BAA11 DA7CBEA8 32635EC5 957C1913 E45A694C 9F33FADD
      FAFAD854 8B6AE7F3 827B9DD5 1A2E89D8 A452E6B1 13A8D437


------------
tmp is
                           C12142 4391C2D8 C9C494BA 80BB4C14
```

```
       CC7BAA11 DA7CBEA8 32635EC5 957C1913 E45A694C 9F33FADD
       FAFAD854 8B6AE7F3 827B9DD5 1A2E89D8 A452E6B1 13A8D437


  ------------
  i=1
  t is
                    0123 1265E5A0 1AC55186 49AF0A53 7B9F1E7F
       CB0068CD 6B8BE36C D18FC8CE 194C5EEC FCEBA029 B45DC1F0
       3438D2F1 5B75E1EF 2C03BB3E EE7B25EF 875D25B5 47D71582


  s is
                    0121 DA398754 ED51D31B BC0E3D9C 25DA44B8
       8C58588D 3EA1BD70 84278D83 3CB75BDB 65938DE9 4C0C917B
       D26F31FE 60CB8611 B7BE8DC4 B9A73D4A BC34A80C D8769F8B


  r is
                    01CE 4D103CEC C778E5F1 5F87C168 B0D3E95D
       E2556C17 141637D9 04F05A3B 6F3B22B5 0B95B06C E82808B0
       6661EFC7 E8B793C5 F05BE585 897BB8EE 32BA550F F8743764


  ------------
  tmp is
                                                 C121 424391C2
       D8C9C494 BA80BB4C 14CC7BAA 11DA7CBE A832635E C5957C19
       13E45A69 4C9F33FA DDFAFAD8 548B6AE7 F3827B9D D51A2E89
       D8A452E6 B113A8D4 37103CEC C778E5F1 5F87C168 B0D3E95D
       E2556C17 141637D9 04F05A3B 6F3B22B5 0B95B06C E82808B0
       6661EFC7 E8B793C5 F05BE585 897BB8EE 32BA550F F8743764


  ------------
  s is
                    01E7 96661838 BBFB2277 3A52BF87 9BE0C63B
       AE1A66FA CB0C761A 9361B15E 08E97565 089391BF 274EBDEF
       7A281444 D4D6B492 35A0FA55 D36442EF 4688C9BA D60DB8BB


----------------------------------------------------------------

Second call to Generate

****************************************************************
```

```
DualEC_DRBG_Generate_algorithm

    additional_input is
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    requested_number_of_bits is 1008
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 521

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 00000209 A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    Hash(counter||no_of_bits_to_return||input_string) is
                            DB75DB8E 03FA70C0 3ECD5F40 1DCE9119
        2CE3529B 213AB30F ED9781FD FB7576AB C820CD47 E953366B
        08CC3413 31C6D719 696B36E6 95E7A768 31AA2A3C 5299A50E


    temp =
                            DB75DB8E 03FA70C0 3ECD5F40 1DCE9119
        2CE3529B 213AB30F ED9781FD FB7576AB C820CD47 E953366B
        08CC3413 31C6D719 696B36E6 95E7A768 31AA2A3C 5299A50E


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 00000209 A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    Hash(counter||no_of_bits_to_return||input_string) is
                            941A4B0B 5B8431CD 2CEAC831 7B434043
        A2D385D1 7D912713 448773CA 4D3FC3C4 4397BD98 5AA68BDB
```

```
      01E39E52 6601E95C DD0002AC 0DD1B479 4476B12C 4DF0EF7A


  temp =
                  DB75 DB8E03FA 70C03ECD 5F401DCE 91192CE3
      529B213A B30FED97 81FDFB75 76ABC820 CD47E953 366B08CC
      341331C6 D719696B 36E695E7 A76831AA 2A3C5299 A50E941A


------------
i=0
t is
                  0051 7DD1043F 4F1AA20A A0EC3FBC 06C2F462
      68BF50B8 BE6A69C1 BC624AA8 E20422F5 49091E6D 81226BFE
      E2403227 59788640 E3CD377E 1C2A928C 12DCB11F E547A593


s is
                  0183 5B2634CD 556890DD 9B1872C6 7701AA3F
      EE112A27 3521BFDD 3DC0C047 AF3EBC43 44C615B6 85877378
      0B61DFE9 D59409CF BB30CB68 9B433D98 A917070E 535F0112


r is
                  0091 3990182A E9EBE7AC B67F5198 56E5A591
      F2AECAB9 3E0D3BFE CDFAC9BA 3263A346 61F682DC 8A9919F8
      184CAE4E 0E7CBD0E 97484985 728C2129 6E3FD78B 544586F0


------------
tmp is
                        90182A E9EBE7AC B67F5198 56E5A591
      F2AECAB9 3E0D3BFE CDFAC9BA 3263A346 61F682DC 8A9919F8
      184CAE4E 0E7CBD0E 97484985 728C2129 6E3FD78B 544586F0


------------
i=1
t is
                  0183 5B2634CD 556890DD 9B1872C6 7701AA3F
      EE112A27 3521BFDD 3DC0C047 AF3EBC43 44C615B6 85877378
      0B61DFE9 D59409CF BB30CB68 9B433D98 A917070E 535F0112


s is
                  0073 D92FFD61 4142EC08 313ECC5B 7836DF5F
```

```
        49538058 22742606 99212E29 7F2906CA F7AF9478 A8F036B2
        A3D6090F FD111C0C E8E68345 7870131A E883D6B8 B90E15B0


  r is
                    01B0 A8B84ECE C65888F2 7C435787 9ABC41C9
        874CB9DD FE50D295 A09C5CB0 503C6605 64185B13 F715C39B
        321F921D 3F110679 C3A0793A B713A933 509CE35D 94A0534B


  ------------
  tmp is
                                                9018 2AE9EBE7
        ACB67F51 9856E5A5 91F2AECA B93E0D3B FECDFAC9 BA3263A3
        4661F682 DC8A9919 F8184CAE 4E0E7CBD 0E974849 85728C21
        296E3FD7 8B544586 F0B84ECE C65888F2 7C435787 9ABC41C9
        874CB9DD FE50D295 A09C5CB0 503C6605 64185B13 F715C39B
        321F921D 3F110679 C3A0793A B713A933 509CE35D 94A0534B


  ------------
  s is
                    0165 2BE6B646 E49827CE 61BF98AF 4028194D
        AF0C8B23 506CA931 9EAC5953 1BA39AB8 BF3F0109 2A9EACAA
        AB8C8AE8 EC90AA94 69867DDD DC0FFE71 12A82ADB 15A308BD


rnd_val is
                                                9018 2AE9EBE7
        ACB67F51 9856E5A5 91F2AECA B93E0D3B FECDFAC9 BA3263A3
        4661F682 DC8A9919 F8184CAE 4E0E7CBD 0E974849 85728C21
        296E3FD7 8B544586 F0B84ECE C65888F2 7C435787 9ABC41C9
        874CB9DD FE50D295 A09C5CB0 503C6605 64185B13 F715C39B
        321F921D 3F110679 C3A0793A B713A933 509CE35D 94A0534B


###############################################################

DualEC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
```

```
                                            00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                            80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                            C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString =
                                            40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    AdditionalInput = <empty>

###############################################################

***************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                                            00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    nonce is
                          20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
                                            40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    prediction_resistance_flag = "No PredictionResistance"
```

```
Hash_df()
----------------------------
  no_of_bits_to_return = 521

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                               01 00000209 00010203 04050607
      08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
      20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
      48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


  Hash(counter||no_of_bits_to_return||input_string) is
                         FFAE2834 4D1E7E85 C08DCD7A 4643D401
      2FDC1557 F0012317 50ED5169 571DF59C 27835ECB 69B35314
      9744C13B 022FD21F 1797B206 56766C32 943DA50D 3ED374BD


  temp =
                         FFAE2834 4D1E7E85 C08DCD7A 4643D401
      2FDC1557 F0012317 50ED5169 571DF59C 27835ECB 69B35314
      9744C13B 022FD21F 1797B206 56766C32 943DA50D 3ED374BD


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                               02 00000209 00010203 04050607
      08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
      20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
      48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


  Hash(counter||no_of_bits_to_return||input_string) is
                         13B24000 56345ED8 7121E329 23656AF5
      63CB0C9F 6FA3F671 1A31A9EE 306A0962 01A9509E 8EEDA764
      EA71EFC6 9FE343AB 0CFD0CEF 5B7547C0 A1D66875 2BE96C9E


  temp =
```

```
                    FFAE 28344D1E 7E85C08D CD7A4643 D4012FDC
        1557F001 231750ED 5169571D F59C2783 5ECB69B3 53149744
        C13B022F D21F1797 B2065676 6C32943D A50D3ED3 74BD13B2


s is
                      01 FF5C5068 9A3CFD0B 811B9AF4 8C87A802
        5FB82AAF E002462E A1DAA2D2 AE3BEB38 4F06BD96 D366A629
        2E898276 045FA43E 2F2F640C ACECD865 287B4A1A 7DA6E97A


------------------------------------------------------------

First call to Generate

************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
  ------------
  i=0
  t is
                    01FF 5C50689A 3CFD0B81 1B9AF48C 87A8025F
        B82AAFE0 02462EA1 DAA2D2AE 3BEB384F 06BD96D3 66A6292E
        89827604 5FA43E2F 2F640CAC ECD86528 7B4A1A7D A6E97A27


  s is
                    007E 47C9EB86 4BBD8EE2 318C49C8 E830C129
        0F3187A3 E426A3F9 D1B956AC DFF74E9F 527E523C 52B576C1
        FD400C98 089B76D7 840212D5 222EC870 0C6002D3 EA4B842F


  r is
                    01B9 4CB233F4 1CF7DA2F 6F3FD39C 2F9301C3
        9352A16D 0035143E 27F970F6 3C205E7B 5C5D59A4 48DB4D96
        2D9A8C57 C6ADD612 D024D5B5 2D3B800E 163838EB 173AE77F


  ------------
  tmp is
                           B233F4 1CF7DA2F 6F3FD39C 2F9301C3
        9352A16D 0035143E 27F970F6 3C205E7B 5C5D59A4 48DB4D96
```

```
       2D9A8C57 C6ADD612 D024D5B5 2D3B800E 163838EB 173AE77F


  ------------
  i=1
  t is
                    007E 47C9EB86 4BBD8EE2 318C49C8 E830C129
       0F3187A3 E426A3F9 D1B956AC DFF74E9F 527E523C 52B576C1
       FD400C98 089B76D7 840212D5 222EC870 0C6002D3 EA4B842F


  s is
                    01E5 761AE4AE 582DA988 08B0E444 9EBF11EB
       8F42685E 204A128C F38AC41B ECF17CCF C139C3E3 52CC5E68
       603A9B1E CD179648 F70F6C66 4BE2F6B7 7BC78FF1 F3A52A11


  r is
                    0168 95B56219 F41A9238 49628632 6F011DCB
       2E09037E ED6680E0 3324474A 2410E0FB 0541A168 107DEF5B
       ED3B468F 8EF30276 3D7FE745 C85720F8 A33C52C4 42370E60


  ------------
  tmp is
                                                 B233 F41CF7DA
       2F6F3FD3 9C2F9301 C39352A1 6D003514 3E27F970 F63C205E
       7B5C5D59 A448DB4D 962D9A8C 57C6ADD6 12D024D5 B52D3B80
       0E163838 EB173AE7 7FB56219 F41A9238 49628632 6F011DCB
       2E09037E ED6680E0 3324474A 2410E0FB 0541A168 107DEF5B
       ED3B468F 8EF30276 3D7FE745 C85720F8 A33C52C4 42370E60


  ------------
  s is
                    0109 37EBC4D9 37641E0C 57D80A32 AD16FFF5
       40A54D29 2E71491C 857D5DC1 B8DB4AE2 D374A356 921C4F67
       5A6421BE EB6D43DD 3B9E3DF3 19B2958D 8A86153E A3312B7C


---------------------------------------------------------------

Second call to Generate

***************************************************************
```

```
DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
  ------------
  i=0
  t is
                      0109 37EBC4D9 37641E0C 57D80A32 AD16FFF5
        40A54D29 2E71491C 857D5DC1 B8DB4AE2 D374A356 921C4F67
        5A6421BE EB6D43DD 3B9E3DF3 19B2958D 8A86153E A3312B7C


  s is
                      01DC DA5DDB2F 61019B11 9B3B6818 64B9042C
        A9829995 84A9C3DD F726A398 AAE586FC BC517A19 BD51D421
        40785C4E 6D498E3D B4FF90D2 8D8B7A80 C61432AA BF4AE9B3


  r is
                      01B7 12EEAF0F AEDE0D3E 25B25A79 48F1B3DE
        57972757 1FDA50E7 921E2D43 F59F2815 12AF3DDA 8A3E8AF6
        BE0F6202 C97DEA78 2B9A13C7 5D042306 7527F266 1D49A5BF


  ------------
  tmp is
                            EEAF0F AEDE0D3E 25B25A79 48F1B3DE
        57972757 1FDA50E7 921E2D43 F59F2815 12AF3DDA 8A3E8AF6
        BE0F6202 C97DEA78 2B9A13C7 5D042306 7527F266 1D49A5BF


  ------------
  i=1
  t is
                      01DC DA5DDB2F 61019B11 9B3B6818 64B9042C
        A9829995 84A9C3DD F726A398 AAE586FC BC517A19 BD51D421
        40785C4E 6D498E3D B4FF90D2 8D8B7A80 C61432AA BF4AE9B3


  s is
                      01BC 1B45D8D0 779FC5C8 68F53A20 98745744
        C5BDA16E 9D907A74 86E8A772 BE037D8E D2B199B7 F84719B3
        974649C2 0BD29410 9BA708F5 46F94A51 21C5CBA1 E2014A5B
```

```
  r is
                    010F 1B251DA4 A5750971 48B17EEF 8164CB47
        CC42B4B7 BF926827 A7E2E8E4 EB681C03 B6279C50 8F98F064
        594CD5C6 E0157A8B 3AFB6B12 B597F0B1 955D58A9 F5A2AA5B


  ------------
  tmp is
                                                EEAF 0FAEDE0D
        3E25B25A 7948F1B3 DE579727 571FDA50 E7921E2D 43F59F28
        1512AF3D DA8A3E8A F6BE0F62 02C97DEA 782B9A13 C75D0423
        067527F2 661D49A5 BF251DA4 A5750971 48B17EEF 8164CB47
        CC42B4B7 BF926827 A7E2E8E4 EB681C03 B6279C50 8F98F064
        594CD5C6 E0157A8B 3AFB6B12 B597F0B1 955D58A9 F5A2AA5B


  ------------
  s is
                    01A7 1FE27958 AAB33D33 764E22C1 C8237BA3
        A3AE7C4A 179A9F7D AC1A2809 D71185A8 182FF9C8 1185E779
        5FAA1BC8 DEBA36BD CE88BC27 E7845C5C 049001E7 7DE4E845


rnd_val is
                                                EEAF 0FAEDE0D
        3E25B25A 7948F1B3 DE579727 571FDA50 E7921E2D 43F59F28
        1512AF3D DA8A3E8A F6BE0F62 02C97DEA 782B9A13 C75D0423
        067527F2 661D49A5 BF251DA4 A5750971 48B17EEF 8164CB47
        CC42B4B7 BF926827 A7E2E8E4 EB681C03 B6279C50 8F98F064
        594CD5C6 E0157A8B 3AFB6B12 B597F0B1 955D58A9 F5A2AA5B


##############################################################

DualEC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                              00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
```

```
    EntropyInput1 (for Reseed1) =
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    Nonce =
                           20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString =
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    AdditionalInput1  =
                                                60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    AdditionalInput2  =
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


##################################################################

******************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    nonce is
                           20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
                                                40414243 44454647
```

```
      48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


  prediction_resistance_flag = "No PredictionResistance"

Hash_df()
----------------------------
  no_of_bits_to_return = 521

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                              01 00000209 00010203 04050607
      08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
      20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
      48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


  Hash(counter||no_of_bits_to_return||input_string) is
                        FFAE2834 4D1E7E85 C08DCD7A 4643D401
      2FDC1557 F0012317 50ED5169 571DF59C 27835ECB 69B35314
      9744C13B 022FD21F 1797B206 56766C32 943DA50D 3ED374BD


  temp =
                        FFAE2834 4D1E7E85 C08DCD7A 4643D401
      2FDC1557 F0012317 50ED5169 571DF59C 27835ECB 69B35314
      9744C13B 022FD21F 1797B206 56766C32 943DA50D 3ED374BD


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                              02 00000209 00010203 04050607
      08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
      20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
      48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


  Hash(counter||no_of_bits_to_return||input_string) is
                        13B24000 56345ED8 7121E329 23656AF5
      63CB0C9F 6FA3F671 1A31A9EE 306A0962 01A9509E 8EEDA764
```

```
        EA71EFC6 9FE343AB 0CFD0CEF 5B7547C0 A1D66875 2BE96C9E


    temp =
                      FFAE 28344D1E 7E85C08D CD7A4643 D4012FDC
        1557F001 231750ED 5169571D F59C2783 5ECB69B3 53149744
        C13B022F D21F1797 B2065676 6C32943D A50D3ED3 74BD13B2


s is
                        01 FF5C5068 9A3CFD0B 811B9AF4 8C87A802
        5FB82AAF E002462E A1DAA2D2 AE3BEB38 4F06BD96 D366A629
        2E898276 045FA43E 2F2F640C ACECD865 287B4A1A 7DA6E97A


------------------------------------------------------------

First call to Generate

************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
                                              60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    requested_number_of_bits is 1008
  Hash_df()
  --------------------------
    no_of_bits_to_return = 521

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                 01 00000209 60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    Hash(counter||no_of_bits_to_return||input_string) is
                           DD40BFFA 030E77F8 FA7D9879 56C20710
        375466E8 3CB744D8 C0446A19 281AC290 6B67BD14 F2D61258
        FABDD1B3 26CE70C3 A1598A72 68CCBAA0 8C8A2627 3214342D
```

```
  temp =
                       DD40BFFA 030E77F8 FA7D9879 56C20710
      375466E8 3CB744D8 C0446A19 281AC290 6B67BD14 F2D61258
      FABDD1B3 26CE70C3 A1598A72 68CCBAA0 8C8A2627 3214342D


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                              02 00000209 60616263 64656667
      68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


  Hash(counter||no_of_bits_to_return||input_string) is
                       65976B23 DEBAE6F7 53B1ACC6 F0D9ADCF
      CB60A084 FA65AC58 81966BB9 8CD2EBCD 65575220 B97738B9
      5E3E883D B4078A79 F792E81E D23C19A1 8625F9B2 D681A407


  temp =
                   DD40 BFFA030E 77F8FA7D 987956C2 07103754
      66E83CB7 44D8C044 6A19281A C2906B67 BD14F2D6 1258FABD
      D1B326CE 70C3A159 8A7268CC BAA08C8A 26273214 342D6597


------------
i=0
t is
                   0045 DD2F9C9C 2012FA75 E0AA0621 03A62231
      10E77F99 6CCF9F21 5276E0FE 0E6E1899 C9C7BF36 CA8298DB
      F2211049 C345B96D 9C70E87D 75AD2431 6F065419 8E8120EC


s is
                   007E EA32A86F BC93635F 30E0A1C8 56BBDE35
      00E5111D DD21B932 6994FD0E E7714F27 2A29D975 45A39FEA
      8C3EE3C7 87DA3C5F 1C0EFC08 10C77B60 DF9EC715 CBAA14B4


r is
                   008D B19462C0 6F93A486 99E4783A B1543A0D
      F9174859 BBBC60D7 36163FE7 45BFF4FA 73F2577B BCC4FB1F
```

```
      6C0A7A53 8F57FB61 A386B236 C183A714 A5B0ACE3 D4D43302


------------
tmp is
                          9462C0 6F93A486 99E4783A B1543A0D
      F9174859 BBBC60D7 36163FE7 45BFF4FA 73F2577B BCC4FB1F
      6C0A7A53 8F57FB61 A386B236 C183A714 A5B0ACE3 D4D43302


------------
i=1
t is
                  007E EA32A86F BC93635F 30E0A1C8 56BBDE35
      00E5111D DD21B932 6994FD0E E7714F27 2A29D975 45A39FEA
      8C3EE3C7 87DA3C5F 1C0EFC08 10C77B60 DF9EC715 CBAA14B4


s is
                  01CC 4EE0CC06 83713A92 F7306BB2 208983D2
      06275779 4EC9018F 78BD5967 FCE18C90 374CDFBA 2D7142BF
      B55E24BB 5D72BB6D 2C6940AB 7C229C53 C8CF8DEB 699A8B63


r is
                  0077 2943A243 0193DF55 5FE116DE 25A7BC5A
      EA1A3E35 15D0026C A1F77B1E 84158DE7 F4E7A400 74368611
      4FD580B5 EE792444 6749B8D0 984D4B4F 3AF9D75A BC055F8B


------------
tmp is
                                                9462 C06F93A4
      8699E478 3AB1543A 0DF91748 59BBBC60 D736163F E745BFF4
      FA73F257 7BBCC4FB 1F6C0A7A 538F57FB 61A386B2 36C183A7
      14A5B0AC E3D4D433 0243A243 0193DF55 5FE116DE 25A7BC5A
      EA1A3E35 15D0026C A1F77B1E 84158DE7 F4E7A400 74368611
      4FD580B5 EE792444 6749B8D0 984D4B4F 3AF9D75A BC055F8B


------------
s is
                  00C9 B2309A19 05D548A4 A50607F2 E48FB4F5
      1634A566 09BE01C3 1B0EAE8E 4490A582 0AE5EFA5 9E2BA363
      98E7DA97 4DD3DCF8 9DEF6432 F8B22640 930B2C72 9C54E4CA
```

```
---------------------------------------------------------------

Second call to Generate

***************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    requested_number_of_bits is 1008
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 521

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 00000209 A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    Hash(counter||no_of_bits_to_return||input_string) is
                           DB75DB8E 03FA70C0 3ECD5F40 1DCE9119
        2CE3529B 213AB30F ED9781FD FB7576AB C820CD47 E953366B
        08CC3413 31C6D719 696B36E6 95E7A768 31AA2A3C 5299A50E


    temp =
                           DB75DB8E 03FA70C0 3ECD5F40 1DCE9119
        2CE3529B 213AB30F ED9781FD FB7576AB C820CD47 E953366B
        08CC3413 31C6D719 696B36E6 95E7A768 31AA2A3C 5299A50E


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 00000209 A0A1A2A3 A4A5A6A7
```

```
      A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


  Hash(counter||no_of_bits_to_return||input_string) is
                         941A4B0B 5B8431CD 2CEAC831 7B434043
      A2D385D1 7D912713 448773CA 4D3FC3C4 4397BD98 5AA68BDB
      01E39E52 6601E95C DD0002AC 0DD1B479 4476B12C 4DF0EF7A


  temp =
                   DB75 DB8E03FA 70C03ECD 5F401DCE 91192CE3
      529B213A B30FED97 81FDFB75 76ABC820 CD47E953 366B08CC
      341331C6 D719696B 36E695E7 A76831AA 2A3C5299 A50E941A


------------
i=0
t is
                   017F 5987861E F134C8D9 3FB887C9 79AD86AC
      D0919324 7CD81E18 340D5578 AE7DF212 4B7F6077 38477572
      008FFCF4 C07DEE2A 4B82A919 37FCF623 C75F54D7 AF1EF9E2


s is
                   002E 0F52033E 2A853582 B286F4DE 50D509B5
      8D68D0D8 68A7403B B0C9B806 A3CC092B 7C5BC376 47FD7D8A
      4BECC9DA C1B1E701 4EF154C8 8A3BC58F 6E932255 144AD0A6


r is
                   01CA 8B789408 89105781 A9DCAAA2 0D1B8A0F
      2FDC1572 373F5175 51E015F5 04F260C2 5C4B7AE7 C4C012F1
      07670EDE 138FCD6E 690240F4 A184801A E84664E3 5299B4B3


------------
tmp is
                     789408 89105781 A9DCAAA2 0D1B8A0F
      2FDC1572 373F5175 51E015F5 04F260C2 5C4B7AE7 C4C012F1
      07670EDE 138FCD6E 690240F4 A184801A E84664E3 5299B4B3


------------
i=1
t is
                   002E 0F52033E 2A853582 B286F4DE 50D509B5
```

```
        8D68D0D8 68A7403B B0C9B806 A3CC092B 7C5BC376 47FD7D8A
        4BECC9DA C1B1E701 4EF154C8 8A3BC58F 6E932255 144AD0A6


  s is
                    00A3 40652AF2 F5C3A4A6 F2A9CDC0 775CD7D3
        86E930B3 D80B271F 1FF86BF7 79D7B042 B85234F4 5814AAF5
        00F509ED 890980A4 C4603074 5F190C73 BF4B4E84 6AAB9111


  r is
                    00BE 3CCEA434 4724560B 0E8BC01E 6F4DE330
        A94E31B0 4E88A93F 7C8DAFAE F749E23B F92961A5 B81F2DDD
        7C465E21 15DB831A BBFEFDBD F399E8E8 4C822AD6 A674F210


  ------------
  tmp is
                                                7894 08891057
        81A9DCAA A20D1B8A 0F2FDC15 72373F51 7551E015 F504F260
        C25C4B7A E7C4C012 F107670E DE138FCD 6E690240 F4A18480
        1AE84664 E35299B4 B3CEA434 4724560B 0E8BC01E 6F4DE330
        A94E31B0 4E88A93F 7C8DAFAE F749E23B F92961A5 B81F2DDD
        7C465E21 15DB831A BBFEFDBD F399E8E8 4C822AD6 A674F210


  ------------
  s is
                    014E CB76781E 6CA03B01 CE5664C7 11A26260
        EBEA9536 92176FA6 987A8070 F4C5418C 617D949B DA529DE0
        43EB2619 54F8A4A5 4F2AEE0D 693D12C0 AF365029 34B1AF5E


rnd_val is
                                                7894 08891057
        81A9DCAA A20D1B8A 0F2FDC15 72373F51 7551E015 F504F260
        C25C4B7A E7C4C012 F107670E DE138FCD 6E690240 F4A18480
        1AE84664 E35299B4 B3CEA434 4724560B 0E8BC01E 6F4DE330
        A94E31B0 4E88A93F 7C8DAFAE F749E23B F92961A5 B81F2DDD
        7C465E21 15DB831A BBFEFDBD F399E8E8 4C822AD6 A674F210


############################################################

DualEC_DRBG
```

```
    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                              00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                              80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                              C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                                              00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    nonce is
                          20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"
```

```
Hash_df()
----------------------------
  no_of_bits_to_return = 521

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                                                    01 00000209
      00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
      18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


  Hash(counter||no_of_bits_to_return||input_string) is
                         E4CD803E 82C6D10E 8D8F3E5A 2A80F4A4
      9F5C3DE4 E5946995 FBE2131F 6A3DAC66 DB4DEE1A AC0C37DA
      BBB31BB5 F6885BF6 E94BFB19 BD1CD4FC E1D96840 7E2AD9FA


  temp =
                         E4CD803E 82C6D10E 8D8F3E5A 2A80F4A4
      9F5C3DE4 E5946995 FBE2131F 6A3DAC66 DB4DEE1A AC0C37DA
      BBB31BB5 F6885BF6 E94BFB19 BD1CD4FC E1D96840 7E2AD9FA


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                                                    02 00000209
      00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
      18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


  Hash(counter||no_of_bits_to_return||input_string) is
                         0BF4E84E 26C435F1 A8C9DDAF B866D3E9
      C7556662 F08A12DA AE1B2239 3FDBEE40 5525C9EB 5A450CF2
      909A7569 FC96F424 56BD7D86 65B70B4D EB24620D FD48A7BF


  temp =
                    E4CD 803E82C6 D10E8D8F 3E5A2A80 F4A49F5C
      3DE4E594 6995FBE2 131F6A3D AC66DB4D EE1AAC0C 37DABBB3
```

```
        1BB5F688 5BF6E94B FB19BD1C D4FCE1D9 68407E2A D9FA0BF4


s is
                      01 C99B007D 058DA21D 1B1E7CB4 5501E949
        3EB87BC9 CB28D32B F7C4263E D47B58CD B69BDC35 58186FB5
        7766376B ED10B7ED D297F633 7A39A9F9 C3B2D080 FC55B3F4


------------------------------------------------------------

First call to Generate

************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
Generate FAILED: Reseed is required
************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                                            80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    additional_input is  <empty>

  Hash_df()
  --------------------------
    no_of_bits_to_return = 521

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                              010000 0209E4CD
        803E82C6 D10E8D8F 3E5A2A80 F4A49F5C 3DE4E594 6995FBE2
        131F6A3D AC66DB4D EE1AAC0C 37DABBB3 1BB5F688 5BF6E94B
        FB19BD1C D4FCE1D9 68407E2A D9FA0B80 80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                         6FF8D7B4 7F5CB216 28E52304 2C2EE652
        44989379 160501FB 3385FA1E 969DCE4F 7E767642 7280F8B0
        CE10DAE5 232CEB20 17981B0D 63B21295 E8169BDA 9B3ACC02


    temp =
                         6FF8D7B4 7F5CB216 28E52304 2C2EE652
        44989379 160501FB 3385FA1E 969DCE4F 7E767642 7280F8B0
        CE10DAE5 232CEB20 17981B0D 63B21295 E8169BDA 9B3ACC02


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                 020000 0209E4CD
        803E82C6 D10E8D8F 3E5A2A80 F4A49F5C 3DE4E594 6995FBE2
        131F6A3D AC66DB4D EE1AAC0C 37DABBB3 1BB5F688 5BF6E94B
        FB19BD1C D4FCE1D9 68407E2A D9FA0B80 80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    Hash(counter||no_of_bits_to_return||input_string) is
                         CD251E66 D6CDD324 FAE2776E E4A929DB
        B40B7FBF 3F507A25 26F9F641 99823BED 2546D568 0E294FA1
        FE22D539 98721A5E 9AC16DB2 03BAA2D6 D490B4BE 780E63AB


    temp =
                     6FF8 D7B47F5C B21628E5 23042C2E E6524498
        93791605 01FB3385 FA1E969D CE4F7E76 76427280 F8B0CE10
        DAE5232C EB201798 1B0D63B2 1295E816 9BDA9B3A CC02CD25


s is
                       00 DFF1AF68 FEB9642C 51CA4608 585DCCA4
        893126F2 2C0A03F6 670BF43D 2D3B9C9E FCECEC84 E501F161
        9C21B5CA 4659D640 2F30361A C764252B D02D37B5 36759805


************************************************************
```

```
DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
  ------------
  i=0
  t is
                     00DF F1AF68FE B9642C51 CA460858 5DCCA489
        3126F22C 0A03F667 0BF43D2D 3B9C9EFC ECEC84E5 01F1619C
        21B5CA46 59D6402F 30361AC7 64252BD0 2D37B536 7598059A


  s is
                     0083 30653E13 A4748FFB A78E01AB 49190611
        22F66327 2C458D53 9AF06964 6B599B77 C2CA8C26 4FE9C88A
        6775E827 CC6212D5 6EE4C16E 18FEC8B0 1E6ECB33 DAD5725C


  r is
                     01F0 94CC7035 C730405C F5DF7137 ED9E1074
        4B75B540 AFFC68EB 564B71C0 F737E8F6 56B61719 40497FA9
        0D8F383E FB6FC671 7BA14AAA 164EF566 41C0F513 312551DC


  ------------
  tmp is
                           CC7035 C730405C F5DF7137 ED9E1074
        4B75B540 AFFC68EB 564B71C0 F737E8F6 56B61719 40497FA9
        0D8F383E FB6FC671 7BA14AAA 164EF566 41C0F513 312551DC


  ------------
  i=1
  t is
                     0083 30653E13 A4748FFB A78E01AB 49190611
        22F66327 2C458D53 9AF06964 6B599B77 C2CA8C26 4FE9C88A
        6775E827 CC6212D5 6EE4C16E 18FEC8B0 1E6ECB33 DAD5725C


  s is
                     01B9 93CFCFFE 46AC4CBF A396EC57 8D9A53DB
        547F7A3A 2374D4FD FE358857 1A8176D0 4D3F8247 8C172202
        98192057 62A89E00 8FD25175 C54F8DC5 C9F29323 3006F035
```

```
  r is
                    0173 83D21D0A 5B0DBDCD 97F627E9 68DFD752
        56C11CF2 BCCA5822 EAACE796 A34CB7D2 F8CD8CC6 DBE76274
        498289BB C4C2F1CA DA6185D8 2605CF99 2EC285BC 4945EE9E


  ------------
  tmp is
                                                CC70 35C73040
        5CF5DF71 37ED9E10 744B75B5 40AFFC68 EB564B71 C0F737E8
        F656B617 1940497F A90D8F38 3EFB6FC6 717BA14A AA164EF5
        6641C0F5 13312551 DCD21D0A 5B0DBDCD 97F627E9 68DFD752
        56C11CF2 BCCA5822 EAACE796 A34CB7D2 F8CD8CC6 DBE76274
        498289BB C4C2F1CA DA6185D8 2605CF99 2EC285BC 4945EE9E


  ------------
  s is
                    0070 45526E05 494A03D2 35B291BC 79A8E138
        3DE73F74 AEF11435 527FBDA7 FF116508 148193D4 68609096
        87BE6855 099206DE 1E1D8F8D DD87FD8C EC321F19 B9E67338


----------------------------------------------------------------

Second call to Generate

****************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
Generate FAILED: Reseed is required
****************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                                            C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    additional_input is  <empty>
```

```
Hash_df()
----------------------------
  no_of_bits_to_return = 521

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                                                 010000 02093822
      A93702A4 A501E91A D948DE3C D4709C1E F39FBA57 788A1AA9
      3FDED3FF 88B2840A 40C9EA34 30484B43 DF342A84 C9036F0F
      0EC7C6EE C3FEC676 190F8CDC F3399C00 C0C1C2C3 C4C5C6C7
      C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


  Hash(counter||no_of_bits_to_return||input_string) is
                        9F748EAB 34B6E861 36A34F9B 50E0E695
      F78C9E12 4C90F392 6B8A174F F7CFF986 99097F61 675E346B
      FE834A45 7A8347D4 1825D774 E4E45B98 74AE6810 D9D5F758


  temp =
                        9F748EAB 34B6E861 36A34F9B 50E0E695
      F78C9E12 4C90F392 6B8A174F F7CFF986 99097F61 675E346B
      FE834A45 7A8347D4 1825D774 E4E45B98 74AE6810 D9D5F758


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                                                 020000 02093822
      A93702A4 A501E91A D948DE3C D4709C1E F39FBA57 788A1AA9
      3FDED3FF 88B2840A 40C9EA34 30484B43 DF342A84 C9036F0F
      0EC7C6EE C3FEC676 190F8CDC F3399C00 C0C1C2C3 C4C5C6C7
      C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


  Hash(counter||no_of_bits_to_return||input_string) is
                        33740A7D 1EF1977F 507E9177 C152BEA5
      C70DB477 0267C11D 1C1019A7 DEC43331 9E15FFC8 B4298E36
      3DCCE478 1C824BAF E19422B7 214C0492 E8900E5A 492E103B
```

```
    temp =
                      9F74 8EAB34B6 E86136A3 4F9B50E0 E695F78C
         9E124C90 F3926B8A 174FF7CF F9869909 7F61675E 346BFE83
         4A457A83 47D41825 D774E4E4 5B9874AE 6810D9D5 F7583374


s is
                        01 3EE91D56 696DD0C2 6D469F36 A1C1CD2B
         EF193C24 9921E724 D7142E9F EF9FF30D 3212FEC2 CEBC68D7
         FD06948A F5068FA8 304BAEE9 C9C8B730 E95CD021 B3ABEEB0


************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
  ------------
  i=0
  t is
                      013E E91D5669 6DD0C26D 469F36A1 C1CD2BEF
         193C2499 21E724D7 142E9FEF 9FF30D32 12FEC2CE BC68D7FD
         06948AF5 068FA830 4BAEE9C9 C8B730E9 5CD021B3 ABEEB066


  s is
                      0152 3C6A9E3F 8676F0CF 659B9AA0 12524176
         45178E38 1AB13BAA 171F9317 66AE6B7D 295CE3C6 21A29228
         50BA7236 5F5709CD 2DC0EB4E DADFE148 3CDD4A11 FFE03182


  r is
                      012B 5B0E6C32 9AD1BE68 1EB1E6F5 E03A89E3
         D80153D6 CCDD5A3E CF865003 EE4A2DE5 A23B7F43 681361CF
         AFC3A3FE F17777E7 5CF9D668 5573C887 A3962CB9 55076D45


  ------------
  tmp is
                           0E6C32 9AD1BE68 1EB1E6F5 E03A89E3
         D80153D6 CCDD5A3E CF865003 EE4A2DE5 A23B7F43 681361CF
         AFC3A3FE F17777E7 5CF9D668 5573C887 A3962CB9 55076D45
```

```
  ------------
  i=1
  t is
                    0152 3C6A9E3F 8676F0CF 659B9AA0 12524176
        45178E38 1AB13BAA 171F9317 66AE6B7D 295CE3C6 21A29228
        50BA7236 5F5709CD 2DC0EB4E DADFE148 3CDD4A11 FFE03182


  s is
                    014D 744125FF 85FA1354 EE5A5F07 1D594335
        0603543C 17149140 B87907C7 85B984F0 4C3DE2AF 2B8F186B
        F30442D3 250BA25B E0ADADE3 0D25F8ED 3578E4AB E7A9FCAF


  r is
                    0137 31D6F1E4 5EE4B8CB 31A4731C DA031FA2
        815B6D34 E29F2603 526CE186 576F4CCA 3FEDF7F8 ACDB37C9
        9D762706 ABE4967D 44739C8C FCFCC76C 58B1ED24 3AC394C0


  ------------
  tmp is
                                                0E6C 329AD1BE
        681EB1E6 F5E03A89 E3D80153 D6CCDD5A 3ECF8650 03EE4A2D
        E5A23B7F 43681361 CFAFC3A3 FEF17777 E75CF9D6 685573C8
        87A3962C B955076D 45D6F1E4 5EE4B8CB 31A4731C DA031FA2
        815B6D34 E29F2603 526CE186 576F4CCA 3FEDF7F8 ACDB37C9
        9D762706 ABE4967D 44739C8C FCFCC76C 58B1ED24 3AC394C0


  ------------
  s is
                    00DD 55587B02 0FD02426 2799D5E8 9A1A839F
        4B04EC08 BCE4836F 19464A7F D0002EF0 40BC621A 48782B1B
        1D403002 AEE59428 0F0675A9 C691A764 2ED6DBC6 C26B1771


rnd_val is
                                                0E6C 329AD1BE
        681EB1E6 F5E03A89 E3D80153 D6CCDD5A 3ECF8650 03EE4A2D
        E5A23B7F 43681361 CFAFC3A3 FEF17777 E75CF9D6 685573C8
        87A3962C B955076D 45D6F1E4 5EE4B8CB 31A4731C DA031FA2
        815B6D34 E29F2603 526CE186 576F4CCA 3FEDF7F8 ACDB37C9
        9D762706 ABE4967D 44739C8C FCFCC76C 58B1ED24 3AC394C0
```

```
##############################################################

DualEC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                              00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                              80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                              C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput1  =
                                              60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    AdditionalInput2  =
                                              A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


##############################################################

**************************************************************

DualEC_DRBG_Instantiate_algorithm
```

```
  entropy_input is
                                                00010203 04050607
      08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


  nonce is
                        20212223 24252627 28292A2B 2C2D2E2F


  personal_str is  <empty>

  prediction_resistance_flag = "PredictionResistance"

Hash_df()
----------------------------
  no_of_bits_to_return = 521

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                                                    01 00000209
      00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
      18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


  Hash(counter||no_of_bits_to_return||input_string) is
                        E4CD803E 82C6D10E 8D8F3E5A 2A80F4A4
      9F5C3DE4 E5946995 FBE2131F 6A3DAC66 DB4DEE1A AC0C37DA
      BBB31BB5 F6885BF6 E94BFB19 BD1CD4FC E1D96840 7E2AD9FA


  temp =
                        E4CD803E 82C6D10E 8D8F3E5A 2A80F4A4
      9F5C3DE4 E5946995 FBE2131F 6A3DAC66 DB4DEE1A AC0C37DA
      BBB31BB5 F6885BF6 E94BFB19 BD1CD4FC E1D96840 7E2AD9FA


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                                                    02 00000209
      00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
```

```
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    Hash(counter||no_of_bits_to_return||input_string) is
                          0BF4E84E 26C435F1 A8C9DDAF B866D3E9
        C7556662 F08A12DA AE1B2239 3FDBEE40 5525C9EB 5A450CF2
        909A7569 FC96F424 56BD7D86 65B70B4D EB24620D FD48A7BF


    temp =
                     E4CD 803E82C6 D10E8D8F 3E5A2A80 F4A49F5C
        3DE4E594 6995FBE2 131F6A3D AC66DB4D EE1AAC0C 37DABBB3
        1BB5F688 5BF6E94B FB19BD1C D4FCE1D9 68407E2A D9FA0BF4


s is
                       01 C99B007D 058DA21D 1B1E7CB4 5501E949
        3EB87BC9 CB28D32B F7C4263E D47B58CD B69BDC35 58186FB5
        7766376B ED10B7ED D297F633 7A39A9F9 C3B2D080 FC55B3F4


------------------------------------------------------------

First call to Generate

**************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
                                            60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    requested_number_of_bits is 1008
Generate FAILED: Reseed is required
**************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                                            80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    additional_input is
```

```
                                                60616263 64656667
      68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


Hash_df()
----------------------------
  no_of_bits_to_return = 521

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                           010000 0209E4CD 803E82C6 D10E8D8F
      3E5A2A80 F4A49F5C 3DE4E594 6995FBE2 131F6A3D AC66DB4D
      EE1AAC0C 37DABBB3 1BB5F688 5BF6E94B FB19BD1C D4FCE1D9
      68407E2A D9FA0B80 80818283 84858687 88898A8B 8C8D8E8F
      90919293 94959697 98999A9B 9C9D9E9F 60616263 64656667
      68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


  Hash(counter||no_of_bits_to_return||input_string) is
                         B55DB916 3FE7CD2C 33683701 6001C24E
      94DF2D24 90EE2EB4 7AF051FB E7F186A3 B46217B2 D998E376
      EE66AE04 61CA6155 8E5906EE 12D9D633 A4F37C7B 79B47667


  temp =
                         B55DB916 3FE7CD2C 33683701 6001C24E
      94DF2D24 90EE2EB4 7AF051FB E7F186A3 B46217B2 D998E376
      EE66AE04 61CA6155 8E5906EE 12D9D633 A4F37C7B 79B47667


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                           020000 0209E4CD 803E82C6 D10E8D8F
      3E5A2A80 F4A49F5C 3DE4E594 6995FBE2 131F6A3D AC66DB4D
      EE1AAC0C 37DABBB3 1BB5F688 5BF6E94B FB19BD1C D4FCE1D9
      68407E2A D9FA0B80 80818283 84858687 88898A8B 8C8D8E8F
      90919293 94959697 98999A9B 9C9D9E9F 60616263 64656667
      68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                          C8EFD0FA 5CA2202E F0F719FE EBB712AB
        1A47E1D0 82F5391B 82D05FFB C90AF393 736F7AF1 22798AA1
        1E7394FB 57297FE1 CD8E0C13 274DA456 F2FADB85 7643AF08


    temp =
                     B55D B9163FE7 CD2C3368 37016001 C24E94DF
        2D2490EE 2EB47AF0 51FBE7F1 86A3B462 17B2D998 E376EE66
        AE0461CA 61558E59 06EE12D9 D633A4F3 7C7B79B4 7667C8EF


s is
                       01 6ABB722C 7FCF9A58 66D06E02 C003849D
        29BE5A49 21DC5D68 F5E0A3F7 CFE30D47 68C42F65 B331C6ED
        DCCD5C08 C394C2AB 1CB20DDC 25B3AC67 49E6F8F6 F368ECCF


**************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
  ------------
  i=0
  t is
                     016A BB722C7F CF9A5866 D06E02C0 03849D29
        BE5A4921 DC5D68F5 E0A3F7CF E30D4768 C42F65B3 31C6EDDC
        CD5C08C3 94C2AB1C B20DDC25 B3AC6749 E6F8F6F3 68ECCF91


  s is
                     01FE 071FA43E E7329DCC A1E0D757 A4B0C5BA
        ACE64803 CA78DAE6 E0A9869A D1E2F691 9F890FA4 C4FFC098
        34AF37FB BDB33678 17E5290B 1F4E5933 0BA1D05A 341A40BC


  r is
                     01DF 6F00DB66 B6372D8D 6DC38BBE 048063D9
        AB0F7CDD 49A06DEC 668DE109 039D22DA D7A0B4A7 A68855DA
        752C8EDC 1CD36111 28C5C664 C6349543 9437C423 8482333B


  ------------
```

```
  tmp is
                            00DB66 B6372D8D 6DC38BBE 048063D9
        AB0F7CDD 49A06DEC 668DE109 039D22DA D7A0B4A7 A68855DA
        752C8EDC 1CD36111 28C5C664 C6349543 9437C423 8482333B


  ------------
  i=1
  t is
                     01FE 071FA43E E7329DCC A1E0D757 A4B0C5BA
        ACE64803 CA78DAE6 E0A9869A D1E2F691 9F890FA4 C4FFC098
        34AF37FB BDB33678 17E5290B 1F4E5933 0BA1D05A 341A40BC


  s is
                     00EB 5EFF4CA1 532110A5 D7B9E7BF 4799B003
        19D323E7 57192AF5 6905F82E C361355E 8845A00E 8D7EA8A3
        E01FEFDE E8BD6E4B 32E12386 714CC431 9C2782DD F3739149


  r is
                     0084 34E66A41 05A0F2E9 EF462C42 49A5468A
        0E7E6736 063A19E9 ACA84639 66B76B5D 6C5B17D5 8648D1A4
        A22FF4FA 1FF847BA 8E814E8F 323F9D71 75FF4EBD 592C72F9


  ------------
  tmp is
                                                  00DB 66B6372D
        8D6DC38B BE048063 D9AB0F7C DD49A06D EC668DE1 09039D22
        DAD7A0B4 A7A68855 DA752C8E DC1CD361 1128C5C6 64C63495
        439437C4 23848233 3BE66A41 05A0F2E9 EF462C42 49A5468A
        0E7E6736 063A19E9 ACA84639 66B76B5D 6C5B17D5 8648D1A4
        A22FF4FA 1FF847BA 8E814E8F 323F9D71 75FF4EBD 592C72F9


  ------------
  s is
                     011E 23D41ACD 554D5DAC 41B0D98E 18738D4C
        C3E2187C 0380965A CF4DB981 81C37208 5A021E70 3FEC3EFF
        9845A783 1CB515C4 C90EC470 675AC92E AB389748 F4455656


------------------------------------------------------------

Second call to Generate
```

```
************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
                                              A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    requested_number_of_bits is 1008
Generate FAILED: Reseed is required
************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                                              C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    additional_input is
                                              A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


  Hash_df()
  --------------------------
    no_of_bits_to_return = 521

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                            010000 02098F11 EA0D66AA A6AED620
        D86CC70C 39C6A661 F10C3E01 C04B2D67 A6DCC0C0 E1B9042D
        010F381F F61F7FCC 22D3C18E 5A8AE264 87623833 AD649755
        9C4BA47A 22AB2B00 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    Hash(counter||no_of_bits_to_return||input_string) is
                          9B3A66CC 3A3753CE 6176E75C 6EA2FF41
        FEB59307 B1A0D8A1 619E6893 5252752B 0D50B904 D6475151
```

```
        D3020756 6898B346 1FD25534 2F8796E4 BED89701 2F41B635


    temp =
                          9B3A66CC 3A3753CE 6176E75C 6EA2FF41
        FEB59307 B1A0D8A1 619E6893 5252752B 0D50B904 D6475151
        D3020756 6898B346 1FD25534 2F8796E4 BED89701 2F41B635


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                            020000 02098F11 EA0D66AA A6AED620
        D86CC70C 39C6A661 F10C3E01 C04B2D67 A6DCC0C0 E1B9042D
        010F381F F61F7FCC 22D3C18E 5A8AE264 87623833 AD649755
        9C4BA47A 22AB2B00 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    Hash(counter||no_of_bits_to_return||input_string) is
                          A6ED31D8 A3A99462 1EC4E4CB AE6F54D5
        0533FCC4 7228EF3B 39020F11 F0A090BE 9011002E C0174CC2
        0DC17A4B EC691BFD B1C6D86B 5D2BEC24 3A5D1E7C 4FE55AB2


    temp =
                      9B3A 66CC3A37 53CE6176 E75C6EA2 FF41FEB5
        9307B1A0 D8A1619E 68935252 752B0D50 B904D647 5151D302
        07566898 B3461FD2 55342F87 96E4BED8 97012F41 B635A6ED


s is
                        01 3674CD98 746EA79C C2EDCEB8 DD45FE83
        FD6B260F 6341B142 C33CD126 A4A4EA56 1AA17209 AC8EA2A3
        A6040EAC D131668C 3FA4AA68 5F0F2DC9 7DB12E02 5E836C6B


****************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>
```

```
  requested_number_of_bits is 1008
------------
i=0
t is
                  0136 74CD9874 6EA79CC2 EDCEB8DD 45FE83FD
      6B260F63 41B142C3 3CD126A4 A4EA561A A17209AC 8EA2A3A6
      040EACD1 31668C3F A4AA685F 0F2DC97D B12E025E 836C6B4D


s is
                  004F F1C9791A 4FA39027 3229B6AF 7502DA85
      0D16DC48 A8410530 6D79167D CABA439C 98EB0218 793A7780
      EC7DE88B 9C696570 3A4737BC 81818934 402AAEBA A7C49B37


r is
                  0025 290CB8DC 021E0057 CD78A001 77C81DAF
      3D06E48A 0B0D15BB 407D4527 25FA2A1C 8D95292A 6D8A977F
      DD9B3457 1E8E6E37 560251F5 75AEFC8B A99F5871 1AEEC222


------------
tmp is
                        0CB8DC 021E0057 CD78A001 77C81DAF
      3D06E48A 0B0D15BB 407D4527 25FA2A1C 8D95292A 6D8A977F
      DD9B3457 1E8E6E37 560251F5 75AEFC8B A99F5871 1AEEC222


------------
i=1
t is
                  004F F1C9791A 4FA39027 3229B6AF 7502DA85
      0D16DC48 A8410530 6D79167D CABA439C 98EB0218 793A7780
      EC7DE88B 9C696570 3A4737BC 81818934 402AAEBA A7C49B37


s is
                  01C2 036F2107 7A6360FC 31A1FEE3 28910608
      C96A154C 0B0DB6CF 83BB542B D40767B2 0F727CF2 94BB6437
      904C6163 56A3C07C 89E546BC F5400BDA F4B22ECA 62AA0A9A


r is
                  0036 CF8180B8 A636D434 E8800BCA A47F7540
      6CA0E2FD 888C1F66 C0601E50 C8999B90 3579ED1A 8FB2B0E7
      379EBC72 DEDA031A D02DFDEE 2714125E 2556F5FE AE6ECED4
```

```
  ------------
  tmp is
                                                  0CB8 DC021E00
        57CD78A0 0177C81D AF3D06E4 8A0B0D15 BB407D45 2725FA2A
        1C8D9529 2A6D8A97 7FDD9B34 571E8E6E 37560251 F575AEFC
        8BA99F58 711AEEC2 228180B8 A636D434 E8800BCA A47F7540
        6CA0E2FD 888C1F66 C0601E50 C8999B90 3579ED1A 8FB2B0E7
        379EBC72 DEDA031A D02DFDEE 2714125E 2556F5FE AE6ECED4


  ------------
  s is
                    0057 DBAB7BCE DC39393F 9B284879 57CB8685
        E0A83F7E D76919DE 812A969F 8E188096 7F90013B 682934D2
        67FDC778 AB0C7501 861BD33D A241E632 B17AE8FF 463713CC


rnd_val is
                                                  0CB8 DC021E00
        57CD78A0 0177C81D AF3D06E4 8A0B0D15 BB407D45 2725FA2A
        1C8D9529 2A6D8A97 7FDD9B34 571E8E6E 37560251 F575AEFC
        8BA99F58 711AEEC2 228180B8 A636D434 E8800BCA A47F7540
        6CA0E2FD 888C1F66 C0601E50 C8999B90 3579ED1A 8FB2B0E7
        379EBC72 DEDA031A D02DFDEE 2714125E 2556F5FE AE6ECED4


################################################################

DualEC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
```

```
    EntropyInput2 (for Reseed2) =
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    Nonce =
                           20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString =
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    AdditionalInput = <empty>

##################################################################

******************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    nonce is
                           20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    prediction_resistance_flag = "PredictionResistance"

  Hash_df()
  ----------------------------
    no_of_bits_to_return = 521

    ------------

    i = 1
```

```
    counter||no_of_bits_to_return||input_string is
                                01 00000209 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    Hash(counter||no_of_bits_to_return||input_string) is
                          FFAE2834 4D1E7E85 C08DCD7A 4643D401
        2FDC1557 F0012317 50ED5169 571DF59C 27835ECB 69B35314
        9744C13B 022FD21F 1797B206 56766C32 943DA50D 3ED374BD


    temp =
                          FFAE2834 4D1E7E85 C08DCD7A 4643D401
        2FDC1557 F0012317 50ED5169 571DF59C 27835ECB 69B35314
        9744C13B 022FD21F 1797B206 56766C32 943DA50D 3ED374BD


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 00000209 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    Hash(counter||no_of_bits_to_return||input_string) is
                          13B24000 56345ED8 7121E329 23656AF5
        63CB0C9F 6FA3F671 1A31A9EE 306A0962 01A9509E 8EEDA764
        EA71EFC6 9FE343AB 0CFD0CEF 5B7547C0 A1D66875 2BE96C9E


    temp =
                      FFAE 28344D1E 7E85C08D CD7A4643 D4012FDC
        1557F001 231750ED 5169571D F59C2783 5ECB69B3 53149744
        C13B022F D21F1797 B2065676 6C32943D A50D3ED3 74BD13B2


s is
                        01 FF5C5068 9A3CFD0B 811B9AF4 8C87A802
        5FB82AAF E002462E A1DAA2D2 AE3BEB38 4F06BD96 D366A629
```

```
        2E898276 045FA43E 2F2F640C ACECD865 287B4A1A 7DA6E97A


------------------------------------------------------------

First call to Generate

************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
Generate FAILED: Reseed is required
************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                                            80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    additional_input is  <empty>

  Hash_df()
  --------------------------
    no_of_bits_to_return = 521

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                              010000 0209FFAE
        28344D1E 7E85C08D CD7A4643 D4012FDC 1557F001 231750ED
        5169571D F59C2783 5ECB69B3 53149744 C13B022F D21F1797
        B2065676 6C32943D A50D3ED3 74BD1380 80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    Hash(counter||no_of_bits_to_return||input_string) is
                          A07EDE04 6D52F125 7BDD31EF 41A32A49
        D2D3CF41 D02C865E 20640917 0DC9F36A E2E3BFFF 58A8788A
        471D90C6 7C48BD28 8DF9296A E544BC8F 1CD6ED9F 87003A2B
```

```
    temp =
                          A07EDE04 6D52F125 7BDD31EF 41A32A49
        D2D3CF41 D02C865E 20640917 0DC9F36A E2E3BFFF 58A8788A
        471D90C6 7C48BD28 8DF9296A E544BC8F 1CD6ED9F 87003A2B


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                 020000 0209FFAE
        28344D1E 7E85C08D CD7A4643 D4012FDC 1557F001 231750ED
        5169571D F59C2783 5ECB69B3 53149744 C13B022F D21F1797
        B2065676 6C32943D A50D3ED3 74BD1380 80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    Hash(counter||no_of_bits_to_return||input_string) is
                          88AFEFF9 553A9792 50A85B63 6278976C
        EFD5FC41 7FCCD2C3 AEA6450B 3C69BAF1 DE0A92C5 FE79D405
        831E047A A14674EF 66760CC7 561CEBF3 5BB15AF6 69254A76


    temp =
                       A07E DE046D52 F1257BDD 31EF41A3 2A49D2D3
        CF41D02C 865E2064 09170DC9 F36AE2E3 BFFF58A8 788A471D
        90C67C48 BD288DF9 296AE544 BC8F1CD6 ED9F8700 3A2B88AF


s is
                         01 40FDBC08 DAA5E24A F7BA63DE 83465493
        A5A79E83 A0590CBC 40C8122E 1B93E6D5 C5C77FFE B150F114
        8E3B218C F8917A51 1BF252D5 CA89791E 39ADDB3F 0E007457


****************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
  ------------
```

```
i=0
t is
                  0140 FDBC08DA A5E24AF7 BA63DE83 465493A5
      A79E83A0 590CBC40 C8122E1B 93E6D5C5 C77FFEB1 50F1148E
      3B218CF8 917A511B F252D5CA 89791E39 ADDB3F0E 00745711


s is
                  00D8 F65E802E 31FDC676 86170D85 F56F2103
      687D9306 4F80CCD7 DB6317C5 E587D493 2F2910F2 AC40965D
      7B33F1DF 08AFFE47 B2306033 5506E429 8B6A8631 A484BB6B


r is
                  0012 0E4B447A E985BCC4 861F3A8A BACB4F80
      F0B04D38 4207959B 2743FF28 DFBD3712 6C29C526 5358AD7B
      0B127286 CE944EDB FAA116A9 DC2D0274 A975BF25 7C340311


------------
tmp is
                        4B447A E985BCC4 861F3A8A BACB4F80
      F0B04D38 4207959B 2743FF28 DFBD3712 6C29C526 5358AD7B
      0B127286 CE944EDB FAA116A9 DC2D0274 A975BF25 7C340311


------------
i=1
t is
                  00D8 F65E802E 31FDC676 86170D85 F56F2103
      687D9306 4F80CCD7 DB6317C5 E587D493 2F2910F2 AC40965D
      7B33F1DF 08AFFE47 B2306033 5506E429 8B6A8631 A484BB6B


s is
                  00AB 4412E019 B6C40EA4 CA845A6B D9D09C94
      D4A4FA91 7EFDBC4E 3E27BC78 A85881F9 7763DCD0 56CAC5E7
      5207F8EF 329AF0C1 8B9DB00B 4D0A22EF EAE79794 2065C2AB


r is
                  0171 03820FA8 2B10C121 D8981D2C C6EFB51F
      329EBA69 9FFBD410 3D1DBDDB 561962D3 43EA46C3 6D1FF67B
      A6AFEE12 F0EE580A 6050D746 44ACF69D D9A390B6 8BC2543B
```

```
  ------------
  tmp is
                                                    4B44 7AE985BC
        C4861F3A 8ABACB4F 80F0B04D 38420795 9B2743FF 28DFBD37
        126C29C5 265358AD 7B0B1272 86CE944E DBFAA116 A9DC2D02
        74A975BF 257C3403 11820FA8 2B10C121 D8981D2C C6EFB51F
        329EBA69 9FFBD410 3D1DBDDB 561962D3 43EA46C3 6D1FF67B
        A6AFEE12 F0EE580A 6050D746 44ACF69D D9A390B6 8BC2543B


  ------------
  s is
                     0119 402C8A29 037AFEE3 3FB82018 90FAE7AE
        C1D2E13D 885248E9 B747A434 A0496733 5E7D0CAE D7FC08B3
        89B58456 C8756ED8 8E151427 640438A0 8F06A0DD 6BF5F187


---------------------------------------------------------------

Second call to Generate

***************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
Generate FAILED: Reseed is required
***************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    additional_input is  <empty>

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 521

    ------------
```

```
i = 1

counter||no_of_bits_to_return||input_string is
                                                010000 02098CA0
    16451481 BD7F719F DC100C48 7D73D760 E9709EC4 292474DB
    A3D21A50 24B399AF 3E86576B FE0459C4 DAC22B64 3AB76C47
    0A8A13B2 021C5047 83506EB5 FAF8C380 C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


Hash(counter||no_of_bits_to_return||input_string) is
                        B6577447 85583872 B8633A71 26638396
    F7350FC6 CC052AA8 06E4A3C3 483DBDDA D0D29DF3 29141612
    35372020 0498EAF3 D6C7C134 6A09B2D6 BE60B293 E15309EC


temp =
                        B6577447 85583872 B8633A71 26638396
    F7350FC6 CC052AA8 06E4A3C3 483DBDDA D0D29DF3 29141612
    35372020 0498EAF3 D6C7C134 6A09B2D6 BE60B293 E15309EC


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                020000 02098CA0
    16451481 BD7F719F DC100C48 7D73D760 E9709EC4 292474DB
    A3D21A50 24B399AF 3E86576B FE0459C4 DAC22B64 3AB76C47
    0A8A13B2 021C5047 83506EB5 FAF8C380 C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


Hash(counter||no_of_bits_to_return||input_string) is
                        44C6D1E4 6E0A7743 509B225C 91D076B9
    326F147D 74EEA7EE 264B8BB0 D12574FC C12CEE44 3FD86689
    DA878137 C4210E53 D779E53A FCFD1FFF 8BC7B62C 4C43B770


temp =
                   B657 74478558 3872B863 3A712663 8396F735
    0FC6CC05 2AA806E4 A3C3483D BDDAD0D2 9DF32914 16123537
    20200498 EAF3D6C7 C1346A09 B2D6BE60 B293E153 09EC44C6
```

```
s is
                    01 6CAEE88F 0AB070E5 70C674E2 4CC7072D
       EE6A1F8D 980A5550 0DC94786 907B7BB5 A1A53BE6 52282C24
       6A6E4040 0931D5E7 AD8F8268 D41365AD 7CC16527 C2A613D8


**************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
  ------------
  i=0
  t is
                   016C AEE88F0A B070E570 C674E24C C7072DEE
       6A1F8D98 0A55500D C9478690 7B7BB5A1 A53BE652 282C246A
       6E404009 31D5E7AD 8F8268D4 1365AD7C C16527C2 A613D889


  s is
                   019D 73484D48 3CE45ADA 93CBA87E 0B6FBCB0
       30E324E6 02181283 0F4ECE02 932B2C73 459BA189 2AD98D84
       31BE1970 86A37ABB E86F19A8 ABA2BCB0 6C489969 08D68491


  r is
                   007A 84D594BB AB5DFB63 471DC655 2B009B88
       6AD1DB71 19516668 F1E88675 F5E42501 E0BAC65C 03EC2042
       5388895F B7D0B994 7213DB93 4E5F859A 6C785DE0 C78F872F


  ------------
  tmp is
                         D594BB AB5DFB63 471DC655 2B009B88
       6AD1DB71 19516668 F1E88675 F5E42501 E0BAC65C 03EC2042
       5388895F B7D0B994 7213DB93 4E5F859A 6C785DE0 C78F872F


  ------------
  i=1
  t is
                   019D 73484D48 3CE45ADA 93CBA87E 0B6FBCB0
       30E324E6 02181283 0F4ECE02 932B2C73 459BA189 2AD98D84
       31BE1970 86A37ABB E86F19A8 ABA2BCB0 6C489969 08D68491
```

```
  s is
                    0199 67CF5600 3F48081D A94DBF1B DA67B985
        4CC9D3A2 57A912E4 61695F89 C0ED6F7C E2991072 0A6E6E8E
        273BE496 0D5FE2D5 C40BE028 1E0CC219 A8C41C10 4F5D7643


  r is
                    0121 ABF43EAE EC7F9044 19D2264E C9DD1130
        FB62F847 10460B4C BF8C4964 1B56D428 D1085F42 91FDE162
        01F18E10 4DAE3A6D 9A4AC46B B908E56E 22EDB4B8 843B6038


  ------------
  tmp is
                                                D594 BBAB5DFB
        63471DC6 552B009B 886AD1DB 71195166 68F1E886 75F5E425
        01E0BAC6 5C03EC20 42538889 5FB7D0B9 947213DB 934E5F85
        9A6C785D E0C78F87 2FF43EAE EC7F9044 19D2264E C9DD1130
        FB62F847 10460B4C BF8C4964 1B56D428 D1085F42 91FDE162
        01F18E10 4DAE3A6D 9A4AC46B B908E56E 22EDB4B8 843B6038


  ------------
  s is
                    0122 77038985 6741F22A 744C4050 7B5F7010
        F2CAD7D8 CA1FFEE9 B3155675 A0711010 435992D2 067F766F
        FBB5F25E 4E216B95 A120CCD8 F60CD374 0949B974 B12BB35A


rnd_val is
                                                D594 BBAB5DFB
        63471DC6 552B009B 886AD1DB 71195166 68F1E886 75F5E425
        01E0BAC6 5C03EC20 42538889 5FB7D0B9 947213DB 934E5F85
        9A6C785D E0C78F87 2FF43EAE EC7F9044 19D2264E C9DD1130
        FB62F847 10460B4C BF8C4964 1B56D428 D1085F42 91FDE162
        01F18E10 4DAE3A6D 9A4AC46B B908E56E 22EDB4B8 843B6038


################################################################

DualEC_DRBG

    Requested Security Strength = 256
```

```
    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                            00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                            80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                            C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString =
                                            40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    AdditionalInput1  =
                                            60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    AdditionalInput2  =
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


###############################################################

***************************************************************

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                                            00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
```

```
  nonce is
                        20212223 24252627 28292A2B 2C2D2E2F


  personal_str is
                                                40414243 44454647
      48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


  prediction_resistance_flag = "PredictionResistance"

Hash_df()
----------------------------
  no_of_bits_to_return = 521

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                                01 00000209 00010203 04050607
      08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
      20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
      48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


  Hash(counter||no_of_bits_to_return||input_string) is
                        FFAE2834 4D1E7E85 C08DCD7A 4643D401
      2FDC1557 F0012317 50ED5169 571DF59C 27835ECB 69B35314
      9744C13B 022FD21F 1797B206 56766C32 943DA50D 3ED374BD


  temp =
                        FFAE2834 4D1E7E85 C08DCD7A 4643D401
      2FDC1557 F0012317 50ED5169 571DF59C 27835ECB 69B35314
      9744C13B 022FD21F 1797B206 56766C32 943DA50D 3ED374BD


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                                02 00000209 00010203 04050607
```

```
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    Hash(counter||no_of_bits_to_return||input_string) is
                          13B24000 56345ED8 7121E329 23656AF5
        63CB0C9F 6FA3F671 1A31A9EE 306A0962 01A9509E 8EEDA764
        EA71EFC6 9FE343AB 0CFD0CEF 5B7547C0 A1D66875 2BE96C9E


    temp =
                     FFAE 28344D1E 7E85C08D CD7A4643 D4012FDC
        1557F001 231750ED 5169571D F59C2783 5ECB69B3 53149744
        C13B022F D21F1797 B2065676 6C32943D A50D3ED3 74BD13B2


s is
                       01 FF5C5068 9A3CFD0B 811B9AF4 8C87A802
        5FB82AAF E002462E A1DAA2D2 AE3BEB38 4F06BD96 D366A629
        2E898276 045FA43E 2F2F640C ACECD865 287B4A1A 7DA6E97A


---------------------------------------------------------------

First call to Generate

***************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
                                            60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    requested_number_of_bits is 1008
Generate FAILED: Reseed is required
***************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                                            80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
```

```
  additional_input is
                                              60616263 64656667
      68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


Hash_df()
----------------------------
  no_of_bits_to_return = 521

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                          010000 0209FFAE 28344D1E 7E85C08D
      CD7A4643 D4012FDC 1557F001 231750ED 5169571D F59C2783
      5ECB69B3 53149744 C13B022F D21F1797 B2065676 6C32943D
      A50D3ED3 74BD1380 80818283 84858687 88898A8B 8C8D8E8F
      90919293 94959697 98999A9B 9C9D9E9F 60616263 64656667
      68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


  Hash(counter||no_of_bits_to_return||input_string) is
                         46015029 C46238FF 075EAF04 77141082
      B71E8CE1 1EF7D77B E990C0E2 70475F5B 945CB46A F8E5FB44
      60C7ADB6 A0468132 DBB830D5 80823A12 5EA250B3 65149682


  temp =
                         46015029 C46238FF 075EAF04 77141082
      B71E8CE1 1EF7D77B E990C0E2 70475F5B 945CB46A F8E5FB44
      60C7ADB6 A0468132 DBB830D5 80823A12 5EA250B3 65149682


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                          020000 0209FFAE 28344D1E 7E85C08D
      CD7A4643 D4012FDC 1557F001 231750ED 5169571D F59C2783
      5ECB69B3 53149744 C13B022F D21F1797 B2065676 6C32943D
      A50D3ED3 74BD1380 80818283 84858687 88898A8B 8C8D8E8F
      90919293 94959697 98999A9B 9C9D9E9F 60616263 64656667
      68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                          481B45CC 7118C054 581CE5C8 327BC255
        576BE388 FEFA4E7A FD60C16B F9DD0759 4D5A834A 782528E2
        5678F76A 8952798C 7507C78D 1DC43E75 DB0D9240 E50688B9


    temp =
                      4601 5029C462 38FF075E AF047714 1082B71E
        8CE11EF7 D77BE990 C0E27047 5F5B945C B46AF8E5 FB4460C7
        ADB6A046 8132DBB8 30D58082 3A125EA2 50B36514 9682481B


s is
                        00 8C02A053 88C471FE 0EBD5E08 EE282105
        6E3D19C2 3DEFAEF7 D32181C4 E08EBEB7 28B968D5 F1CBF688
        C18F5B6D 408D0265 B77061AB 01047424 BD44A166 CA292D04


****************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
  ------------
  i=0
  t is
                      008C 02A05388 C471FE0E BD5E08EE 2821056E
        3D19C23D EFAEF7D3 2181C4E0 8EBEB728 B968D5F1 CBF688C1
        8F5B6D40 8D0265B7 7061AB01 047424BD 44A166CA 292D0490


  s is
                      009F AC93AA48 4BC03AA2 72F00C74 FFAB2FD8
        32466448 88005AAB 4881F8D8 721163FD D97DAC86 B9D3F61D
        6C0D7AE9 7C114C5C 72482217 8634F2A9 55F1BAD5 3FACAA4C


  r is
                      0127 16C7ED88 A2C6901C 04802BA2 BB042629
        21B19664 835A4A3C 002CB9F1 3E35E3DE B3698A43 6BF1C85B
        070E9E69 77CA78A5 130905AA 0C01A941 30F5133D F904A4AC
```

```
  ------------
  tmp is
                            C7ED88 A2C6901C 04802BA2 BB042629
        21B19664 835A4A3C 002CB9F1 3E35E3DE B3698A43 6BF1C85B
        070E9E69 77CA78A5 130905AA 0C01A941 30F5133D F904A4AC


  ------------
  i=1
  t is
                     009F AC93AA48 4BC03AA2 72F00C74 FFAB2FD8
        32466448 88005AAB 4881F8D8 721163FD D97DAC86 B9D3F61D
        6C0D7AE9 7C114C5C 72482217 8634F2A9 55F1BAD5 3FACAA4C


  s is
                     0195 41808856 E77C1E0E 5921347B 658CBF72
        2286FF22 542119F6 484E8365 35F5A448 11FFEB2F CCDCF87A
        A0E6F8A9 32E404AA 28793F91 123B4B72 6B7FD74B 7170819A


  r is
                     00FB E2F59A7D D01227E8 FCA1C8D5 1F093839
        46ECD950 11310476 0D7E216C AF581FE9 D3AACE6F C4CDDC4C
        CD736D26 A60BE8BE 2A6A78CD 752D1EC7 CCC80263 8B177307


  ------------
  tmp is
                                                 C7ED 88A2C690
        1C04802B A2BB0426 2921B196 64835A4A 3C002CB9 F13E35E3
        DEB3698A 436BF1C8 5B070E9E 6977CA78 A5130905 AA0C01A9
        4130F513 3DF904A4 ACF59A7D D01227E8 FCA1C8D5 1F093839
        46ECD950 11310476 0D7E216C AF581FE9 D3AACE6F C4CDDC4C
        CD736D26 A60BE8BE 2A6A78CD 752D1EC7 CCC80263 8B177307


  ------------
  s is
                     0001 E2928DB7 FEB26C5A 4078C4B9 D12014E4
        D15FC2AA ECCCBE4F 1CF0D35B 7AF6DD60 B960D18D 547C0C0F
        310B832D F33961B7 1553D019 8D83DC74 1165FCA5 759478C7


------------------------------------------------------------
```

```
Second call to Generate

************************************************************

DualEC_DRBG_Generate_algorithm

    additional_input is
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    requested_number_of_bits is 1008
Generate FAILED: Reseed is required
************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                                            C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    additional_input is
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


  Hash_df()
  ---------------------------
    no_of_bits_to_return = 521

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                             010000 020900F1 4946DBFF 59362D20
        3C625CE8 900A7268 AFE15576 665F278E 7869ADBD 7B6EB05C
        B068C6AA 3E060798 85C196F9 9CB0DB8A A9E80CC6 C1EE3A08
        B2FE52BA CA3C6380 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
                        F8A5ADF3 B0C52B4A 48ECAF75 E4610EFD
        7AF72B36 8C2567D1 941DB67F A608ED5C BB3363F8 4BA8E080
        EE86BEA5 EEADC93D 8B130FB6 D35A7A48 1F6FDAB0 7C1090C2


    temp =
                        F8A5ADF3 B0C52B4A 48ECAF75 E4610EFD
        7AF72B36 8C2567D1 941DB67F A608ED5C BB3363F8 4BA8E080
        EE86BEA5 EEADC93D 8B130FB6 D35A7A48 1F6FDAB0 7C1090C2


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                             020000 020900F1 4946DBFF 59362D20
        3C625CE8 900A7268 AFE15576 665F278E 7869ADBD 7B6EB05C
        B068C6AA 3E060798 85C196F9 9CB0DB8A A9E80CC6 C1EE3A08
        B2FE52BA CA3C6380 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    Hash(counter||no_of_bits_to_return||input_string) is
                        474C0D33 75C318A8 FED8EF73 696B9E5E
        3AA7244A 5F7B92C9 504DDED4 29F0B2E0 F93DD3B7 6D79E142
        F7BDE638 635A1B5A CF6EDACB 74A60ACA 6DF0BB20 316CC953


    temp =
                     F8A5 ADF3B0C5 2B4A48EC AF75E461 0EFD7AF7
        2B368C25 67D1941D B67FA608 ED5CBB33 63F84BA8 E080EE86
        BEA5EEAD C93D8B13 0FB6D35A 7A481F6F DAB07C10 90C2474C


s is
                       01 F14B5BE7 618A5694 91D95EEB C8C21DFA
        F5EE566D 184ACFA3 283B6CFF 4C11DAB9 7666C7F0 9751C101
        DD0D7D4B DD5B927B 16261F6D A6B4F490 3EDFB560 F8212184


**************************************************************

DualEC_DRBG_Generate_algorithm
```

```
  additional_input is  <empty>

  requested_number_of_bits is 1008
------------
i=0
t is
                  01F1 4B5BE761 8A569491 D95EEBC8 C21DFAF5
      EE566D18 4ACFA328 3B6CFF4C 11DAB976 66C7F097 51C101DD
      0D7D4BDD 5B927B16 261F6DA6 B4F4903E DFB560F8 2121848E


s is
                  0050 F49247E7 838E0870 E127C9DA 71FC315C
      72AE5B72 EDA017C4 385853A5 6F576F1D 21711BFA 4E14A261
      4A0C6381 5FD4C255 1024FACD DDD48FFA A95FD223 5583E7FE


r is
                  0105 CF83B78B 20678544 12EEB24A EA86064D
      510C68FD 96DBF94E AC1BC202 2752D755 8AEB9F97 B9CBC1B9
      648FE4D8 8E2C82A6 F530675E 1DB92D39 6D6D85BD AD2A23CB


------------
tmp is
                        83B78B 20678544 12EEB24A EA86064D
      510C68FD 96DBF94E AC1BC202 2752D755 8AEB9F97 B9CBC1B9
      648FE4D8 8E2C82A6 F530675E 1DB92D39 6D6D85BD AD2A23CB


------------
i=1
t is
                  0050 F49247E7 838E0870 E127C9DA 71FC315C
      72AE5B72 EDA017C4 385853A5 6F576F1D 21711BFA 4E14A261
      4A0C6381 5FD4C255 1024FACD DDD48FFA A95FD223 5583E7FE


s is
                  0144 5F925D29 26DA7FEF C2321DE0 4291E6A2
      1D1CE2E0 996C30C4 22B3B7B6 E9A082F4 29D7C99D 7705C43A
      350FF0D9 94D00279 DF9AD924 BBF89BEA 6815CC57 9456C3D3


r is
                  0144 7DD10AD8 08ECCCFB FC811EB6 8AE835E4
```

```
        912E011D D10A4399 C8DE2D9D 88F81B61 68B05D28 2B9DAC1E
        65E0A45F 61043E1F A047870D D582295E 6C50DD11 85B13594


  ------------
  tmp is
                                                  83B7 8B206785
        4412EEB2 4AEA8606 4D510C68 FD96DBF9 4EAC1BC2 022752D7
        558AEB9F 97B9CBC1 B9648FE4 D88E2C82 A6F53067 5E1DB92D
        396D6D85 BDAD2A23 CBD10AD8 08ECCCFB FC811EB6 8AE835E4
        912E011D D10A4399 C8DE2D9D 88F81B61 68B05D28 2B9DAC1E
        65E0A45F 61043E1F A047870D D582295E 6C50DD11 85B13594


  ------------
  s is
                    016D 61DC3D5D 4D16A71F CAFAC01A 0386F31B
        15C55FF0 761A21D9 406B317B BB567F9C E892DEB7 02FD5895
        882B71DF 19D757F4 76BCC728 373F63F0 1FB5B85D ABDD1E27


rnd_val is
                                                  83B7 8B206785
        4412EEB2 4AEA8606 4D510C68 FD96DBF9 4EAC1BC2 022752D7
        558AEB9F 97B9CBC1 B9648FE4 D88E2C82 A6F53067 5E1DB92D
        396D6D85 BDAD2A23 CBD10AD8 08ECCCFB FC811EB6 8AE835E4
        912E011D D10A4399 C8DE2D9D 88F81B61 68B05D28 2B9DAC1E
        65E0A45F 61043E1F A047870D D582295E 6C50DD11 85B13594
```