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

  Block Cipher Modes of Operation

     FF3 Method for Format-Preserving Encryption

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

Sample #1

FF3-AES128

Key is EF 43 59 D8 D5 80 AA 4F 7F 03 6D 6F 04 FC 6A 94
Radix = 10
------------------------------------------------------------------


PT is <890121234567890000>

FF3.Encrypt()

X is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0
Tweak is D8 E7 92 0A FA 33 0A 73

Step 1
        u is <9>, and v is <9>
Step 2
        A is    8 9 0 1 2 1 2 3 4
        B is    5 6 7 8 9 0 0 0 0
Step 3
        T_L is      D8E7920A
        T_R is      FA330A73

Round #0
        Step 4.i
                m is <9>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 115, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 129, 205 ]
        Step 4.iii
                S is        DE7F3E4A 210E3DFF 346924FB FF750039
        Step 4.iv
                y is  295749300147794922410226583415804985401
        Step 4.v
                c is  237106499
        Step 4.vi
                C is    9 9 4 6 0 1 7 3 2
        Step 4.vii
                A is    5 6 7 8 9 0 0 0 0
```

```
        Step 4.viii
                B is    9 9 4 6 0 1 7 3 2

Round #1
        Step 4.i
                m is <9>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 11, 0, 0, 0, 0, 0, 0, 0, 0,
14, 33, 245, 67 ]
        Step 4.iii
                S is        F36C5439 2D06A707 CBD5F74E AAF6FBD2
        Step 4.iv
                y is  323564879288803156328785244944160193490
        Step 4.v
                c is  160292255
        Step 4.vi
                C is    5 5 2 2 9 2 0 6 1
        Step 4.vii
                A is    9 9 4 6 0 1 7 3 2
        Step 4.viii
                B is    5 5 2 2 9 2 0 6 1

Round #2
        Step 4.i
                m is <9>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 113, 0, 0, 0, 0, 0, 0, 0, 0, 9,
141, 221, 159 ]
        Step 4.iii
                S is        2C97C094 4C1C063F 490DBDF6 963F18C8
        Step 4.iv
                y is  592739746121417507824982584225934276 56
        Step 4.v
                c is  830534155
        Step 4.vi
                C is    5 5 1 4 3 5 0 3 8
        Step 4.vii
                A is    5 5 2 2 9 2 0 6 1
        Step 4.viii
                B is    5 5 1 4 3 5 0 3 8

Round #3
        Step 4.i
                m is <9>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 9, 0, 0, 0, 0, 0, 0, 0, 0, 49,
128, 242, 11 ]
```

```
        Step 4.iii
                S is        AC61CE4A FCB73F97 CBCCA980 C85CEB2E
        Step 4.iv
                y is  229135052187757542928291096799108459310
        Step 4.v
                c is  268751565
        Step 4.vi
                C is    5 6 5 1 5 7 8 6 2
        Step 4.vii
                A is    5 5 1 4 3 5 0 3 8
        Step 4.viii
                B is    5 6 5 1 5 7 8 6 2

Round #4
        Step 4.i
                m is <9>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 119, 0, 0, 0, 0, 0, 0, 0, 0, 16,
4, 210, 205 ]
        Step 4.iii
                S is        33BC0C3B 6D0386D8 E486726E BED5F40B
        Step 4.iv
                y is  68767027691550218919956754510046950411
        Step 4.v
                c is  877484566
        Step 4.vi
                C is    6 6 5 4 8 4 7 7 8
        Step 4.vii
                A is    5 6 5 1 5 7 8 6 2
        Step 4.viii
                B is    6 6 5 4 8 4 7 7 8

Round #5
        Step 4.i
                m is <9>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 15, 0, 0, 0, 0, 0, 0, 0, 0,
52, 77, 90, 22 ]
        Step 4.iii
                S is        EA297167 D4B452EB F582DEAC 3382AA38
        Step 4.iv
                y is  311254535323485014116628468200718379576
        Step 4.v
                c is  987131141
        Step 4.vi
                C is    1 4 1 1 3 1 7 8 9
        Step 4.vii
                A is    6 6 5 4 8 4 7 7 8
```

```
        Step 4.viii
                B is    1 4 1 1 3 1 7 8 9

Round #6
        Step 4.i
                m is <9>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 117, 0, 0, 0, 0, 0, 0, 0, 0, 58,
214, 109, 5 ]
        Step 4.iii
                S is        1AA22CC7 0FC44D52 E710D167 736ED9DB
        Step 4.iv
                y is  354019881787969455428896351875413344 91
        Step 4.v
                c is  418819057
        Step 4.vi
                C is    7 5 0 9 1 8 8 1 4
        Step 4.vii
                A is    1 4 1 1 3 1 7 8 9
        Step 4.viii
                B is    7 5 0 9 1 8 8 1 4

Round #7
        Step 4.i
                m is <9>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 13, 0, 0, 0, 0, 0, 0, 0, 0,
24, 246, 171, 241 ]
        Step 4.iii
                S is        EDF38D53 6E192148 43FEA1C1 88FBAA0D
        Step 4.iv
                y is  316291629567414359958402343312719325709
        Step 4.v
                c is  706456850
        Step 4.vi
                C is    0 5 8 6 5 4 6 0 7
        Step 4.vii
                A is    7 5 0 9 1 8 8 1 4
        Step 4.viii
                B is    0 5 8 6 5 4 6 0 7
Step 5
        A || B is    7 5 0 9 1 8 8 1 4 0 5 8 6 5 4 6 0 7

CT is 750918814058654607
------------------------------------------------------------

FF3.Decrypt()
```

```
X is    7 5 0 9 1 8 8 1 4 0 5 8 6 5 4 6 0 7
Tweak is D8 E7 92 0A FA 33 0A 73

Step 1
        u is <9>, and v is <9>
Step 2
        A is    7 5 0 9 1 8 8 1 4
        B is    0 5 8 6 5 4 6 0 7
Step 3
        T_L is      D8E7920A
        T_R is      FA330A73

Round #7
        Step 4.i
                m is <9>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 13, 0, 0, 0, 0, 0, 0, 0, 0,
24, 246, 171, 241 ]
        Step 4.iii
                S is        EDF38D53 6E192148 43FEA1C1 88FBAA0D
        Step 4.iv
                y is  316291629567414359958402343312719325709
        Step 4.v
                c is  987131141
        Step 4.vi
                C is    1 4 1 1 3 1 7 8 9
        Step 4.vii
                B is    7 5 0 9 1 8 8 1 4
        Step 4.viii
                A is    1 4 1 1 3 1 7 8 9

Round #6
        Step 4.i
                m is <9>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 117, 0, 0, 0, 0, 0, 0, 0, 0, 58,
214, 109, 5 ]
        Step 4.iii
                S is        1AA22CC7 0FC44D52 E710D167 736ED9DB
        Step 4.iv
                y is  354019881787969455428896351875413344 91
        Step 4.v
                c is  877484566
        Step 4.vi
                C is    6 6 5 4 8 4 7 7 8
        Step 4.vii
                B is    1 4 1 1 3 1 7 8 9
        Step 4.viii
```

```
                A is    6 6 5 4 8 4 7 7 8

Round #5
        Step 4.i
                m is <9>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 15, 0, 0, 0, 0, 0, 0, 0, 0,
52, 77, 90, 22 ]
        Step 4.iii
                S is        EA297167 D4B452EB F582DEAC 3382AA38
        Step 4.iv
                y is  311254535323485014116628468200718379576
        Step 4.v
                c is  268751565
        Step 4.vi
                C is    5 6 5 1 5 7 8 6 2
        Step 4.vii
                B is    6 6 5 4 8 4 7 7 8
        Step 4.viii
                A is    5 6 5 1 5 7 8 6 2

Round #4
        Step 4.i
                m is <9>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 119, 0, 0, 0, 0, 0, 0, 0, 0, 16,
4, 210, 205 ]
        Step 4.iii
                S is        33BC0C3B 6D0386D8 E486726E BED5F40B
        Step 4.iv
                y is  68767027691550218919956754510046950411
        Step 4.v
                c is  830534155
        Step 4.vi
                C is    5 5 1 4 3 5 0 3 8
        Step 4.vii
                B is    5 6 5 1 5 7 8 6 2
        Step 4.viii
                A is    5 5 1 4 3 5 0 3 8

Round #3
        Step 4.i
                m is <9>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 9, 0, 0, 0, 0, 0, 0, 0, 0, 49,
128, 242, 11 ]
        Step 4.iii
```

```
                S is         AC61CE4A FCB73F97 CBCCA980 C85CEB2E
        Step 4.iv
                y is  229135052187757542928291096799108459310
        Step 4.v
                c is  160292255
        Step 4.vi
                C is    5 5 2 2 9 2 0 6 1
        Step 4.vii
                B is    5 5 1 4 3 5 0 3 8
        Step 4.viii
                A is    5 5 2 2 9 2 0 6 1

Round #2
        Step 4.i
                m is <9>
                W is         FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 113, 0, 0, 0, 0, 0, 0, 0, 0, 9,
141, 221, 159 ]
        Step 4.iii
                S is         2C97C094 4C1C063F 490DBDF6 963F18C8
        Step 4.iv
                y is  592739746121417507824982584225934276 56
        Step 4.v
                c is  237106499
        Step 4.vi
                C is    9 9 4 6 0 1 7 3 2
        Step 4.vii
                B is    5 5 2 2 9 2 0 6 1
        Step 4.viii
                A is    9 9 4 6 0 1 7 3 2

Round #1
        Step 4.i
                m is <9>
                W is         D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 11, 0, 0, 0, 0, 0, 0, 0, 0,
14, 33, 245, 67 ]
        Step 4.iii
                S is         F36C5439 2D06A707 CBD5F74E AAF6FBD2
        Step 4.iv
                y is  323564879288803156328785244944160193490
        Step 4.v
                c is  98765
        Step 4.vi
                C is    5 6 7 8 9 0 0 0 0
        Step 4.vii
                B is    9 9 4 6 0 1 7 3 2
        Step 4.viii
```

```
                A is    5 6 7 8 9 0 0 0 0

Round #0
        Step 4.i
                m is <9>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 115, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 129, 205 ]
        Step 4.iii
                S is        DE7F3E4A 210E3DFF 346924FB FF750039
        Step 4.iv
                y is  295749300147794922410226583415804985401
        Step 4.v
                c is  432121098
        Step 4.vi
                C is    8 9 0 1 2 1 2 3 4
        Step 4.vii
                B is    5 6 7 8 9 0 0 0 0
        Step 4.viii
                A is    8 9 0 1 2 1 2 3 4
Step 5
        A || B is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0

PTout is <890121234567890000>
================================================================

Sample #2

FF3-AES128

Key is EF 43 59 D8 D5 80 AA 4F 7F 03 6D 6F 04 FC 6A 94
Radix = 10
----------------------------------------------------------------


PT is <890121234567890000>

FF3.Encrypt()

X is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0
Tweak is 9A 76 8A 92 F6 0E 12 D8

Step 1
        u is <9>, and v is <9>
Step 2
        A is    8 9 0 1 2 1 2 3 4
        B is    5 6 7 8 9 0 0 0 0
Step 3
        T_L is      9A768A92
```

```
        T_R is      F60E12D8

Round #0
        Step 4.i
                m is <9>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 216, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 129, 205 ]
        Step 4.iii
                S is        FDB2567A E7E40CE8 8A0487AF 96948AB8
        Step 4.iv
                y is  337220665799231389260037749402473106104
        Step 4.v
                c is  905227202
        Step 4.vi
                C is    2 0 2 7 2 2 5 0 9
        Step 4.vii
                A is    5 6 7 8 9 0 0 0 0
        Step 4.viii
                B is    2 0 2 7 2 2 5 0 9

Round #1
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 147, 0, 0, 0, 0, 0, 0, 0, 0,
53, 244, 171, 194 ]
        Step 4.iii
                S is        0D356803 4135675E 46445392 26336D11
        Step 4.iv
                y is  175572653071706063782106584676263150 25
        Step 4.v
                c is  626413790
        Step 4.vi
                C is    0 9 7 3 1 4 6 2 6
        Step 4.vii
                A is    2 0 2 7 2 2 5 0 9
        Step 4.viii
                B is    0 9 7 3 1 4 6 2 6

Round #2
        Step 4.i
                m is <9>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 218, 0, 0, 0, 0, 0, 0, 0, 0, 37,
86, 80, 222 ]
        Step 4.iii
```

```
                S is        6760F993 53421724 0A34C3C4 08101140
        Step 4.iv
                y is  13741400605656403142273777074396725689 6
        Step 4.v
                c is  872484098
        Step 4.vi
                C is    8 9 0 4 8 4 2 7 8
        Step 4.vii
                A is    0 9 7 3 1 4 6 2 6
        Step 4.viii
                B is    8 9 0 4 8 4 2 7 8

Round #3
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 145, 0, 0, 0, 0, 0, 0, 0, 0,
52, 1, 13, 2 ]
        Step 4.iii
                S is        9EBB2AA5 B9C353D7 C58129D3 C689FC7A
        Step 4.iv
                y is  21098984783790375219758367377543620108 2
        Step 4.v
                c is  62614872
        Step 4.vi
                C is    2 7 8 4 1 6 2 6 0
        Step 4.vii
                A is    8 9 0 4 8 4 2 7 8
        Step 4.viii
                B is    2 7 8 4 1 6 2 6 0

Round #4
        Step 4.i
                m is <9>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 220, 0, 0, 0, 0, 0, 0, 0, 0, 3,
187, 109, 88 ]
        Step 4.iii
                S is        696B4A33 5A6B9591 D5153A0B 2BCFF676
        Step 4.iv
                y is  14012602028821006393160299590018871871 0
        Step 4.v
                c is  61202808
        Step 4.vi
                C is    8 0 8 2 0 2 1 6 0
        Step 4.vii
                A is    2 7 8 4 1 6 2 6 0
        Step 4.viii
```

```
                B is    8 0 8 2 0 2 1 6 0

Round #5
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 151, 0, 0, 0, 0, 0, 0, 0, 0,
3, 165, 225, 120 ]
        Step 4.iii
                S is        A2898EEC 17B9B88A FDB7AFEC DE422FF6
        Step 4.iv
                y is  216049178794128392680994742157411758070
        Step 4.v
                c is  474372942
        Step 4.vi
                C is    2 4 9 2 7 3 4 7 4
        Step 4.vii
                A is    8 0 8 2 0 2 1 6 0
        Step 4.viii
                B is    2 4 9 2 7 3 4 7 4

Round #6
        Step 4.i
                m is <9>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 222, 0, 0, 0, 0, 0, 0, 0, 0, 28,
70, 91, 78 ]
        Step 4.iii
                S is        4FA53B92 77E3C101 4EA9DA02 E70BD97A
        Step 4.iv
                y is  105866948915248996819895414429877787002
        Step 4.v
                c is  938989810
        Step 4.vi
                C is    0 1 8 9 8 9 8 3 9
        Step 4.vii
                A is    2 4 9 2 7 3 4 7 4
        Step 4.viii
                B is    0 1 8 9 8 9 8 3 9

Round #7
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 149, 0, 0, 0, 0, 0, 0, 0, 0,
55, 247, 216, 242 ]
        Step 4.iii
```

```
                S is         38D2CA1C 5A2082FD 14803B53 D1F121AF
        Step 4.iv
                y is  75531249397269045807726683499009221039
        Step 4.v
                c is  483593981
        Step 4.vi
                C is    1 8 9 3 9 5 3 8 4
        Step 4.vii
                A is    0 1 8 9 8 9 8 3 9
        Step 4.viii
                B is    1 8 9 3 9 5 3 8 4
Step 5
        A || B is    0 1 8 9 8 9 8 3 9 1 8 9 3 9 5 3 8 4

CT is 018989839189395384
----------------------------------------------------------------

FF3.Decrypt()

X is    0 1 8 9 8 9 8 3 9 1 8 9 3 9 5 3 8 4
Tweak is 9A 76 8A 92 F6 0E 12 D8

Step 1
        u is <9>, and v is <9>
Step 2
        A is    0 1 8 9 8 9 8 3 9
        B is    1 8 9 3 9 5 3 8 4
Step 3
        T_L is      9A768A92
        T_R is      F60E12D8

Round #7
        Step 4.i
                m is <9>
                W is         9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 149, 0, 0, 0, 0, 0, 0, 0, 0,
55, 247, 216, 242 ]
        Step 4.iii
                S is         38D2CA1C 5A2082FD 14803B53 D1F121AF
        Step 4.iv
                y is  75531249397269045807726683499009221039
        Step 4.v
                c is  474372942
        Step 4.vi
                C is    2 4 9 2 7 3 4 7 4
        Step 4.vii
                B is    0 1 8 9 8 9 8 3 9
        Step 4.viii
                A is    2 4 9 2 7 3 4 7 4
```

```
Round #6
        Step 4.i
                m is <9>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 222, 0, 0, 0, 0, 0, 0, 0, 0, 28,
70, 91, 78 ]
        Step 4.iii
                S is        4FA53B92 77E3C101 4EA9DA02 E70BD97A
        Step 4.iv
                y is  105866948915248996819895414429877787002
        Step 4.v
                c is  61202808
        Step 4.vi
                C is   8 0 8 2 0 2 1 6 0
        Step 4.vii
                B is   2 4 9 2 7 3 4 7 4
        Step 4.viii
                A is   8 0 8 2 0 2 1 6 0

Round #5
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 151, 0, 0, 0, 0, 0, 0, 0, 0,
3, 165, 225, 120 ]
        Step 4.iii
                S is        A2898EEC 17B9B88A FDB7AFEC DE422FF6
        Step 4.iv
                y is  216049178794128392680994742157411758070
        Step 4.v
                c is  62614872
        Step 4.vi
                C is   2 7 8 4 1 6 2 6 0
        Step 4.vii
                B is   8 0 8 2 0 2 1 6 0
        Step 4.viii
                A is   2 7 8 4 1 6 2 6 0

Round #4
        Step 4.i
                m is <9>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 220, 0, 0, 0, 0, 0, 0, 0, 0, 3,
187, 109, 88 ]
        Step 4.iii
                S is        696B4A33 5A6B9591 D5153A0B 2BCFF676
```

```
        Step 4.iv
                y is  1401260202882100639316029959001887187l0
        Step 4.v
                c is  872484098
        Step 4.vi
                C is    8 9 0 4 8 4 2 7 8
        Step 4.vii
                B is    2 7 8 4 1 6 2 6 0
        Step 4.viii
                A is    8 9 0 4 8 4 2 7 8

Round #3
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 145, 0, 0, 0, 0, 0, 0, 0, 0,
52, 1, 13, 2 ]
        Step 4.iii
                S is        9EBB2AA5 B9C353D7 C58129D3 C689FC7A
        Step 4.iv
                y is  21098984783790375219758367377543620l082
        Step 4.v
                c is  626413790
        Step 4.vi
                C is    0 9 7 3 1 4 6 2 6
        Step 4.vii
                B is    8 9 0 4 8 4 2 7 8
        Step 4.viii
                A is    0 9 7 3 1 4 6 2 6

Round #2
        Step 4.i
                m is <9>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 218, 0, 0, 0, 0, 0, 0, 0, 0, 37,
86, 80, 222 ]
        Step 4.iii
                S is        6760F993 53421724 0A34C3C4 08101140
        Step 4.iv
                y is  13741400605656403142273777074396725689l
        Step 4.v
                c is  905227202
        Step 4.vi
                C is    2 0 2 7 2 2 5 0 9
        Step 4.vii
                B is    0 9 7 3 1 4 6 2 6
        Step 4.viii
                A is    2 0 2 7 2 2 5 0 9
```

```
Round #1
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 147, 0, 0, 0, 0, 0, 0, 0, 0,
53, 244, 171, 194 ]
        Step 4.iii
                S is        0D356803 4135675E 46445392 26336D11
        Step 4.iv
                y is  175572653071706063782106584676263l5025
        Step 4.v
                c is  98765
        Step 4.vi
                C is    5 6 7 8 9 0 0 0 0
        Step 4.vii
                B is    2 0 2 7 2 2 5 0 9
        Step 4.viii
                A is    5 6 7 8 9 0 0 0 0

Round #0
        Step 4.i
                m is <9>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 216, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 129, 205 ]
        Step 4.iii
                S is        FDB2567A E7E40CE8 8A0487AF 96948AB8
        Step 4.iv
                y is  337220665799231389260037749402473106104
        Step 4.v
                c is  432121098
        Step 4.vi
                C is    8 9 0 1 2 1 2 3 4
        Step 4.vii
                B is    5 6 7 8 9 0 0 0 0
        Step 4.viii
                A is    8 9 0 1 2 1 2 3 4
Step 5
        A || B is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0

PTout is <890121234567890000>
============================================================

Sample #3

FF3-AES128
```

```
Key is EF 43 59 D8 D5 80 AA 4F 7F 03 6D 6F 04 FC 6A 94
Radix = 10
------------------------------------------------------------


PT is <8901212345678900000789000000>

FF3.Encrypt()

X is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0 0 0 7 8 9 0 0 0 0 0 0
Tweak is D8 E7 92 0A FA 33 0A 73

Step 1
        u is <15>, and v is <14>
Step 2
        A is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0
        B is    0 0 0 0 0 7 8 9 0 0 0 0 0 0
Step 3
        T_L is      D8E7920A
        T_R is      FA330A73

Round #0
        Step 4.i
                m is <15>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 115, 0, 0, 0, 0, 0, 0, 0, 0, 5,
226, 10, 224 ]
        Step 4.iii
                S is        634FEEAF 800BF73C D4A390F8 E6E5711A
        Step 4.iv
                y is  132008604152573578881746879192339149082
        Step 4.v
                c is  977957771270180
        Step 4.vi
                C is    0 8 1 0 7 2 1 7 7 7 5 9 7 7 9
        Step 4.vii
                A is    0 0 0 0 0 7 8 9 0 0 0 0 0 0 0
        Step 4.viii
                B is    0 8 1 0 7 2 1 7 7 7 5 9 7 7 9

Round #1
        Step 4.i
                m is <14>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 11, 0, 0, 0, 0, 0, 3, 121,
114, 137, 143, 216, 36 ]
        Step 4.iii
                S is        D33E2B0E DB505A21 06CBB217 7B8D0B69
```

```
        Step 4.iv
                y is  280789902836527997555860570416599599977
        Step 4.v
                c is  70416698299977
        Step 4.vi
                C is    7 7 9 9 9 2 8 9 6 6 1 4 0 7
        Step 4.vii
                A is    0 8 1 0 7 2 1 7 7 7 5 9 7 7 9
        Step 4.viii
                B is    7 7 9 9 9 2 8 9 6 6 1 4 0 7

Round #2
        Step 4.i
                m is <15>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 113, 0, 0, 0, 0, 0, 0, 64, 11,
42, 73, 214, 73 ]
        Step 4.iii
                S is        5340C6B3 C0C35F8E 8F397D8E 94EA5CAC
        Step 4.iv
                y is  110662260807694173178399363608171142316
        Step 4.v
                c is  341565942412496
        Step 4.vi
                C is    6 9 4 2 1 4 2 4 9 5 6 5 1 4 3
        Step 4.vii
                A is    7 7 9 9 9 2 8 9 6 6 1 4 0 7
        Step 4.viii
                B is    6 9 4 2 1 4 2 4 9 5 6 5 1 4 3

Round #3
        Step 4.i
                m is <14>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 9, 0, 0, 0, 0, 0, 1, 54, 167,
4, 170, 52, 208 ]
        Step 4.iii
                S is        B592D097 D9958238 1D78A272 AF422160
        Step 4.iv
                y is  241352573350404949051856214707889381728
        Step 4.v
                c is  85124587681705
        Step 4.vi
                C is    5 0 7 1 8 6 7 8 5 4 2 1 5 8
        Step 4.vii
                A is    6 9 4 2 1 4 2 4 9 5 6 5 1 4 3
        Step 4.viii
                B is    5 0 7 1 8 6 7 8 5 4 2 1 5 8
```

```
Round #4
        Step 4.i
                m is <15>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 119, 0, 0, 0, 0, 0, 0, 77, 107,
156, 207, 119, 169 ]
        Step 4.iii
                S is        76FA5867 E94E0BC6 F4847242 B9774DBA
        Step 4.iv
                y is  158148770802003999344415250210700611002
        Step 4.v
                c is  591776643023498
        Step 4.vi
                C is    8 9 4 3 2 0 3 4 6 6 7 7 1 9 5
        Step 4.vii
                A is    5 0 7 1 8 6 7 8 5 4 2 1 5 8
        Step 4.viii
                B is    8 9 4 3 2 0 3 4 6 6 7 7 1 9 5

Round #5
        Step 4.i
                m is <14>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 15, 0, 0, 0, 0, 0, 2, 26, 55,
188, 152, 2, 138 ]
        Step 4.iii
                S is        78A37F18 1F2ED4D4 E8C6D110 24BCA627
        Step 4.iv
                y is  160356281659277296717736667474441315879
        Step 4.v
                c is  52599028997584
        Step 4.vi
                C is    4 8 5 7 9 9 8 2 0 9 9 5 2 5
        Step 4.vii
                A is    8 9 4 3 2 0 3 4 6 6 7 7 1 9 5
        Step 4.viii
                B is    4 8 5 7 9 9 8 2 0 9 9 5 2 5

Round #6
        Step 4.i
                m is <15>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 117, 0, 0, 0, 0, 0, 0, 47, 214,
170, 112, 93, 208 ]
        Step 4.iii
                S is        9096C6CD 62491A65 5C249C15 9D0A9F46
```

```
        Step 4.iv
                y is  192191708111100855495973933449533366086
        Step 4.v
                c is  525226176389584
        Step 4.vi
                C is    4 8 5 9 8 3 6 7 1 6 2 2 5 2 5
        Step 4.vii
                A is    4 8 5 7 9 9 8 2 0 9 9 5 2 5
        Step 4.viii
                B is    4 8 5 9 8 3 6 7 1 6 2 2 5 2 5

Round #7
        Step 4.i
                m is <14>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 13, 0, 0, 0, 0, 0, 1, 221,
176, 191, 171, 161, 208 ]
        Step 4.iii
                S is        53AA0A4B 1C5C3B43 F92C5EF9 39EA27E8
        Step 4.iv
                y is  111208822891084244558307109662450395112
        Step 4.v
                c is  62261479392696
        Step 4.vi
                C is    6 9 6 2 9 3 9 7 4 1 6 2 2 6
        Step 4.vii
                A is    4 8 5 9 8 3 6 7 1 6 2 2 5 2 5
        Step 4.viii
                B is    6 9 6 2 9 3 9 7 4 1 6 2 2 6
Step 5
        A || B is    4 8 5 9 8 3 6 7 1 6 2 2 5 2 5 6 9 6 2 9 3 9 7 4 1
6 2 2 6

CT is 485983671622525696293974162 26
----------------------------------------------------------------

FF3.Decrypt()

X is    4 8 5 9 8 3 6 7 1 6 2 2 5 2 5 6 9 6 2 9 3 9 7 4 1 6 2 2 6
Tweak is D8 E7 92 0A FA 33 0A 73

Step 1
        u is <15>, and v is <14>
Step 2
        A is    4 8 5 9 8 3 6 7 1 6 2 2 5 2 5
        B is    6 9 6 2 9 3 9 7 4 1 6 2 2 6
Step 3
        T_L is      D8E7920A
        T_R is      FA330A73
```

```
Round #7
        Step 4.i
                m is <14>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 13, 0, 0, 0, 0, 0, 1, 221,
176, 191, 171, 161, 208 ]
        Step 4.iii
                S is        53AA0A4B 1C5C3B43 F92C5EF9 39EA27E8
        Step 4.iv
                y is  111208822891084244558307109662450395112
        Step 4.v
                c is  52599028997584
        Step 4.vi
                C is    4 8 5 7 9 9 8 2 0 9 9 5 2 5
        Step 4.vii
                B is    4 8 5 9 8 3 6 7 1 6 2 2 5 2 5
        Step 4.viii
                A is    4 8 5 7 9 9 8 2 0 9 9 5 2 5

Round #6
        Step 4.i
                m is <15>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 117, 0, 0, 0, 0, 0, 0, 47, 214,
170, 112, 93, 208 ]
        Step 4.iii
                S is        9096C6CD 62491A65 5C249C15 9D0A9F46
        Step 4.iv
                y is  192191708111100855495973933449533366086
        Step 4.v
                c is  591776643023498
        Step 4.vi
                C is    8 9 4 3 2 0 3 4 6 6 7 7 1 9 5
        Step 4.vii
                B is    4 8 5 7 9 9 8 2 0 9 9 5 2 5
        Step 4.viii
                A is    8 9 4 3 2 0 3 4 6 6 7 7 1 9 5

Round #5
        Step 4.i
                m is <14>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 15, 0, 0, 0, 0, 0, 2, 26, 55,
188, 152, 2, 138 ]
        Step 4.iii
                S is        78A37F18 1F2ED4D4 E8C6D110 24BCA627
```

```
        Step 4.iv
                y is  160356281659277296717736667474441315879
        Step 4.v
                c is  85124587681705
        Step 4.vi
                C is    5 0 7 1 8 6 7 8 5 4 2 1 5 8
        Step 4.vii
                B is    8 9 4 3 2 0 3 4 6 6 7 7 1 9 5
        Step 4.viii
                A is    5 0 7 1 8 6 7 8 5 4 2 1 5 8

Round #4
        Step 4.i
                m is <15>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 119, 0, 0, 0, 0, 0, 0, 77, 107,
156, 207, 119, 169 ]
        Step 4.iii
                S is        76FA5867 E94E0BC6 F4847242 B9774DBA
        Step 4.iv
                y is  158148770802003999344415250210700611002
        Step 4.v
                c is  341565942412496
        Step 4.vi
                C is    6 9 4 2 1 4 2 4 9 5 6 5 1 4 3
        Step 4.vii
                B is    5 0 7 1 8 6 7 8 5 4 2 1 5 8
        Step 4.viii
                A is    6 9 4 2 1 4 2 4 9 5 6 5 1 4 3

Round #3
        Step 4.i
                m is <14>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 9, 0, 0, 0, 0, 0, 1, 54, 167,
4, 170, 52, 208 ]
        Step 4.iii
                S is        B592D097 D9958238 1D78A272 AF422160
        Step 4.iv
                y is  241352573350404949051856214707889381728
        Step 4.v
                c is  70416698299977
        Step 4.vi
                C is    7 7 9 9 9 2 8 9 6 6 1 4 0 7
        Step 4.vii
                B is    6 9 4 2 1 4 2 4 9 5 6 5 1 4 3
        Step 4.viii
                A is    7 7 9 9 9 2 8 9 6 6 1 4 0 7
```

```
Round #2
        Step 4.i
                m is <15>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 113, 0, 0, 0, 0, 0, 0, 64, 11,
42, 73, 214, 73 ]
        Step 4.iii
                S is        5340C6B3 C0C35F8E 8F397D8E 94EA5CAC
        Step 4.iv
                y is  1106622608076941731783993636081711423l6
        Step 4.v
                c is  977957771270180
        Step 4.vi
                C is    0 8 1 0 7 2 1 7 7 7 5 9 7 7 9
        Step 4.vii
                B is    7 7 9 9 9 2 8 9 6 6 1 4 0 7
        Step 4.viii
                A is    0 8 1 0 7 2 1 7 7 7 5 9 7 7 9

Round #1
        Step 4.i
                m is <14>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 11, 0, 0, 0, 0, 0, 3, 121,
114, 137, 143, 216, 36 ]
        Step 4.iii
                S is        D33E2B0E DB505A21 06CBB217 7B8D0B69
        Step 4.iv
                y is  280789902836527997555860570416599599977
        Step 4.v
                c is  98700000
        Step 4.vi
                C is    0 0 0 0 0 7 8 9 0 0 0 0 0 0
        Step 4.vii
                B is    0 8 1 0 7 2 1 7 7 7 5 9 7 7 9
        Step 4.viii
                A is    0 0 0 0 0 7 8 9 0 0 0 0 0 0

Round #0
        Step 4.i
                m is <15>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 115, 0, 0, 0, 0, 0, 0, 0, 0, 5,
226, 10, 224 ]
        Step 4.iii
                S is        634FEEAF 800BF73C D4A390F8 E6E5711A
```

```
        Step 4.iv
                y is  132008604152573578881746879192339149082
        Step 4.v
                c is  98765432121098
        Step 4.vi
                C is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0
        Step 4.vii
                B is    0 0 0 0 0 7 8 9 0 0 0 0 0 0 0
        Step 4.viii
                A is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0
Step 5
        A || B is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0 0 0 7 8 9 0 0
0 0 0 0

PTout is <8901212345678900000789000000>
================================================================

Sample #4

FF3-AES128

Key is EF 43 59 D8 D5 80 AA 4F 7F 03 6D 6F 04 FC 6A 94
Radix = 10
----------------------------------------------------------------


PT is <8901212345678900000789000000>

FF3.Encrypt()

X is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0 0 0 7 8 9 0 0 0 0 0 0
Tweak is 00 00 00 00 00 00 00 00

Step 1
        u is <15>, and v is <14>
Step 2
        A is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0
        B is    0 0 0 0 0 7 8 9 0 0 0 0 0 0 0
Step 3
        T_L is      00000000
        T_R is      00000000

Round #0
        Step 4.i
                m is <15>
                W is        00000000
        Step 4.ii
                P is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 226,
10, 224 ]
        Step 4.iii
```

```
                S is         879BB739 333ED8AF C3D7EC2C B4A78019
        Step 4.iv
                y is  1802543016568589848683482311383417815 29
        Step 4.v
                c is  329903773902627
        Step 4.vi
                C is    7 2 6 2 0 9 3 7 7 3 0 9 9 2 3
        Step 4.vii
                A is    0 0 0 0 0 7 8 9 0 0 0 0 0 0 0
        Step 4.viii
                B is    7 2 6 2 0 9 3 7 7 3 0 9 9 2 3

Round #1
        Step 4.i
                m is <14>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 44, 11, 181,
64, 231, 35 ]
        Step 4.iii
                S is         14415453 954EDB05 E3E2BF10 19C77F89
        Step 4.iv
                y is  269237695560558736624109777039502539 61
        Step 4.v
                c is  77704048953961
        Step 4.vi
                C is    1 6 9 3 5 9 8 4 0 4 0 7 7 7
        Step 4.vii
                A is    7 2 6 2 0 9 3 7 7 3 0 9 9 2 3
        Step 4.viii
                B is    1 6 9 3 5 9 8 4 0 4 0 7 7 7

Round #2
        Step 4.i
                m is <15>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 70, 171, 226,
60, 74, 105 ]
        Step 4.iii
                S is         A92219C4 C77DCB40 0C81317B BBA38A9F
        Step 4.iv
                y is  224816592031540503251472393464877124255
        Step 4.v
                c is  723368651026882
        Step 4.vi
                C is    2 8 8 6 2 0 1 5 6 8 6 3 3 2 7
        Step 4.vii
                A is    1 6 9 3 5 9 8 4 0 4 0 7 7 7
        Step 4.viii
```

```
                B is    2 8 8 6 2 0 1 5 6 8 6 3 3 2 7

Round #3
        Step 4.i
                m is <14>
                W is        00000000
        Step 4.ii
                P is  [ 0, 0, 0, 3, 0, 0, 0, 0, 0, 2, 145, 230, 99,
124, 113, 194 ]
        Step 4.iii
                S is        51D806D5 3774A6C6 269564E0 4B055B6A
        Step 4.iv
                y is  108789142367240644424618408177379400554
        Step 4.v
                c is  85881428354515
        Step 4.vi
                C is    5 1 5 4 5 3 8 2 4 1 8 8 5 8
        Step 4.vii
                A is    2 8 8 6 2 0 1 5 6 8 6 3 3 2 7
        Step 4.viii
                B is    5 1 5 4 5 3 8 2 4 1 8 8 5 8

Round #4
        Step 4.i
                m is <15>
                W is        00000000
        Step 4.ii
                P is  [ 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 78, 27, 212, 7,
165, 211 ]
        Step 4.iii
                S is        B927EC0C 70E45B85 B7EBF794 17BAC72C
        Step 4.iv
                y is  246114466432035095118991742816520685356
        Step 4.v
                c is  466185171712238
        Step 4.vi
                C is    8 3 2 2 1 7 1 7 1 5 8 1 6 6 4
        Step 4.vii
                A is    5 1 5 4 5 3 8 2 4 1 8 8 5 8
        Step 4.viii
                B is    8 3 2 2 1 7 1 7 1 5 8 1 6 6 4

Round #5
        Step 4.i
                m is <14>
                W is        00000000
        Step 4.ii
                P is  [ 0, 0, 0, 5, 0, 0, 0, 0, 0, 1, 167, 254, 49,
143, 56, 238 ]
        Step 4.iii
```

```
                S is         C1C4F817 CB99449A 2BDDC15D 20F30795
        Step 4.iv
                y is  257563725293601779736986048305682384789
        Step 4.v
                c is  34187110739304
        Step 4.vi
                C is    4 0 3 9 3 7 0 1 1 7 8 1 4 3
        Step 4.vii
                A is    8 3 2 2 1 7 1 7 1 5 8 1 6 6 4
        Step 4.viii
                B is    4 0 3 9 3 7 0 1 1 7 8 1 4 3

Round #6
        Step 4.i
                m is <15>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 6, 0, 0, 0, 0, 0, 0, 31, 23, 206,
151, 109, 104 ]
        Step 4.iii
                S is         DAAA1292 B326B8AE 8F8F61AA 0D8063CD
        Step 4.iv
                y is  290654770253191801877218077527670547405
        Step 4.v
                c is  543712842259643
        Step 4.vi
                C is    3 4 6 9 5 2 2 4 8 2 1 7 3 4 5
        Step 4.vii
                A is    4 0 3 9 3 7 0 1 1 7 8 1 4 3
        Step 4.viii
                B is    3 4 6 9 5 2 2 4 8 2 1 7 3 4 5

Round #7
        Step 4.i
                m is <14>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 7, 0, 0, 0, 0, 0, 1, 238, 129, 2,
210, 156, 187 ]
        Step 4.iii
                S is         4EA538DF F3D522F2 73849D6C 9B6731A1
        Step 4.iv
                y is  104537666211162253438756709223620882849
        Step 4.v
                c is  43410731622153
        Step 4.vi
                C is    3 5 1 2 2 6 1 3 7 0 1 4 3 4
        Step 4.vii
                A is    3 4 6 9 5 2 2 4 8 2 1 7 3 4 5
        Step 4.viii
```

```
                B is    3 5 1 2 2 6 1 3 7 0 1 4 3 4
Step 5
        A || B is    3 4 6 9 5 2 2 4 8 2 1 7 3 4 5 3 5 1 2 2 6 1 3 7 0
1 4 3 4

CT is 346952248217345351226137014 34
------------------------------------------------------------

FF3.Decrypt()

X is    3 4 6 9 5 2 2 4 8 2 1 7 3 4 5 3 5 1 2 2 6 1 3 7 0 1 4 3 4
Tweak is 00 00 00 00 00 00 00 00

Step 1
        u is <15>, and v is <14>
Step 2
        A is    3 4 6 9 5 2 2 4 8 2 1 7 3 4 5
        B is    3 5 1 2 2 6 1 3 7 0 1 4 3 4
Step 3
        T_L is      00000000
        T_R is      00000000

Round #7
        Step 4.i
                m is <14>
                W is        00000000
        Step 4.ii
                P is  [ 0, 0, 0, 7, 0, 0, 0, 0, 0, 1, 238, 129, 2,
210, 156, 187 ]
        Step 4.iii
                S is        4EA538DF F3D522F2 73849D6C 9B6731A1
        Step 4.iv
                y is  104537666211162253438756709223620882849
        Step 4.v
                c is  34187110739304
        Step 4.vi
                C is    4 0 3 9 3 7 0 1 1 7 8 1 4 3
        Step 4.vii
                B is    3 4 6 9 5 2 2 4 8 2 1 7 3 4 5
        Step 4.viii
                A is    4 0 3 9 3 7 0 1 1 7 8 1 4 3

Round #6
        Step 4.i
                m is <15>
                W is        00000000
        Step 4.ii
                P is  [ 0, 0, 0, 6, 0, 0, 0, 0, 0, 0, 31, 23, 206,
151, 109, 104 ]
        Step 4.iii
```

```
                S is        DAAA1292 B326B8AE 8F8F61AA 0D8063CD
        Step 4.iv
                y is  290654770253191801877218077527670547405
        Step 4.v
                c is  466185171712238
        Step 4.vi
                C is    8 3 2 2 1 7 1 7 1 5 8 1 6 6 4
        Step 4.vii
                B is    4 0 3 9 3 7 0 1 1 7 8 1 4 3
        Step 4.viii
                A is    8 3 2 2 1 7 1 7 1 5 8 1 6 6 4

Round #5
        Step 4.i
                m is <14>
                W is        00000000
        Step 4.ii
                P is  [ 0, 0, 0, 5, 0, 0, 0, 0, 0, 1, 167, 254, 49,
143, 56, 238 ]
        Step 4.iii
                S is        C1C4F817 CB99449A 2BDDC15D 20F30795
        Step 4.iv
                y is  257563725293601779736986048305682384789
        Step 4.v
                c is  85881428354515
        Step 4.vi
                C is    5 1 5 4 5 3 8 2 4 1 8 8 5 8
        Step 4.vii
                B is    8 3 2 2 1 7 1 7 1 5 8 1 6 6 4
        Step 4.viii
                A is    5 1 5 4 5 3 8 2 4 1 8 8 5 8

Round #4
        Step 4.i
                m is <15>
                W is        00000000
        Step 4.ii
                P is  [ 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 78, 27, 212, 7,
165, 211 ]
        Step 4.iii
                S is        B927EC0C 70E45B85 B7EBF794 17BAC72C
        Step 4.iv
                y is  246114466432035095118991742816520685356
        Step 4.v
                c is  723368651026882
        Step 4.vi
                C is    2 8 8 6 2 0 1 5 6 8 6 3 3 2 7
        Step 4.vii
                B is    5 1 5 4 5 3 8 2 4 1 8 8 5 8
        Step 4.viii
```

```
                A is    2 8 8 6 2 0 1 5 6 8 6 3 3 2 7

Round #3
        Step 4.i
                m is <14>
                W is        00000000
        Step 4.ii
                P is  [ 0, 0, 0, 3, 0, 0, 0, 0, 0, 2, 145, 230, 99,
124, 113, 194 ]
        Step 4.iii
                S is        51D806D5 3774A6C6 269564E0 4B055B6A
        Step 4.iv
                y is  108789142367240644424618408177379400554
        Step 4.v
                c is  77704048953961
        Step 4.vi
                C is    1 6 9 3 5 9 8 4 0 4 0 7 7 7
        Step 4.vii
                B is    2 8 8 6 2 0 1 5 6 8 6 3 3 2 7
        Step 4.viii
                A is    1 6 9 3 5 9 8 4 0 4 0 7 7 7

Round #2
        Step 4.i
                m is <15>
                W is        00000000
        Step 4.ii
                P is  [ 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 70, 171, 226,
60, 74, 105 ]
        Step 4.iii
                S is        A92219C4 C77DCB40 0C81317B BBA38A9F
        Step 4.iv
                y is  22481659203154050325147239346487712425 5
        Step 4.v
                c is  329903773902627
        Step 4.vi
                C is    7 2 6 2 0 9 3 7 7 3 0 9 9 2 3
        Step 4.vii
                B is    1 6 9 3 5 9 8 4 0 4 0 7 7 7
        Step 4.viii
                A is    7 2 6 2 0 9 3 7 7 3 0 9 9 2 3

Round #1
        Step 4.i
                m is <14>
                W is        00000000
        Step 4.ii
                P is  [ 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 44, 11, 181,
64, 231, 35 ]
        Step 4.iii
```

```
                S is         14415453 954EDB05 E3E2BF10 19C77F89
        Step 4.iv
                y is  269237695560558736624109777039502539 61
        Step 4.v
                c is  98700000
        Step 4.vi
                C is    0 0 0 0 0 7 8 9 0 0 0 0 0 0
        Step 4.vii
                B is    7 2 6 2 0 9 3 7 7 3 0 9 9 2 3
        Step 4.viii
                A is    0 0 0 0 0 7 8 9 0 0 0 0 0 0

Round #0
        Step 4.i
                m is <15>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 226,
10, 224 ]
        Step 4.iii
                S is         879BB739 333ED8AF C3D7EC2C B4A78019
        Step 4.iv
                y is  180254301656858984868348231138341781529
        Step 4.v
                c is  98765432121098
        Step 4.vi
                C is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0
        Step 4.vii
                B is    0 0 0 0 0 7 8 9 0 0 0 0 0 0 0
        Step 4.viii
                A is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0
Step 5
        A || B is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0 0 0 7 8 9 0 0
0 0 0 0

PTout is <8901212345678900000789000000>
================================================================

Sample #5

FF3-AES128

Key is EF 43 59 D8 D5 80 AA 4F 7F 03 6D 6F 04 FC 6A 94
Radix = 26
----------------------------------------------------------------


PT is <0123456789abcdefghi>

FF3.Encrypt()
```

```
X is    0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
Tweak is 9A 76 8A 92 F6 0E 12 D8

Step 1
        u is <10>, and v is <9>
Step 2
        A is    0 1 2 3 4 5 6 7 8 9
        B is    10 11 12 13 14 15 16 17 18
Step 3
        T_L is      9A768A92
        T_R is      F60E12D8

Round #0
        Step 4.i
                m is <10>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 216, 0, 0, 0, 0, 0, 0, 3, 140,
43, 56, 187, 32 ]
        Step 4.iii
                S is        2092463E A3019625 0D0BAF3E 5BB19E6A
        Step 4.iv
                y is  432947959377296988331467451352996655l4
        Step 4.v
                c is  53466973912356
        Step 4.vi
                C is    4 2 13 1 21 11 23 0 22 9
        Step 4.vii
                A is    10 11 12 13 14 15 16 17 18
        Step 4.viii
                B is    4 2 13 1 21 11 23 0 22 9

Round #1
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 147, 0, 0, 0, 0, 0, 0, 48,
160, 191, 252, 189, 36 ]
        Step 4.iii
                S is        53D17649 29968A7A 612D0763 ED274EA3
        Step 4.iv
                y is  111413512814441769083482546159355383459
        Step 4.v
                c is  783066858435
        Step 4.vi
                C is    17 17 12 5 2 23 12 19 3
        Step 4.vii
                A is    4 2 13 1 21 11 23 0 22 9
```

```
        Step 4.viii
                B is    17 17 12 5 2 23 12 19 3

Round #2
        Step 4.i
                m is <10>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 218, 0, 0, 0, 0, 0, 0, 0, 182,
82, 108, 3, 195 ]
        Step 4.iii
                S is        346317A6 C8FFB5F9 2AC777F2 19FBA4BA
        Step 4.iv
                y is  6963437287931257207544825988187446597 8
        Step 4.v
                c is  70478395266526
        Step 4.vi
                C is    0 13 11 20 20 15 23 12 25 12
        Step 4.vii
                A is    17 17 12 5 2 23 12 19 3
        Step 4.viii
                B is    0 13 11 20 20 15 23 12 25 12

Round #3
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 145, 0, 0, 0, 0, 0, 0, 64, 25,
135, 182, 213, 222 ]
        Step 4.iii
                S is        2222A95F 0A19C4D6 607A3FB9 0EDDB1F0
        Step 4.iv
                y is  45373725206901782587602825076639904240
        Step 4.v
                c is  4485780042675
        Step 4.vi
                C is    9 23 23 19 4 1 13 12 21
        Step 4.vii
                A is    0 13 11 20 20 15 23 12 25 12
        Step 4.viii
                B is    9 23 23 19 4 1 13 12 21

Round #4
        Step 4.i
                m is <10>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 220, 0, 0, 0, 0, 0, 0, 4, 20,
109, 83, 115, 179 ]
```

```
        Step 4.iii
                S is         F0DEC672 B02929A1 39EC6E05 9142AE4C
        Step 4.iv
                y is  320171433894605715165612249211407085132
        Step 4.v
                c is  21704262742058
        Step 4.vi
                C is    0 11 23 14 14 12 7 24 25 3
        Step 4.vii
                A is    9 23 23 19 4 1 13 12 21
        Step 4.viii
                B is    0 11 23 14 14 12 7 24 25 3

Round #5
        Step 4.i
                m is <9>
                W is         9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 151, 0, 0, 0, 0, 0, 0, 19,
189, 106, 222, 240, 42 ]
        Step 4.iii
                S is         A4199DFE C704C487 61C4A6F3 8162D31B
        Step 4.iv
                y is  218126403254043906521248087648896209691
        Step 4.v
                c is  4644812701902
        Step 4.vi
                C is    22 24 0 19 5 22 7 6 22
        Step 4.vii
                A is    0 11 23 14 14 12 7 24 25 3
        Step 4.viii
                B is    22 24 0 19 5 22 7 6 22

Round #6
        Step 4.i
                m is <10>
                W is         F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 222, 0, 0, 0, 0, 0, 0, 4, 57,
116, 105, 64, 206 ]
        Step 4.iii
                S is         33506215 D6701B6D 3DF142E9 B17A877E
        Step 4.iv
                y is  68208000940011387704247483042289583998
        Step 4.v
                c is  12816299911080
        Step 4.vi
                C is    16 2 25 20 4 0 18 9 9 2
        Step 4.vii
                A is    22 24 0 19 5 22 7 6 22
```

```
        Step 4.viii
                B is    16 2 25 20 4 0 18 9 9 2

Round #7
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 149, 0, 0, 0, 0, 0, 0, 11,
168, 7, 0, 231, 168 ]
        Step 4.iii
                S is        A3FDF98A F7DE8768 87E1FE0F 263AADFF
        Step 4.iv
                y is  217982875748340153313307554297226636799
        Step 4.v
                c is  2461054303437
        Step 4.vi
                C is    15 23 2 0 12 19 10 20 11
        Step 4.vii
                A is    16 2 25 20 4 0 18 9 9 2
        Step 4.viii
                B is    15 23 2 0 12 19 10 20 11
Step 5
        A || B is    16 2 25 20 4 0 18 9 9 2 15 23 2 0 12 19 10 20 11

CT is g2pk40i992fn20cjakb
------------------------------------------------------------

FF3.Decrypt()

X is    16 2 25 20 4 0 18 9 9 2 15 23 2 0 12 19 10 20 11
Tweak is 9A 76 8A 92 F6 0E 12 D8

Step 1
        u is <10>, and v is <9>
Step 2
        A is    16 2 25 20 4 0 18 9 9 2
        B is    15 23 2 0 12 19 10 20 11
Step 3
        T_L is      9A768A92
        T_R is      F60E12D8

Round #7
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 149, 0, 0, 0, 0, 0, 0, 11,
168, 7, 0, 231, 168 ]
        Step 4.iii
```

```
                S is         A3FDF98A F7DE8768 87E1FE0F 263AADFF
        Step 4.iv
                y is  217982875748340153313307554297226636799
        Step 4.v
                c is  4644812701902
        Step 4.vi
                C is    22 24 0 19 5 22 7 6 22
        Step 4.vii
                B is    16 2 25 20 4 0 18 9 9 2
        Step 4.viii
                A is    22 24 0 19 5 22 7 6 22

Round #6
        Step 4.i
                m is <10>
                W is         F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 222, 0, 0, 0, 0, 0, 0, 4, 57,
116, 105, 64, 206 ]
        Step 4.iii
                S is         33506215 D6701B6D 3DF142E9 B17A877E
        Step 4.iv
                y is  68208000940011387704247483042289583998
        Step 4.v
                c is  21704262742058
        Step 4.vi
                C is    0 11 23 14 14 12 7 24 25 3
        Step 4.vii
                B is    22 24 0 19 5 22 7 6 22
        Step 4.viii
                A is    0 11 23 14 14 12 7 24 25 3

Round #5
        Step 4.i
                m is <9>
                W is         9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 151, 0, 0, 0, 0, 0, 0, 19,
189, 106, 222, 240, 42 ]
        Step 4.iii
                S is         A4199DFE C704C487 61C4A6F3 8162D31B
        Step 4.iv
                y is  218126403254043906521248087648896209691
        Step 4.v
                c is  4485780042675
        Step 4.vi
                C is    9 23 23 19 4 1 13 12 21
        Step 4.vii
                B is    0 11 23 14 14 12 7 24 25 3
        Step 4.viii
```

```
                A is    9 23 23 19 4 1 13 12 21

Round #4
        Step 4.i
                m is <10>
                W is         F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 220, 0, 0, 0, 0, 0, 0, 4, 20,
109, 83, 115, 179 ]
        Step 4.iii
                S is         F0DEC672 B02929A1 39EC6E05 9142AE4C
        Step 4.iv
                y is  320171433894605715165612249211407085132
        Step 4.v
                c is  70478395266526
        Step 4.vi
                C is    0 13 11 20 20 15 23 12 25 12
        Step 4.vii
                B is    9 23 23 19 4 1 13 12 21
        Step 4.viii
                A is    0 13 11 20 20 15 23 12 25 12

Round #3
        Step 4.i
                m is <9>
                W is         9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 145, 0, 0, 0, 0, 0, 0, 64, 25,
135, 182, 213, 222 ]
        Step 4.iii
                S is         2222A95F 0A19C4D6 607A3FB9 0EDDB1F0
        Step 4.iv
                y is  45373725206901782587602825076639904240
        Step 4.v
                c is  783066858435
        Step 4.vi
                C is    17 17 12 5 2 23 12 19 3
        Step 4.vii
                B is    0 13 11 20 20 15 23 12 25 12
        Step 4.viii
                A is    17 17 12 5 2 23 12 19 3

Round #2
        Step 4.i
                m is <10>
                W is         F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 218, 0, 0, 0, 0, 0, 0, 0, 182,
82, 108, 3, 195 ]
        Step 4.iii
```

```
                S is        346317A6 C8FFB5F9 2AC777F2 19FBA4BA
        Step 4.iv
                y is  6963437287931257207544825988187446597 8
        Step 4.v
                c is  53466973912356
        Step 4.vi
                C is    4 2 13 1 21 11 23 0 22 9
        Step 4.vii
                B is    17 17 12 5 2 23 12 19 3
        Step 4.viii
                A is    4 2 13 1 21 11 23 0 22 9

Round #1
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 147, 0, 0, 0, 0, 0, 0, 48,
160, 191, 252, 189, 36 ]
        Step 4.iii
                S is        53D17649 29968A7A 612D0763 ED274EA3
        Step 4.iv
                y is  111413512814441769083482546159355383459
        Step 4.v
                c is  3900555442976
        Step 4.vi
                C is    10 11 12 13 14 15 16 17 18
        Step 4.vii
                B is    4 2 13 1 21 11 23 0 22 9
        Step 4.viii
                A is    10 11 12 13 14 15 16 17 18

Round #0
        Step 4.i
                m is <10>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 216, 0, 0, 0, 0, 0, 0, 3, 140,
43, 56, 187, 32 ]
        Step 4.iii
                S is        2092463E A3019625 0D0BAF3E 5BB19E6A
        Step 4.iv
                y is  432947959377296988331467451352996655 14
        Step 4.v
                c is  50594287082170
        Step 4.vi
                C is    0 1 2 3 4 5 6 7 8 9
        Step 4.vii
                B is    10 11 12 13 14 15 16 17 18
        Step 4.viii
```

```
                A is    0 1 2 3 4 5 6 7 8 9
Step 5
        A || B is    0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18

PTout is <0123456789abcdefghi>
==========================================================

Sample #6

FF3-AES192

Key is EF 43 59 D8 D5 80 AA 4F 7F 03 6D 6F 04 FC 6A 94 2B 7E 15 16 28
AE D2 A6
Radix = 10
----------------------------------------------------------


PT is <890121234567890000>

FF3.Encrypt()

X is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0
Tweak is D8 E7 92 0A FA 33 0A 73

Step 1
        u is <9>, and v is <9>
Step 2
        A is    8 9 0 1 2 1 2 3 4
        B is    5 6 7 8 9 0 0 0 0
Step 3
        T_L is      D8E7920A
        T_R is      FA330A73

Round #0
        Step 4.i
                m is <9>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 115, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 129, 205 ]
        Step 4.iii
                S is        94D5DC0E 76A16010 0DF75E21 5BC14A57
        Step 4.iv
                y is  197836165883056867901047745955565226583
        Step 4.v
                c is  997347681
        Step 4.vi
                C is    1 8 6 7 4 3 7 9 9
        Step 4.vii
                A is    5 6 7 8 9 0 0 0 0
```

```
        Step 4.viii
                B is    1 8 6 7 4 3 7 9 9

Round #1
        Step 4.i
                m is <9>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 11, 0, 0, 0, 0, 0, 0, 0, 0,
59, 114, 81, 97 ]
        Step 4.iii
                S is        32BF3F1E BF7C6431 A948F514 6451690E
        Step 4.iv
                y is  67454408717137868035652652075098138894
        Step 4.v
                c is  98237659
        Step 4.vi
                C is    9 5 6 7 3 2 8 9 0
        Step 4.vii
                A is    1 8 6 7 4 3 7 9 9
        Step 4.viii
                B is    9 5 6 7 3 2 8 9 0

Round #2
        Step 4.i
                m is <9>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 113, 0, 0, 0, 0, 0, 0, 0, 0, 5,
218, 252, 219 ]
        Step 4.iii
                S is        8516AD28 0E006DC5 255BFDB9 A569456E
        Step 4.iv
                y is  176905066000602818125736927003085981038
        Step 4.v
                c is  83328719
        Step 4.vi
                C is    9 1 7 8 2 3 3 8 0
        Step 4.vii
                A is    9 5 6 7 3 2 8 9 0
        Step 4.viii
                B is    9 1 7 8 2 3 3 8 0

Round #3
        Step 4.i
                m is <9>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 9, 0, 0, 0, 0, 0, 0, 0, 0, 4,
247, 126, 207 ]
```

```
        Step 4.iii
                S is        08C99645 5FCC05F9 042EF130 36452A3E
        Step 4.iv
                y is  116805234926763135769702702834917811 82
        Step 4.v
                c is  590018841
        Step 4.vi
                C is    1 4 8 8 1 0 0 9 5
        Step 4.vii
                A is    9 1 7 8 2 3 3 8 0
        Step 4.viii
                B is    1 4 8 8 1 0 0 9 5

Round #4
        Step 4.i
                m is <9>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 119, 0, 0, 0, 0, 0, 0, 0, 0, 35,
42, 249, 25 ]
        Step 4.iii
                S is        BE06B0D4 65B60CDD CFE1A7C7 CF4737A7
        Step 4.iv
                y is  252588059512223991786762096467566344103
        Step 4.v
                c is  649672822
        Step 4.vi
                C is    2 2 8 2 7 6 9 4 6
        Step 4.vii
                A is    1 4 8 8 1 0 0 9 5
        Step 4.viii
                B is    2 2 8 2 7 6 9 4 6

Round #5
        Step 4.i
                m is <9>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 15, 0, 0, 0, 0, 0, 0, 0, 0,
38, 185, 56, 118 ]
        Step 4.iii
                S is        AA631F98 4C1A756D 8090CC0B FE4479BD
        Step 4.iv
                y is  226483437493361909053404110117562251709
        Step 4.v
                c is  152270550
        Step 4.vi
                C is    0 5 5 0 7 2 2 5 1
        Step 4.vii
                A is    2 2 8 2 7 6 9 4 6
```

```
        Step 4.viii
                B is    0 5 5 0 7 2 2 5 1

Round #6
        Step 4.i
                m is <9>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 117, 0, 0, 0, 0, 0, 0, 0, 0, 9,
19, 118, 214 ]
        Step 4.iii
                S is        5D30ADBE 4DD04E47 B630BA94 5EDBC4F8
        Step 4.iv
                y is  123870957791501329349587110363743896824
        Step 4.v
                c is  393569646
        Step 4.vi
                C is    6 4 6 9 6 5 3 9 3
        Step 4.vii
                A is    0 5 5 0 7 2 2 5 1
        Step 4.viii
                B is    6 4 6 9 6 5 3 9 3

Round #7
        Step 4.i
                m is <9>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 13, 0, 0, 0, 0, 0, 0, 0, 0,
23, 117, 101, 110 ]
        Step 4.iii
                S is        D38CB6DB 52E49B35 40E4D065 7CEA91CC
        Step 4.iv
                y is  281197737445981719119985453827405550028
        Step 4.v
                c is  557820578
        Step 4.vi
                C is    8 7 5 0 2 8 7 5 5
        Step 4.vii
                A is    6 4 6 9 6 5 3 9 3
        Step 4.viii
                B is    8 7 5 0 2 8 7 5 5
Step 5
        A || B is    6 4 6 9 6 5 3 9 3 8 7 5 0 2 8 7 5 5

CT is 646965393875028755
--------------------------------------------------------------

FF3.Decrypt()
```

```
X is    6 4 6 9 6 5 3 9 3 8 7 5 0 2 8 7 5 5
Tweak is D8 E7 92 0A FA 33 0A 73

Step 1
        u is <9>, and v is <9>
Step 2
        A is    6 4 6 9 6 5 3 9 3
        B is    8 7 5 0 2 8 7 5 5
Step 3
        T_L is      D8E7920A
        T_R is      FA330A73

Round #7
        Step 4.i
                m is <9>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 13, 0, 0, 0, 0, 0, 0, 0, 0,
23, 117, 101, 110 ]
        Step 4.iii
                S is        D38CB6DB 52E49B35 40E4D065 7CEA91CC
        Step 4.iv
                y is  281197737445981719119985453827405550028
        Step 4.v
                c is  152270550
        Step 4.vi
                C is    0 5 5 0 7 2 2 5 1
        Step 4.vii
                B is    6 4 6 9 6 5 3 9 3
        Step 4.viii
                A is    0 5 5 0 7 2 2 5 1

Round #6
        Step 4.i
                m is <9>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 117, 0, 0, 0, 0, 0, 0, 0, 0, 9,
19, 118, 214 ]
        Step 4.iii
                S is        5D30ADBE 4DD04E47 B630BA94 5EDBC4F8
        Step 4.iv
                y is  123870957791501329349587110363743896824
        Step 4.v
                c is  649672822
        Step 4.vi
                C is    2 2 8 2 7 6 9 4 6
        Step 4.vii
                B is    0 5 5 0 7 2 2 5 1
        Step 4.viii
```

```
                A is    2 2 8 2 7 6 9 4 6

Round #5
        Step 4.i
                m is <9>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 15, 0, 0, 0, 0, 0, 0, 0, 0,
38, 185, 56, 118 ]
        Step 4.iii
                S is        AA631F98 4C1A756D 8090CC0B FE4479BD
        Step 4.iv
                y is  226483437493361909053404110117562251709
        Step 4.v
                c is  590018841
        Step 4.vi
                C is    1 4 8 8 1 0 0 9 5
        Step 4.vii
                B is    2 2 8 2 7 6 9 4 6
        Step 4.viii
                A is    1 4 8 8 1 0 0 9 5

Round #4
        Step 4.i
                m is <9>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 119, 0, 0, 0, 0, 0, 0, 0, 0, 35,
42, 249, 25 ]
        Step 4.iii
                S is        BE06B0D4 65B60CDD CFE1A7C7 CF4737A7
        Step 4.iv
                y is  252588059512223991786762096467566344103
        Step 4.v
                c is  83328719
        Step 4.vi
                C is    9 1 7 8 2 3 3 8 0
        Step 4.vii
                B is    1 4 8 8 1 0 0 9 5
        Step 4.viii
                A is    9 1 7 8 2 3 3 8 0

Round #3
        Step 4.i
                m is <9>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 9, 0, 0, 0, 0, 0, 0, 0, 0, 4,
247, 126, 207 ]
        Step 4.iii
```

```
                S is         08C99645 5FCC05F9 042EF130 36452A3E
        Step 4.iv
                y is  116805234926763135769702702834917811 82
        Step 4.v
                c is  98237659
        Step 4.vi
                C is    9 5 6 7 3 2 8 9 0
        Step 4.vii
                B is    9 1 7 8 2 3 3 8 0
        Step 4.viii
                A is    9 5 6 7 3 2 8 9 0

Round #2
        Step 4.i
                m is <9>
                W is         FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 113, 0, 0, 0, 0, 0, 0, 0, 0, 5,
218, 252, 219 ]
        Step 4.iii
                S is         8516AD28 0E006DC5 255BFDB9 A569456E
        Step 4.iv
                y is  176905066000602818125736927003085981038
        Step 4.v
                c is  997347681
        Step 4.vi
                C is    1 8 6 7 4 3 7 9 9
        Step 4.vii
                B is    9 5 6 7 3 2 8 9 0
        Step 4.viii
                A is    1 8 6 7 4 3 7 9 9

Round #1
        Step 4.i
                m is <9>
                W is         D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 11, 0, 0, 0, 0, 0, 0, 0, 0,
59, 114, 81, 97 ]
        Step 4.iii
                S is         32BF3F1E BF7C6431 A948F514 6451690E
        Step 4.iv
                y is  674544087171378680356526520750981388 94
        Step 4.v
                c is  98765
        Step 4.vi
                C is    5 6 7 8 9 0 0 0 0
        Step 4.vii
                B is    1 8 6 7 4 3 7 9 9
        Step 4.viii
```

```
                A is    5 6 7 8 9 0 0 0 0

Round #0
        Step 4.i
                m is <9>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 115, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 129, 205 ]
        Step 4.iii
                S is        94D5DC0E 76A16010 0DF75E21 5BC14A57
        Step 4.iv
                y is  197836165883056867901047745955565226583
        Step 4.v
                c is  432121098
        Step 4.vi
                C is    8 9 0 1 2 1 2 3 4
        Step 4.vii
                B is    5 6 7 8 9 0 0 0 0
        Step 4.viii
                A is    8 9 0 1 2 1 2 3 4
Step 5
        A || B is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0

PTout is <890121234567890000>
================================================================

Sample #7

FF3-AES192

Key is EF 43 59 D8 D5 80 AA 4F 7F 03 6D 6F 04 FC 6A 94 2B 7E 15 16 28
AE D2 A6
Radix = 10
----------------------------------------------------------------


PT is <890121234567890000>

FF3.Encrypt()

X is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0
Tweak is 9A 76 8A 92 F6 0E 12 D8

Step 1
        u is <9>, and v is <9>
Step 2
        A is    8 9 0 1 2 1 2 3 4
        B is    5 6 7 8 9 0 0 0 0
Step 3
```

```
        T_L is      9A768A92
        T_R is      F60E12D8

Round #0
        Step 4.i
                m is <9>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 216, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 129, 205 ]
        Step 4.iii
                S is        97757BFC 9FB91E2B F4E6622B 861B9759
        Step 4.iv
                y is  20132344084728098471116210697023334588l
        Step 4.v
                c is  665466979
        Step 4.vi
                C is    9 7 9 6 6 4 5 6 6
        Step 4.vii
                A is    5 6 7 8 9 0 0 0 0
        Step 4.viii
                B is    9 7 9 6 6 4 5 6 6

Round #1
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 147, 0, 0, 0, 0, 0, 0, 0, 0,
39, 170, 56, 99 ]
        Step 4.iii
                S is        5D9716D7 29C024E9 3E9A9742 A7E30331
        Step 4.iv
                y is  124402703693623329523381064393380004657
        Step 4.v
                c is  380103422
        Step 4.vi
                C is    2 2 4 3 0 1 0 8 3
        Step 4.vii
                A is    9 7 9 6 6 4 5 6 6
        Step 4.viii
                B is    2 2 4 3 0 1 0 8 3

Round #2
        Step 4.i
                m is <9>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 218, 0, 0, 0, 0, 0, 0, 0, 0, 22,
167, 234, 254 ]
```

```
        Step 4.iii
                S is        3E3648A1 14EA512D 4732B51B 57CF2364
        Step 4.iv
                y is  826939928647242647139412437159671980 52
        Step 4.v
                c is  632665031
        Step 4.vi
                C is    1 3 0 5 6 6 2 3 6
        Step 4.vii
                A is    2 2 4 3 0 1 0 8 3
        Step 4.viii
                B is    1 3 0 5 6 6 2 3 6

Round #3
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 145, 0, 0, 0, 0, 0, 0, 0, 0,
37, 181, 179, 199 ]
        Step 4.iii
                S is        835A1B57 52DC930B 6446A2F8 F721A49B
        Step 4.iv
                y is  174596728708645980056743609325326541979
        Step 4.v
                c is  706645401
        Step 4.vi
                C is    1 0 4 5 4 6 6 0 7
        Step 4.vii
                A is    1 3 0 5 6 6 2 3 6
        Step 4.viii
                B is    1 0 4 5 4 6 6 0 7

Round #4
        Step 4.i
                m is <9>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 220, 0, 0, 0, 0, 0, 0, 0, 0, 42,
30, 141, 153 ]
        Step 4.iii
                S is        21EEE299 C35B961B DF4FEF6B 2DEA7A69
        Step 4.iv
                y is  451048865201731007752484383370202630 17
        Step 4.v
                c is  652928048
        Step 4.vi
                C is    8 4 0 8 2 9 2 5 6
        Step 4.vii
                A is    1 0 4 5 4 6 6 0 7
```

```
        Step 4.viii
                B is    8 4 0 8 2 9 2 5 6

Round #5
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 151, 0, 0, 0, 0, 0, 0, 0, 0,
38, 234, 228, 48 ]
        Step 4.iii
                S is        10B970AE 19271C43 9154665E 21F9879C
        Step 4.iv
                y is  22230508274747890371985356286747838364
        Step 4.v
                c is  454483765
        Step 4.vi
                C is    5 6 7 3 8 4 4 5 4
        Step 4.vii
                A is    8 4 0 8 2 9 2 5 6
        Step 4.viii
                B is    5 6 7 3 8 4 4 5 4

Round #6
        Step 4.i
                m is <9>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 222, 0, 0, 0, 0, 0, 0, 0, 0, 27,
22, 223, 53 ]
        Step 4.iii
                S is        FA4BAD69 C2494073 3D5092B1 E1B3D6B9
        Step 4.iv
                y is  33269993844656622388225181841476208812l
        Step 4.v
                c is  415016169
        Step 4.vi
                C is    9 6 1 6 1 0 5 1 4
        Step 4.vii
                A is    5 6 7 3 8 4 4 5 4
        Step 4.viii
                B is    9 6 1 6 1 0 5 1 4

Round #7
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 149, 0, 0, 0, 0, 0, 0, 0, 0,
24, 188, 164, 233 ]
```

```
        Step 4.iii
                S is        34446922 AC4C9298 4EEE6E14 A46F08CD
        Step 4.iv
                y is  69475064367285894906781299751189940429
        Step 4.v
                c is  644424194
        Step 4.vi
                C is    4 9 1 4 2 4 4 4 6
        Step 4.vii
                A is    9 6 1 6 1 0 5 1 4
        Step 4.viii
                B is    4 9 1 4 2 4 4 4 6
Step 5
        A || B is    9 6 1 6 1 0 5 1 4 4 9 1 4 2 4 4 4 6

CT is 961610514491424446
----------------------------------------------------------------

FF3.Decrypt()

X is    9 6 1 6 1 0 5 1 4 4 9 1 4 2 4 4 4 6
Tweak is 9A 76 8A 92 F6 0E 12 D8

Step 1
        u is <9>, and v is <9>
Step 2
        A is    9 6 1 6 1 0 5 1 4
        B is    4 9 1 4 2 4 4 4 6
Step 3
        T_L is      9A768A92
        T_R is      F60E12D8

Round #7
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 149, 0, 0, 0, 0, 0, 0, 0, 0,
24, 188, 164, 233 ]
        Step 4.iii
                S is        34446922 AC4C9298 4EEE6E14 A46F08CD
        Step 4.iv
                y is  69475064367285894906781299751189940429
        Step 4.v
                c is  454483765
        Step 4.vi
                C is    5 6 7 3 8 4 4 5 4
        Step 4.vii
                B is    9 6 1 6 1 0 5 1 4
        Step 4.viii
```

```
                A is    5 6 7 3 8 4 4 5 4

Round #6
        Step 4.i
                m is <9>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 222, 0, 0, 0, 0, 0, 0, 0, 0, 27,
22, 223, 53 ]
        Step 4.iii
                S is        FA4BAD69 C2494073 3D5092B1 E1B3D6B9
        Step 4.iv
                y is  33269993844656622388225181841476208812l
        Step 4.v
                c is  652928048
        Step 4.vi
                C is    8 4 0 8 2 9 2 5 6
        Step 4.vii
                B is    5 6 7 3 8 4 4 5 4
        Step 4.viii
                A is    8 4 0 8 2 9 2 5 6

Round #5
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 151, 0, 0, 0, 0, 0, 0, 0, 0,
38, 234, 228, 48 ]
        Step 4.iii
                S is        10B970AE 19271C43 9154665E 21F9879C
        Step 4.iv
                y is  22230508274747890371985356286747838364
        Step 4.v
                c is  706645401
        Step 4.vi
                C is    1 0 4 5 4 6 6 0 7
        Step 4.vii
                B is    8 4 0 8 2 9 2 5 6
        Step 4.viii
                A is    1 0 4 5 4 6 6 0 7

Round #4
        Step 4.i
                m is <9>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 220, 0, 0, 0, 0, 0, 0, 0, 0, 42,
30, 141, 153 ]
        Step 4.iii
```

```
                S is         21EEE299 C35B961B DF4FEF6B 2DEA7A69
        Step 4.iv
                y is  45104886520173100775248438337020263017
        Step 4.v
                c is  632665031
        Step 4.vi
                C is    1 3 0 5 6 6 2 3 6
        Step 4.vii
                B is    1 0 4 5 4 6 6 0 7
        Step 4.viii
                A is    1 3 0 5 6 6 2 3 6

Round #3
        Step 4.i
                m is <9>
                W is         9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 145, 0, 0, 0, 0, 0, 0, 0, 0,
37, 181, 179, 199 ]
        Step 4.iii
                S is         835A1B57 52DC930B 6446A2F8 F721A49B
        Step 4.iv
                y is  17459672870864598005674360932532654197 9
        Step 4.v
                c is  380103422
        Step 4.vi
                C is    2 2 4 3 0 1 0 8 3
        Step 4.vii
                B is    1 3 0 5 6 6 2 3 6
        Step 4.viii
                A is    2 2 4 3 0 1 0 8 3

Round #2
        Step 4.i
                m is <9>
                W is         F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 218, 0, 0, 0, 0, 0, 0, 0, 0, 22,
167, 234, 254 ]
        Step 4.iii
                S is         3E3648A1 14EA512D 4732B51B 57CF2364
        Step 4.iv
                y is  826939928647242647139412437159671980 52
        Step 4.v
                c is  665466979
        Step 4.vi
                C is    9 7 9 6 6 4 5 6 6
        Step 4.vii
                B is    2 2 4 3 0 1 0 8 3
        Step 4.viii
```

```
                A is    9 7 9 6 6 4 5 6 6

Round #1
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 147, 0, 0, 0, 0, 0, 0, 0, 0,
39, 170, 56, 99 ]
        Step 4.iii
                S is        5D9716D7 29C024E9 3E9A9742 A7E30331
        Step 4.iv
                y is  124402703693623329523381064393380004657
        Step 4.v
                c is  98765
        Step 4.vi
                C is    5 6 7 8 9 0 0 0 0
        Step 4.vii
                B is    9 7 9 6 6 4 5 6 6
        Step 4.viii
                A is    5 6 7 8 9 0 0 0 0

Round #0
        Step 4.i
                m is <9>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 216, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 129, 205 ]
        Step 4.iii
                S is        97757BFC 9FB91E2B F4E6622B 861B9759
        Step 4.iv
                y is  201323440847280984711162106970233345881
        Step 4.v
                c is  432121098
        Step 4.vi
                C is    8 9 0 1 2 1 2 3 4
        Step 4.vii
                B is    5 6 7 8 9 0 0 0 0
        Step 4.viii
                A is    8 9 0 1 2 1 2 3 4
Step 5
        A || B is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0

PTout is <890121234567890000>
================================================================

Sample #8

FF3-AES192
```

```
Key is EF 43 59 D8 D5 80 AA 4F 7F 03 6D 6F 04 FC 6A 94 2B 7E 15 16 28
AE D2 A6
Radix = 10
------------------------------------------------------------


PT is <8901212345678900000789000000>

FF3.Encrypt()

X is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0 0 0 7 8 9 0 0 0 0 0 0
Tweak is D8 E7 92 0A FA 33 0A 73

Step 1
        u is <15>, and v is <14>
Step 2
        A is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0
        B is    0 0 0 0 0 7 8 9 0 0 0 0 0 0
Step 3
        T_L is      D8E7920A
        T_R is      FA330A73

Round #0
        Step 4.i
                m is <15>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 115, 0, 0, 0, 0, 0, 0, 0, 0, 5,
226, 10, 224 ]
        Step 4.iii
                S is        655916C8 41E0754A 0E3D147C 689E577A
        Step 4.iv
                y is  134714604073717764916785235229849573242
        Step 4.v
                c is  333995281694340
        Step 4.vi
                C is    0 4 3 4 9 6 1 8 2 5 9 9 3 3 3
        Step 4.vii
                A is    0 0 0 0 0 7 8 9 0 0 0 0 0 0 0
        Step 4.viii
                B is    0 4 3 4 9 6 1 8 2 5 9 9 3 3 3

Round #1
        Step 4.i
                m is <14>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 11, 0, 0, 0, 0, 0, 1, 47, 196,
86, 31, 62, 132 ]
```

```
        Step 4.iii
                S is         CAB08562 8345FD45 47A9F6B0 D0638DBA
        Step 4.iv
                y is  269420604761119496264120912891527531962
        Step 4.v
                c is  12891626231962
        Step 4.vi
                C is    2 6 9 1 3 2 6 2 6 1 9 8 2 1
        Step 4.vii
                A is    0 4 3 4 9 6 1 8 2 5 9 9 3 3 3
        Step 4.viii
                B is    2 6 9 1 3 2 6 2 6 1 9 8 2 1

Round #2
        Step 4.i
                m is <15>
                W is         FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 113, 0, 0, 0, 0, 0, 0, 11, 185,
144, 205, 88, 154 ]
        Step 4.iii
                S is         80F61479 77AA963A 9B242B3D 19E22E86
        Step 4.iv
                y is  171418903759503479581836378153068670598
        Step 4.v
                c is  712148350364938
        Step 4.vi
                C is    8 3 9 4 6 3 0 5 3 8 4 1 2 1 7
        Step 4.vii
                A is    2 6 9 1 3 2 6 2 6 1 9 8 2 1
        Step 4.viii
                B is    8 3 9 4 6 3 0 5 3 8 4 1 2 1 7

Round #3
        Step 4.i
                m is <14>
                W is         D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 9, 0, 0, 0, 0, 0, 2, 135, 177,
245, 115, 109, 10 ]
        Step 4.iii
                S is         712F89C4 9B31E520 46D65891 5AB571FD
        Step 4.iv
                y is  150449595742912679516123734845540364797
        Step 4.v
                c is  47737166596759
        Step 4.vi
                C is    9 5 7 6 9 5 6 6 1 7 3 7 7 4
        Step 4.vii
                A is    8 3 9 4 6 3 0 5 3 8 4 1 2 1 7
```

```
        Step 4.viii
                B is    9 5 7 6 9 5 6 6 1 7 3 7 7 4

Round #4
        Step 4.i
                m is <15>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 119, 0, 0, 0, 0, 0, 0, 43, 106,
172, 219, 138, 151 ]
        Step 4.iii
                S is        84F02D40 F2BDB692 89D3F28B C15E5F1B
        Step 4.iv
                y is  176705164543816540622765271556919549723
        Step 4.v
                c is  983705269914661
        Step 4.vi
                C is    1 6 6 4 1 9 9 6 2 5 0 7 3 8 9
        Step 4.vii
                A is    9 5 7 6 9 5 6 6 1 7 3 7 7 4
        Step 4.viii
                B is    1 6 6 4 1 9 9 6 2 5 0 7 3 8 9

Round #5
        Step 4.i
                m is <14>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 15, 0, 0, 0, 0, 0, 3, 126,
172, 187, 45, 76, 37 ]
        Step 4.iii
                S is        68F52A89 C278D62B 3A8FE458 EAE196FF
        Step 4.iv
                y is  139512687067620075762909832523467036415
        Step 4.v
                c is  80260633633174
        Step 4.vi
                C is    4 7 1 3 3 6 3 3 6 0 6 2 0 8
        Step 4.vii
                A is    1 6 6 4 1 9 9 6 2 5 0 7 3 8 9
        Step 4.viii
                B is    4 7 1 3 3 6 3 3 6 0 6 2 0 8

Round #6
        Step 4.i
                m is <15>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 117, 0, 0, 0, 0, 0, 0, 72, 255,
34, 142, 161, 150 ]
```

```
        Step 4.iii
                S is        C4D2C50C 640D2A8C 5468052B 1C37551E
        Step 4.iv
                y is  261623066130530112387191221650778969374
        Step 4.v
                c is  205356048884035
        Step 4.vi
                C is    5 3 0 4 8 8 8 4 0 6 5 3 5 0 2
        Step 4.vii
                A is    4 7 1 3 3 6 3 3 6 0 6 2 0 8
        Step 4.viii
                B is    5 3 0 4 8 8 8 4 0 6 5 3 5 0 2

Round #7
        Step 4.i
                m is <14>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 13, 0, 0, 0, 0, 0, 0, 186,
197, 46, 88, 161, 67 ]
        Step 4.iii
                S is        00A42BCE 76440F12 85D5E4EC DB7CF196
        Step 4.iv
                y is  852425186015655983195790547735081366
        Step 4.v
                c is  70808368714540
        Step 4.vi
                C is    0 4 5 4 1 7 8 6 3 8 0 8 0 7
        Step 4.vii
                A is    5 3 0 4 8 8 8 4 0 6 5 3 5 0 2
        Step 4.viii
                B is    0 4 5 4 1 7 8 6 3 8 0 8 0 7
Step 5
        A || B is    5 3 0 4 8 8 8 4 0 6 5 3 5 0 2 0 4 5 4 1 7 8 6 3 8
0 8 0 7

CT is 530488840653502045417863808O7
------------------------------------------------------------

FF3.Decrypt()

X is    5 3 0 4 8 8 8 4 0 6 5 3 5 0 2 0 4 5 4 1 7 8 6 3 8 0 8 0 7
Tweak is D8 E7 92 0A FA 33 0A 73

Step 1
        u is <15>, and v is <14>
Step 2
        A is    5 3 0 4 8 8 8 4 0 6 5 3 5 0 2
        B is    0 4 5 4 1 7 8 6 3 8 0 8 0 7
Step 3
```

```
        T_L is      D8E7920A
        T_R is      FA330A73

Round #7
        Step 4.i
                m is <14>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 13, 0, 0, 0, 0, 0, 0, 186,
197, 46, 88, 161, 67 ]
        Step 4.iii
                S is        00A42BCE 76440F12 85D5E4EC DB7CF196
        Step 4.iv
                y is  852425186015655983195790547735081366
        Step 4.v
                c is  80260633633174
        Step 4.vi
                C is    4 7 1 3 3 6 3 3 6 0 6 2 0 8
        Step 4.vii
                B is    5 3 0 4 8 8 8 4 0 6 5 3 5 0 2
        Step 4.viii
                A is    4 7 1 3 3 6 3 3 6 0 6 2 0 8

Round #6
        Step 4.i
                m is <15>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 117, 0, 0, 0, 0, 0, 0, 72, 255,
34, 142, 161, 150 ]
        Step 4.iii
                S is        C4D2C50C 640D2A8C 5468052B 1C37551E
        Step 4.iv
                y is  261623066130530112387191221650778969374
        Step 4.v
                c is  983705269914661
        Step 4.vi
                C is    1 6 6 4 1 9 9 6 2 5 0 7 3 8 9
        Step 4.vii
                B is    4 7 1 3 3 6 3 3 6 0 6 2 0 8
        Step 4.viii
                A is    1 6 6 4 1 9 9 6 2 5 0 7 3 8 9

Round #5
        Step 4.i
                m is <14>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 15, 0, 0, 0, 0, 0, 3, 126,
172, 187, 45, 76, 37 ]
```

```
        Step 4.iii
                S is        68F52A89 C278D62B 3A8FE458 EAE196FF
        Step 4.iv
                y is  139512687067620075762909832523467036415
        Step 4.v
                c is  47737166596759
        Step 4.vi
                C is    9 5 7 6 9 5 6 6 1 7 3 7 7 4
        Step 4.vii
                B is    1 6 6 4 1 9 9 6 2 5 0 7 3 8 9
        Step 4.viii
                A is    9 5 7 6 9 5 6 6 1 7 3 7 7 4

Round #4
        Step 4.i
                m is <15>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 119, 0, 0, 0, 0, 0, 0, 43, 106,
172, 219, 138, 151 ]
        Step 4.iii
                S is        84F02D40 F2BDB692 89D3F28B C15E5F1B
        Step 4.iv
                y is  176705164543816540622765271556919549723
        Step 4.v
                c is  712148350364938
        Step 4.vi
                C is    8 3 9 4 6 3 0 5 3 8 4 1 2 1 7
        Step 4.vii
                B is    9 5 7 6 9 5 6 6 1 7 3 7 7 4
        Step 4.viii
                A is    8 3 9 4 6 3 0 5 3 8 4 1 2 1 7

Round #3
        Step 4.i
                m is <14>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 9, 0, 0, 0, 0, 0, 2, 135, 177,
245, 115, 109, 10 ]
        Step 4.iii
                S is        712F89C4 9B31E520 46D65891 5AB571FD
        Step 4.iv
                y is  150449595742912679516123734845540364797
        Step 4.v
                c is  12891626231962
        Step 4.vi
                C is    2 6 9 1 3 2 6 2 6 1 9 8 2 1
        Step 4.vii
                B is    8 3 9 4 6 3 0 5 3 8 4 1 2 1 7
```

```
        Step 4.viii
                A is    2 6 9 1 3 2 6 2 6 1 9 8 2 1

Round #2
        Step 4.i
                m is <15>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 113, 0, 0, 0, 0, 0, 0, 11, 185,
144, 205, 88, 154 ]
        Step 4.iii
                S is        80F61479 77AA963A 9B242B3D 19E22E86
        Step 4.iv
                y is  171418903759503479581836378153068670598
        Step 4.v
                c is  333995281694340
        Step 4.vi
                C is    0 4 3 4 9 6 1 8 2 5 9 9 3 3 3
        Step 4.vii
                B is    2 6 9 1 3 2 6 2 6 1 9 8 2 1
        Step 4.viii
                A is    0 4 3 4 9 6 1 8 2 5 9 9 3 3 3

Round #1
        Step 4.i
                m is <14>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 11, 0, 0, 0, 0, 0, 1, 47, 196,
86, 31, 62, 132 ]
        Step 4.iii
                S is        CAB08562 8345FD45 47A9F6B0 D0638DBA
        Step 4.iv
                y is  269420604761119496264120912891527531962
        Step 4.v
                c is  98700000
        Step 4.vi
                C is    0 0 0 0 0 7 8 9 0 0 0 0 0 0
        Step 4.vii
                B is    0 4 3 4 9 6 1 8 2 5 9 9 3 3 3
        Step 4.viii
                A is    0 0 0 0 0 7 8 9 0 0 0 0 0 0

Round #0
        Step 4.i
                m is <15>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 115, 0, 0, 0, 0, 0, 0, 0, 0, 5,
226, 10, 224 ]
```

```
        Step 4.iii
                S is        655916C8 41E0754A 0E3D147C 689E577A
        Step 4.iv
                y is  134714604073717764916785235229849573242
        Step 4.v
                c is  98765432121098
        Step 4.vi
                C is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0
        Step 4.vii
                B is    0 0 0 0 0 7 8 9 0 0 0 0 0 0 0
        Step 4.viii
                A is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0
Step 5
        A || B is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0 0 0 7 8 9 0 0
0 0 0 0

PTout is <8901212345678900000789000000>
============================================================

Sample #9

FF3-AES192

Key is EF 43 59 D8 D5 80 AA 4F 7F 03 6D 6F 04 FC 6A 94 2B 7E 15 16 28
AE D2 A6
Radix = 10
------------------------------------------------------------


PT is <8901212345678900000789000000>

FF3.Encrypt()

X is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0 0 0 7 8 9 0 0 0 0 0 0
Tweak is 00 00 00 00 00 00 00

Step 1
        u is <15>, and v is <14>
Step 2
        A is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0
        B is    0 0 0 0 0 7 8 9 0 0 0 0 0 0 0
Step 3
        T_L is      00000000
        T_R is      00000000

Round #0
        Step 4.i
                m is <15>
                W is        00000000
        Step 4.ii
```

```
                P is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 226,
10, 224 ]
        Step 4.iii
                S is         7A65D538 5FD53EED C59AFCB9 B865359D
        Step 4.iv
                y is  162694562088153306994794199463150040477
        Step 4.v
                c is  298228582161575
        Step 4.vi
                C is    5 7 5 1 6 1 2 8 5 8 2 2 8 9 2
        Step 4.vii
                A is    0 0 0 0 0 7 8 9 0 0 0 0 0 0 0
        Step 4.viii
                B is    5 7 5 1 6 1 2 8 5 8 2 2 8 9 2

Round #1
        Step 4.i
                m is <14>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 15, 60, 192,
179, 156, 167 ]
        Step 4.iii
                S is         1D1562CC 8B1BF838 A06F9991 484FDF97
        Step 4.iv
                y is  38658653993530332021798568042590887831
        Step 4.v
                c is  68042689587831
        Step 4.vi
                C is    1 3 8 7 8 5 9 8 6 2 4 0 8 6
        Step 4.vii
                A is    5 7 5 1 6 1 2 8 5 8 2 2 8 9 2
        Step 4.viii
                B is    1 3 8 7 8 5 9 8 6 2 4 0 8 6

Round #2
        Step 4.i
                m is <15>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 61, 226, 108,
87, 170, 119 ]
        Step 4.iii
                S is         E17C42FE C0F62735 E486F548 B5FA10A3
        Step 4.iv
                y is  29972150268477021246644493796172064784 3
        Step 4.v
                c is  236190302809418
        Step 4.vi
                C is    8 1 4 9 0 8 2 0 3 0 9 1 6 3 2
```

```
        Step 4.vii
                A is    1 3 8 7 8 5 9 8 6 2 4 0 8 6
        Step 4.viii
                B is    8 1 4 9 0 8 2 0 3 0 9 1 6 3 2

Round #3
        Step 4.i
                m is <14>
                W is        00000000
        Step 4.ii
                P is  [ 0, 0, 0, 3, 0, 0, 0, 0, 0, 0, 214, 208, 87,
25, 45, 74 ]
        Step 4.iii
                S is        A409A8FC D7FA9A25 8DF73B9F 84E48D02
        Step 4.iv
                y is  218043549457605620183815879421262597378
        Step 4.v
                c is  47463952185209
        Step 4.vi
                C is    9 0 2 5 8 1 2 5 9 3 6 4 7 4
        Step 4.vii
                A is    8 1 4 9 0 8 2 0 3 0 9 1 6 3 2
        Step 4.viii
                B is    9 0 2 5 8 1 2 5 9 3 6 4 7 4

Round #4
        Step 4.i
                m is <15>
                W is        00000000
        Step 4.ii
                P is  [ 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 43, 43, 16, 2,
119, 121 ]
        Step 4.iii
                S is        A110530F FBB7C1E9 13C2080F A1EF1BA8
        Step 4.iv
                y is  21409046877743044018857303787159886941 6
        Step 4.v
                c is  274061901678834
        Step 4.vi
                C is    4 3 8 8 7 6 1 0 9 1 6 0 4 7 2
        Step 4.vii
                A is    9 0 2 5 8 1 2 5 9 3 6 4 7 4
        Step 4.viii
                B is    4 3 8 8 7 6 1 0 9 1 6 0 4 7 2

Round #5
        Step 4.i
                m is <14>
                W is        00000000
        Step 4.ii
```

```
                P is  [ 0, 0, 0, 5, 0, 0, 0, 0, 0, 0, 249, 66, 2, 75,
200, 242 ]
        Step 4.iii
                S is         3FE53C0C C83F7EBC 8785A841 EFD07005
        Step 4.iv
                y is  84931617672342107578105675598485549061
        Step 4.v
                c is  23062437734270
        Step 4.vi
                C is    0 7 2 4 3 7 7 3 4 2 6 0 3 2
        Step 4.vii
                A is    4 3 8 8 7 6 1 0 9 1 6 0 4 7 2
        Step 4.viii
                B is    0 7 2 4 3 7 7 3 4 2 6 0 3 2

Round #6
        Step 4.i
                m is <15>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 6, 0, 0, 0, 0, 0, 0, 20, 249, 164,
104, 167, 126 ]
        Step 4.iii
                S is         AF61D617 5DC9EAB9 834723AF E44239D7
        Step 4.iv
                y is  233122894344567283782676028825719159255
        Step 4.v
                c is  302887620838089
        Step 4.vi
                C is    9 8 0 8 3 8 0 2 6 7 8 8 2 0 3
        Step 4.vii
                A is    0 7 2 4 3 7 7 3 4 2 6 0 3 2
        Step 4.viii
                B is    9 8 0 8 3 8 0 2 6 7 8 8 2 0 3

Round #7
        Step 4.i
                m is <14>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 7, 0, 0, 0, 0, 0, 1, 19, 121, 133,
12, 2, 201 ]
        Step 4.iii
                S is         DC13EDFB ABCCA2B5 3F6BC34C 1497F7A4
        Step 4.iv
                y is  29253363958350783620347109847597632502 8
        Step 4.v
                c is  21538414059298
        Step 4.vi
                C is    8 9 2 9 5 0 4 1 4 8 3 5 1 2
```

```
        Step 4.vii
                A is    9 8 0 8 3 8 0 2 6 7 8 8 2 0 3
        Step 4.viii
                B is    8 9 2 9 5 0 4 1 4 8 3 5 1 2
Step 5
        A || B is    9 8 0 8 3 8 0 2 6 7 8 8 2 0 3 8 9 2 9 5 0 4 1 4 8
3 5 1 2

CT is 98083802678820389295041483512
------------------------------------------------------------

FF3.Decrypt()

X is    9 8 0 8 3 8 0 2 6 7 8 8 2 0 3 8 9 2 9 5 0 4 1 4 8 3 5 1 2
Tweak is 00 00 00 00 00 00 00 00

Step 1
        u is <15>, and v is <14>
Step 2
        A is    9 8 0 8 3 8 0 2 6 7 8 8 2 0 3
        B is    8 9 2 9 5 0 4 1 4 8 3 5 1 2
Step 3
        T_L is      00000000
        T_R is      00000000

Round #7
        Step 4.i
                m is <14>
                W is        00000000
        Step 4.ii
                P is  [ 0, 0, 0, 7, 0, 0, 0, 0, 0, 1, 19, 121, 133,
12, 2, 201 ]
        Step 4.iii
                S is        DC13EDFB ABCCA2B5 3F6BC34C 1497F7A4
        Step 4.iv
                y is  292533639583507836203471098475976325028
        Step 4.v
                c is  23062437734270
        Step 4.vi
                C is    0 7 2 4 3 7 7 3 4 2 6 0 3 2
        Step 4.vii
                B is    9 8 0 8 3 8 0 2 6 7 8 8 2 0 3
        Step 4.viii
                A is    0 7 2 4 3 7 7 3 4 2 6 0 3 2

Round #6
        Step 4.i
                m is <15>
                W is        00000000
        Step 4.ii
```

```
                P is  [ 0, 0, 0, 6, 0, 0, 0, 0, 0, 0, 20, 249, 164,
104, 167, 126 ]
        Step 4.iii
                S is         AF61D617 5DC9EAB9 834723AF E44239D7
        Step 4.iv
                y is  233122894344567283782676028825719159255
        Step 4.v
                c is  274061901678834
        Step 4.vi
                C is    4 3 8 8 7 6 1 0 9 1 6 0 4 7 2
        Step 4.vii
                B is    0 7 2 4 3 7 7 3 4 2 6 0 3 2
        Step 4.viii
                A is    4 3 8 8 7 6 1 0 9 1 6 0 4 7 2

Round #5
        Step 4.i
                m is <14>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 5, 0, 0, 0, 0, 0, 0, 249, 66, 2, 75,
200, 242 ]
        Step 4.iii
                S is         3FE53C0C C83F7EBC 8785A841 EFD07005
        Step 4.iv
                y is  84931617672342107578105675598485549061
        Step 4.v
                c is  47463952185209
        Step 4.vi
                C is    9 0 2 5 8 1 2 5 9 3 6 4 7 4
        Step 4.vii
                B is    4 3 8 8 7 6 1 0 9 1 6 0 4 7 2
        Step 4.viii
                A is    9 0 2 5 8 1 2 5 9 3 6 4 7 4

Round #4
        Step 4.i
                m is <15>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 43, 43, 16, 2,
119, 121 ]
        Step 4.iii
                S is         A110530F FBB7C1E9 13C2080F A1EF1BA8
        Step 4.iv
                y is  21409046877743044018857303787159886941 6
        Step 4.v
                c is  236190302809418
        Step 4.vi
                C is    8 1 4 9 0 8 2 0 3 0 9 1 6 3 2
```

```
        Step 4.vii
                B is    9 0 2 5 8 1 2 5 9 3 6 4 7 4
        Step 4.viii
                A is    8 1 4 9 0 8 2 0 3 0 9 1 6 3 2

Round #3
        Step 4.i
                m is <14>
                W is        00000000
        Step 4.ii
                P is  [ 0, 0, 0, 3, 0, 0, 0, 0, 0, 0, 214, 208, 87,
25, 45, 74 ]
        Step 4.iii
                S is        A409A8FC D7FA9A25 8DF73B9F 84E48D02
        Step 4.iv
                y is  218043549457605620183815879421262597378
        Step 4.v
                c is  68042689587831
        Step 4.vi
                C is    1 3 8 7 8 5 9 8 6 2 4 0 8 6
        Step 4.vii
                B is    8 1 4 9 0 8 2 0 3 0 9 1 6 3 2
        Step 4.viii
                A is    1 3 8 7 8 5 9 8 6 2 4 0 8 6

Round #2
        Step 4.i
                m is <15>
                W is        00000000
        Step 4.ii
                P is  [ 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 61, 226, 108,
87, 170, 119 ]
        Step 4.iii
                S is        E17C42FE C0F62735 E486F548 B5FA10A3
        Step 4.iv
                y is  299721502684770212466444937961720647843
        Step 4.v
                c is  298228582161575
        Step 4.vi
                C is    5 7 5 1 6 1 2 8 5 8 2 2 8 9 2
        Step 4.vii
                B is    1 3 8 7 8 5 9 8 6 2 4 0 8 6
        Step 4.viii
                A is    5 7 5 1 6 1 2 8 5 8 2 2 8 9 2

Round #1
        Step 4.i
                m is <14>
                W is        00000000
        Step 4.ii
```

```
                P is  [ 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 15, 60, 192,
179, 156, 167 ]
        Step 4.iii
                S is         1D1562CC 8B1BF838 A06F9991 484FDF97
        Step 4.iv
                y is  386586539935303320217985680425908878 31
        Step 4.v
                c is  98700000
        Step 4.vi
                C is    0 0 0 0 0 7 8 9 0 0 0 0 0 0 0
        Step 4.vii
                B is    5 7 5 1 6 1 2 8 5 8 2 2 8 9 2
        Step 4.viii
                A is    0 0 0 0 0 7 8 9 0 0 0 0 0 0 0

Round #0
        Step 4.i
                m is <15>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 226,
10, 224 ]
        Step 4.iii
                S is         7A65D538 5FD53EED C59AFCB9 B865359D
        Step 4.iv
                y is  162694562088153306994794199463150040477
        Step 4.v
                c is  98765432121098
        Step 4.vi
                C is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0
        Step 4.vii
                B is    0 0 0 0 0 7 8 9 0 0 0 0 0 0 0
        Step 4.viii
                A is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0
Step 5
        A || B is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0 0 0 7 8 9 0 0
0 0 0 0

PTout is <8901212345678900000789000000>
================================================================

Sample #10

FF3-AES192

Key is EF 43 59 D8 D5 80 AA 4F 7F 03 6D 6F 04 FC 6A 94 2B 7E 15 16 28
AE D2 A6
Radix = 26
----------------------------------------------------------------
```

```
PT is <0123456789abcdefghi>

FF3.Encrypt()

X is    0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
Tweak is 9A 76 8A 92 F6 0E 12 D8

Step 1
        u is <10>, and v is <9>
Step 2
        A is    0 1 2 3 4 5 6 7 8 9
        B is    10 11 12 13 14 15 16 17 18
Step 3
        T_L is      9A768A92
        T_R is      F60E12D8

Round #0
        Step 4.i
                m is <10>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 216, 0, 0, 0, 0, 0, 0, 3, 140,
43, 56, 187, 32 ]
        Step 4.iii
                S is        D6F4C136 4D09B185 09B40012 35F8E286
        Step 4.iv
                y is  285725630338670839687045919480512832134
        Step 4.v
                c is  99773762621760
        Step 4.vi
                C is    6 25 8 24 5 12 8 20 9 18
        Step 4.vii
                A is    10 11 12 13 14 15 16 17 18
        Step 4.viii
                B is    6 25 8 24 5 12 8 20 9 18

Round #1
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 147, 0, 0, 0, 0, 0, 0, 90,
190, 99, 173, 209, 64 ]
        Step 4.iii
                S is        269AFEEF CF074760 A82043F4 D071D5E2
        Step 4.iv
                y is  513154482876835316433809363517383531 22
        Step 4.v
                c is  3967624097538
```

```
        Step 4.vi
                C is    10 12 0 20 10 18 25 25 18
        Step 4.vii
                A is    6 25 8 24 5 12 8 20 9 18
        Step 4.viii
                B is    10 12 0 20 10 18 25 25 18

Round #2
        Step 4.i
                m is <10>
                W is         F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 218, 0, 0, 0, 0, 0, 0, 3, 155,
200, 211, 47, 2 ]
        Step 4.iii
                S is         FEAB0CDE 038E92BD BFF5174C AF744E68
        Step 4.iv
                y is  338512054670846224690396170214232575592
        Step 4.v
                c is  129674850110376
        Step 4.vi
                C is    12 18 20 17 7 3 4 25 22 23
        Step 4.vii
                A is    10 12 0 20 10 18 25 25 18
        Step 4.viii
                B is    12 18 20 17 7 3 4 25 22 23

Round #3
        Step 4.i
                m is <9>
                W is         9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 145, 0, 0, 0, 0, 0, 0, 117,
240, 71, 96, 139, 168 ]
        Step 4.iii
                S is         FDB98925 971B8AD3 69E51575 4CBA382E
        Step 4.iv
                y is  337258039520735905329190764472490932270
        Step 4.v
                c is  5149084232496
        Step 4.vi
                C is    22 15 13 12 10 6 2 17 24
        Step 4.vii
                A is    12 18 20 17 7 3 4 25 22 23
        Step 4.viii
                B is    22 15 13 12 10 6 2 17 24

Round #4
        Step 4.i
                m is <10>
```

```
                W is         F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 220, 0, 0, 0, 0, 0, 0, 4, 174,
221, 86, 43, 48 ]
        Step 4.iii
                S is         116F6904 0315BD0A 8FC8C0D2 E0A1B603
        Step 4.iv
                y is  231753508505167043823528584264643845l5
        Step 4.v
                c is  28000220519851
        Step 4.vi
                C is    21 25 9 25 24 7 4 2 4 5
        Step 4.vii
                A is    22 15 13 12 10 6 2 17 24
        Step 4.viii
                B is    21 25 9 25 24 7 4 2 4 5

Round #5
        Step 4.i
                m is <9>
                W is         9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 151, 0, 0, 0, 0, 0, 0, 25,
119, 79, 50, 157, 171 ]
        Step 4.iii
                S is         23878299 909B32E3 63102446 229AC931
        Step 4.iv
                y is  472265888082850619102708799949543037 93
        Step 4.v
                c is  713197414497
        Step 4.vi
                C is    9 2 23 25 12 18 20 10 3
        Step 4.vii
                A is    21 25 9 25 24 7 4 2 4 5
        Step 4.viii
                B is    9 2 23 25 12 18 20 10 3

Round #6
        Step 4.i
                m is <10>
                W is         F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 222, 0, 0, 0, 0, 0, 0, 0, 166,
13, 224, 232, 97 ]
        Step 4.iii
                S is         4F62AC9A 185C05C6 243203F0 F497FC77
        Step 4.iv
                y is  105521357542272511029030374679216913527
        Step 4.v
                c is  42100617003554
```

```
        Step 4.vi
                C is    18 0 18 17 14 2 19 15 19 7
        Step 4.vii
                A is    9 2 23 25 12 18 20 10 3
        Step 4.viii
                B is    18 0 18 17 14 2 19 15 19 7

Round #7
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 149, 0, 0, 0, 0, 0, 0, 38, 74,
80, 82, 66, 34 ]
        Step 4.iii
                S is        844FE530 13F25D51 345BED61 8D41D12B
        Step 4.iv
                y is  175872935376357399436166073107286708523
        Step 4.v
                c is  1742708135308
        Step 4.vi
                C is    10 9 24 25 15 9 25 8 8
        Step 4.vii
                A is    18 0 18 17 14 2 19 15 19 7
        Step 4.viii
                B is    10 9 24 25 15 9 25 8 8
Step 5
        A || B is    18 0 18 17 14 2 19 15 19 7 10 9 24 25 15 9 25 8 8

CT is i0ihe2jfj7a9opf9p88
----------------------------------------------------------------

FF3.Decrypt()

X is    18 0 18 17 14 2 19 15 19 7 10 9 24 25 15 9 25 8 8
Tweak is 9A 76 8A 92 F6 0E 12 D8

Step 1
        u is <10>, and v is <9>
Step 2
        A is    18 0 18 17 14 2 19 15 19 7
        B is    10 9 24 25 15 9 25 8 8
Step 3
        T_L is      9A768A92
        T_R is      F60E12D8

Round #7
        Step 4.i
                m is <9>
                W is        9A768A92
```

```
        Step 4.ii
                P is  [ 154, 118, 138, 149, 0, 0, 0, 0, 0, 0, 38, 74,
80, 82, 66, 34 ]
        Step 4.iii
                S is         844FE530 13F25D51 345BED61 8D41D12B
        Step 4.iv
                y is  175872935376357399436166073107286708523
        Step 4.v
                c is  713197414497
        Step 4.vi
                C is    9 2 23 25 12 18 20 10 3
        Step 4.vii
                B is    18 0 18 17 14 2 19 15 19 7
        Step 4.viii
                A is    9 2 23 25 12 18 20 10 3

Round #6
        Step 4.i
                m is <10>
                W is         F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 222, 0, 0, 0, 0, 0, 0, 0, 166,
13, 224, 232, 97 ]
        Step 4.iii
                S is         4F62AC9A 185C05C6 243203F0 F497FC77
        Step 4.iv
                y is  105521357542272511029030374679216913527
        Step 4.v
                c is  28000220519851
        Step 4.vi
                C is    21 25 9 25 24 7 4 2 4 5
        Step 4.vii
                B is    9 2 23 25 12 18 20 10 3
        Step 4.viii
                A is    21 25 9 25 24 7 4 2 4 5

Round #5
        Step 4.i
                m is <9>
                W is         9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 151, 0, 0, 0, 0, 0, 0, 25,
119, 79, 50, 157, 171 ]
        Step 4.iii
                S is         23878299 909B32E3 63102446 229AC931
        Step 4.iv
                y is  472265888082850619102708799949543037 93
        Step 4.v
                c is  5149084232496
        Step 4.vi
```

```
                C is    22 15 13 12 10 6 2 17 24
        Step 4.vii
                B is    21 25 9 25 24 7 4 2 4 5
        Step 4.viii
                A is    22 15 13 12 10 6 2 17 24

Round #4
        Step 4.i
                m is <10>
                W is         F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 220, 0, 0, 0, 0, 0, 0, 4, 174,
221, 86, 43, 48 ]
        Step 4.iii
                S is         116F6904 0315BD0A 8FC8C0D2 E0A1B603
        Step 4.iv
                y is  231753508505167043823528584264643845l5
        Step 4.v
                c is  129674850110376
        Step 4.vi
                C is    12 18 20 17 7 3 4 25 22 23
        Step 4.vii
                B is    22 15 13 12 10 6 2 17 24
        Step 4.viii
                A is    12 18 20 17 7 3 4 25 22 23

Round #3
        Step 4.i
                m is <9>
                W is         9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 145, 0, 0, 0, 0, 0, 0, 117,
240, 71, 96, 139, 168 ]
        Step 4.iii
                S is         FDB98925 971B8AD3 69E51575 4CBA382E
        Step 4.iv
                y is  337258039520735905329190764472490932270
        Step 4.v
                c is  3967624097538
        Step 4.vi
                C is    10 12 0 20 10 18 25 25 18
        Step 4.vii
                B is    12 18 20 17 7 3 4 25 22 23
        Step 4.viii
                A is    10 12 0 20 10 18 25 25 18

Round #2
        Step 4.i
                m is <10>
                W is         F60E12D8
```

```
        Step 4.ii
                P is  [ 246, 14, 18, 218, 0, 0, 0, 0, 0, 0, 3, 155,
200, 211, 47, 2 ]
        Step 4.iii
                S is         FEAB0CDE 038E92BD BFF5174C AF744E68
        Step 4.iv
                y is  338512054670846224690396170214232575592
        Step 4.v
                c is  99773762621760
        Step 4.vi
                C is    6 25 8 24 5 12 8 20 9 18
        Step 4.vii
                B is    10 12 0 20 10 18 25 25 18
        Step 4.viii
                A is    6 25 8 24 5 12 8 20 9 18

Round #1
        Step 4.i
                m is <9>
                W is         9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 147, 0, 0, 0, 0, 0, 0, 90,
190, 99, 173, 209, 64 ]
        Step 4.iii
                S is         269AFEEF CF074760 A82043F4 D071D5E2
        Step 4.iv
                y is  513154482876835316433809363517383531 22
        Step 4.v
                c is  3900555442976
        Step 4.vi
                C is    10 11 12 13 14 15 16 17 18
        Step 4.vii
                B is    6 25 8 24 5 12 8 20 9 18
        Step 4.viii
                A is    10 11 12 13 14 15 16 17 18

Round #0
        Step 4.i
                m is <10>
                W is         F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 216, 0, 0, 0, 0, 0, 0, 3, 140,
43, 56, 187, 32 ]
        Step 4.iii
                S is         D6F4C136 4D09B185 09B40012 35F8E286
        Step 4.iv
                y is  285725630338670839687045919480512832134
        Step 4.v
                c is  50594287082170
        Step 4.vi
```

```
                C is    0 1 2 3 4 5 6 7 8 9
        Step 4.vii
                B is    10 11 12 13 14 15 16 17 18
        Step 4.viii
                A is    0 1 2 3 4 5 6 7 8 9
Step 5
        A || B is    0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18

PTout is <0123456789abcdefghi>
==========================================================

Sample #11

FF3-AES256

Key is EF 43 59 D8 D5 80 AA 4F 7F 03 6D 6F 04 FC 6A 94 2B 7E 15 16 28
AE D2 A6 AB F7 15 88 09 CF 4F 3C
Radix = 10
----------------------------------------------------------


PT is <890121234567890000>

FF3.Encrypt()

X is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0
Tweak is D8 E7 92 0A FA 33 0A 73

Step 1
        u is <9>, and v is <9>
Step 2
        A is    8 9 0 1 2 1 2 3 4
        B is    5 6 7 8 9 0 0 0 0
Step 3
        T_L is      D8E7920A
        T_R is      FA330A73

Round #0
        Step 4.i
                m is <9>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 115, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 129, 205 ]
        Step 4.iii
                S is        CBE8C6FF FC3F0506 F9BBCEFE B3468753
        Step 4.iv
                y is  271041932213867374919564698371299379027
        Step 4.v
                c is  731500125
```

```
        Step 4.vi
                C is    5 2 1 0 0 5 1 3 7
        Step 4.vii
                A is    5 6 7 8 9 0 0 0 0
        Step 4.viii
                B is    5 2 1 0 0 5 1 3 7

Round #1
        Step 4.i
                m is <9>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 11, 0, 0, 0, 0, 0, 0, 0, 0,
43, 153, 206, 93 ]
        Step 4.iii
                S is        714955EA 63122B04 F8A4E2CD 1BD1B858
        Step 4.iv
                y is  150583543769235854575382615855985703000
        Step 4.v
                c is  985801765
        Step 4.vi
                C is    5 6 7 1 0 8 5 8 9
        Step 4.vii
                A is    5 2 1 0 0 5 1 3 7
        Step 4.viii
                B is    5 6 7 1 0 8 5 8 9

Round #2
        Step 4.i
                m is <9>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 113, 0, 0, 0, 0, 0, 0, 0, 0, 58,
194, 36, 37 ]
        Step 4.iii
                S is        DEAC3669 0AF76E4A 2EF8A27D 22434CDE
        Step 4.iv
                y is  295982793696388950929125828211725520094
        Step 4.v
                c is  457020219
        Step 4.vi
                C is    9 1 2 0 2 0 7 5 4
        Step 4.vii
                A is    5 6 7 1 0 8 5 8 9
        Step 4.viii
                B is    9 1 2 0 2 0 7 5 4

Round #3
        Step 4.i
                m is <9>
```

```
                W is         D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 9, 0, 0, 0, 0, 0, 0, 0, 0, 27,
61, 147, 59 ]
        Step 4.iii
                S is         7C879CE9 918C9718 95CE0E6A 93702D05
        Step 4.iv
                y is  165528414114337095023796922888913693957
        Step 4.v
                c is  899495722
        Step 4.vi
                C is    2 2 7 5 9 4 9 9 8
        Step 4.vii
                A is    9 1 2 0 2 0 7 5 4
        Step 4.viii
                B is    2 2 7 5 9 4 9 9 8

Round #4
        Step 4.i
                m is <9>
                W is         FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 119, 0, 0, 0, 0, 0, 0, 0, 0, 53,
157, 55, 42 ]
        Step 4.iii
                S is         EEF1885A CEFA7E1D 7BA6D23B CFE27832
        Step 4.iv
                y is  317610372142014333160693171438181578802
        Step 4.v
                c is  638599021
        Step 4.vi
                C is    1 2 0 9 9 5 8 3 6
        Step 4.vii
                A is    2 2 7 5 9 4 9 9 8
        Step 4.viii
                B is    1 2 0 9 9 5 8 3 6

Round #5
        Step 4.i
                m is <9>
                W is         D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 15, 0, 0, 0, 0, 0, 0, 0, 0,
38, 16, 63, 109 ]
        Step 4.iii
                S is         7EBC063A 1296E0EA C3A41B6B CFB44E7D
        Step 4.iv
                y is  168459005573748126507851651559525207677
        Step 4.v
                c is  424703399
```

```
        Step 4.vi
                C is    9 9 3 3 0 7 4 2 4
        Step 4.vii
                A is    1 2 0 9 9 5 8 3 6
        Step 4.viii
                B is    9 9 3 3 0 7 4 2 4

Round #6
        Step 4.i
                m is <9>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 117, 0, 0, 0, 0, 0, 0, 0, 0, 25,
80, 117, 167 ]
        Step 4.iii
                S is        C654842D 93053F21 3C55555D 50E01AA8
        Step 4.iv
                y is  263625976990365902713155760716863511208
        Step 4.v
                c is  502110229
        Step 4.vi
                C is    9 2 2 0 1 1 2 0 5
        Step 4.vii
                A is    9 9 3 3 0 7 4 2 4
        Step 4.viii
                B is    9 2 2 0 1 1 2 0 5

Round #7
        Step 4.i
                m is <9>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 13, 0, 0, 0, 0, 0, 0, 0, 0,
29, 237, 152, 21 ]
        Step 4.iii
                S is        6471E9E4 D928446B 1E4887DB F8B3F70A
        Step 4.iv
                y is  133514273056171654164803462652170073866
        Step 4.v
                c is  594777265
        Step 4.vi
                C is    5 6 2 7 7 7 4 9 5
        Step 4.vii
                A is    9 2 2 0 1 1 2 0 5
        Step 4.viii
                B is    5 6 2 7 7 7 4 9 5
Step 5
        A || B is    9 2 2 0 1 1 2 0 5 5 6 2 7 7 7 4 9 5

CT is 922011205562777495
```

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

FF3.Decrypt()

X is    9 2 2 0 1 1 2 0 5 5 6 2 7 7 7 4 9 5
Tweak is D8 E7 92 0A FA 33 0A 73

Step 1
        u is <9>, and v is <9>
Step 2
        A is    9 2 2 0 1 1 2 0 5
        B is    5 6 2 7 7 7 4 9 5
Step 3
        T_L is      D8E7920A
        T_R is      FA330A73

Round #7
        Step 4.i
                m is <9>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 13, 0, 0, 0, 0, 0, 0, 0, 0,
29, 237, 152, 21 ]
        Step 4.iii
                S is        6471E9E4 D928446B 1E4887DB F8B3F70A
        Step 4.iv
                y is  133514273056171654164803462652170073866
        Step 4.v
                c is  424703399
        Step 4.vi
                C is    9 9 3 3 0 7 4 2 4
        Step 4.vii
                B is    9 2 2 0 1 1 2 0 5
        Step 4.viii
                A is    9 9 3 3 0 7 4 2 4

Round #6
        Step 4.i
                m is <9>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 117, 0, 0, 0, 0, 0, 0, 0, 0, 25,
80, 117, 167 ]
        Step 4.iii
                S is        C654842D 93053F21 3C55555D 50E01AA8
        Step 4.iv
                y is  263625976990365902713155760716863511208
        Step 4.v
                c is  638599021
        Step 4.vi
```

```
                C is    1 2 0 9 9 5 8 3 6
        Step 4.vii
                B is    9 9 3 3 0 7 4 2 4
        Step 4.viii
                A is    1 2 0 9 9 5 8 3 6

Round #5
        Step 4.i
                m is <9>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 15, 0, 0, 0, 0, 0, 0, 0, 0,
38, 16, 63, 109 ]
        Step 4.iii
                S is        7EBC063A 1296E0EA C3A41B6B CFB44E7D
        Step 4.iv
                y is  168459005573748126507851651559525207677
        Step 4.v
                c is  899495722
        Step 4.vi
                C is    2 2 7 5 9 4 9 9 8
        Step 4.vii
                B is    1 2 0 9 9 5 8 3 6
        Step 4.viii
                A is    2 2 7 5 9 4 9 9 8

Round #4
        Step 4.i
                m is <9>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 119, 0, 0, 0, 0, 0, 0, 0, 0, 53,
157, 55, 42 ]
        Step 4.iii
                S is        EEF1885A CEFA7E1D 7BA6D23B CFE27832
        Step 4.iv
                y is  317610372142014333160693171438181578802
        Step 4.v
                c is  457020219
        Step 4.vi
                C is    9 1 2 0 2 0 7 5 4
        Step 4.vii
                B is    2 2 7 5 9 4 9 9 8
        Step 4.viii
                A is    9 1 2 0 2 0 7 5 4

Round #3
        Step 4.i
                m is <9>
                W is        D8E7920A
```

```
        Step 4.ii
                P is  [ 216, 231, 146, 9, 0, 0, 0, 0, 0, 0, 0, 0, 27,
61, 147, 59 ]
        Step 4.iii
                S is         7C879CE9 918C9718 95CE0E6A 93702D05
        Step 4.iv
                y is  16552841411433709502379692288891369395 7
        Step 4.v
                c is  985801765
        Step 4.vi
                C is    5 6 7 1 0 8 5 8 9
        Step 4.vii
                B is    9 1 2 0 2 0 7 5 4
        Step 4.viii
                A is    5 6 7 1 0 8 5 8 9

Round #2
        Step 4.i
                m is <9>
                W is         FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 113, 0, 0, 0, 0, 0, 0, 0, 0, 58,
194, 36, 37 ]
        Step 4.iii
                S is         DEAC3669 0AF76E4A 2EF8A27D 22434CDE
        Step 4.iv
                y is  29598279369638895092912582821172552009 4
        Step 4.v
                c is  731500125
        Step 4.vi
                C is    5 2 1 0 0 5 1 3 7
        Step 4.vii
                B is    5 6 7 1 0 8 5 8 9
        Step 4.viii
                A is    5 2 1 0 0 5 1 3 7

Round #1
        Step 4.i
                m is <9>
                W is         D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 11, 0, 0, 0, 0, 0, 0, 0, 0,
43, 153, 206, 93 ]
        Step 4.iii
                S is         714955EA 63122B04 F8A4E2CD 1BD1B858
        Step 4.iv
                y is  15058354376923585457538261585598570300 0
        Step 4.v
                c is  98765
        Step 4.vi
```

```
                C is    5 6 7 8 9 0 0 0 0
        Step 4.vii
                B is    5 2 1 0 0 5 1 3 7
        Step 4.viii
                A is    5 6 7 8 9 0 0 0 0

Round #0
        Step 4.i
                m is <9>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 115, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 129, 205 ]
        Step 4.iii
                S is        CBE8C6FF FC3F0506 F9BBCEFE B3468753
        Step 4.iv
                y is  271041932213867374919564698371299379027
        Step 4.v
                c is  432121098
        Step 4.vi
                C is    8 9 0 1 2 1 2 3 4
        Step 4.vii
                B is    5 6 7 8 9 0 0 0 0
        Step 4.viii
                A is    8 9 0 1 2 1 2 3 4
Step 5
        A || B is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0

PTout is <890121234567890000>
============================================================

Sample #12

FF3-AES256

Key is EF 43 59 D8 D5 80 AA 4F 7F 03 6D 6F 04 FC 6A 94 2B 7E 15 16 28
AE D2 A6 AB F7 15 88 09 CF 4F 3C
Radix = 10
------------------------------------------------------------


PT is <890121234567890000>

FF3.Encrypt()

X is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0
Tweak is 9A 76 8A 92 F6 0E 12 D8

Step 1
        u is <9>, and v is <9>
```

```
Step 2
        A is    8 9 0 1 2 1 2 3 4
        B is    5 6 7 8 9 0 0 0 0
Step 3
        T_L is      9A768A92
        T_R is      F60E12D8

Round #0
        Step 4.i
                m is <9>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 216, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 129, 205 ]
        Step 4.iii
                S is        F89ADB25 F087FAEA 471670EC A1EAA126
        Step 4.iv
                y is  330452601524459504934593210673066058022
        Step 4.v
                c is  498179120
        Step 4.vi
                C is    0 2 1 9 7 1 8 9 4
        Step 4.vii
                A is    5 6 7 8 9 0 0 0 0
        Step 4.viii
                B is    0 2 1 9 7 1 8 9 4

Round #1
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 147, 0, 0, 0, 0, 0, 0, 0, 0,
29, 177, 156, 48 ]
        Step 4.iii
                S is        02F7D2B5 801AD3E3 B28A8FCE 53E9C777
        Step 4.iv
                y is  394522700158863005073497285249687743 1
        Step 4.v
                c is  496976196
        Step 4.vi
                C is    6 9 1 6 7 9 6 9 4
        Step 4.vii
                A is    0 2 1 9 7 1 8 9 4
        Step 4.viii
                B is    6 9 1 6 7 9 6 9 4

Round #2
        Step 4.i
                m is <9>
```

```
                W is         F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 218, 0, 0, 0, 0, 0, 0, 0, 0, 29,
159, 65, 68 ]
        Step 4.iii
                S is         D1D1AE87 F70BEC81 CD4BA39A 31B1197F
        Step 4.iv
                y is  27889738107401138371039892420598386521 5
        Step 4.v
                c is  482044335
        Step 4.vi
                C is    5 3 3 4 4 0 2 8 4
        Step 4.vii
                A is    6 9 1 6 7 9 6 9 4
        Step 4.viii
                B is    5 3 3 4 4 0 2 8 4

Round #3
        Step 4.i
                m is <9>
                W is         9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 145, 0, 0, 0, 0, 0, 0, 0, 0,
28, 187, 105, 175 ]
        Step 4.iii
                S is         784896F6 DE0EBF2A 93E57E84 C6DA81F4
        Step 4.iv
                y is  15988426678829643849653343553421328434 0
        Step 4.v
                c is  710260536
        Step 4.vi
                C is    6 3 5 0 6 2 0 1 7
        Step 4.vii
                A is    5 3 3 4 4 0 2 8 4
        Step 4.viii
                B is    6 3 5 0 6 2 0 1 7

Round #4
        Step 4.i
                m is <9>
                W is         F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 220, 0, 0, 0, 0, 0, 0, 0, 0, 42,
85, 183, 56 ]
        Step 4.iii
                S is         7F049BD4 2B5A4CCF 37785442 11794345
        Step 4.iv
                y is  16883588523539449567066181354001906157 3
        Step 4.v
                c is  501105908
```

```
        Step 4.vi
                C is    8 0 9 5 0 1 1 0 5
        Step 4.vii
                A is    6 3 5 0 6 2 0 1 7
        Step 4.viii
                B is    8 0 9 5 0 1 1 0 5

Round #5
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 151, 0, 0, 0, 0, 0, 0, 0, 0,
29, 222, 68, 244 ]
        Step 4.iii
                S is        38217D7E CE328B7A 939A76E8 A585B1E2
        Step 4.iv
                y is  74610658908050888434721887648372601314
        Step 4.v
                c is  82861850
        Step 4.vi
                C is    0 5 8 1 6 8 2 8 0
        Step 4.vii
                A is    8 0 9 5 0 1 1 0 5
        Step 4.viii
                B is    0 5 8 1 6 8 2 8 0

Round #6
        Step 4.i
                m is <9>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 222, 0, 0, 0, 0, 0, 0, 0, 0, 4,
240, 95, 26 ]
        Step 4.iii
                S is        8F6DFF1E 2E5D7CB8 B38A59F4 92D57C69
        Step 4.iv
                y is  190650738160466402174230538935067835497
        Step 4.v
                c is  568941405
        Step 4.vi
                C is    5 0 4 1 4 9 8 6 5
        Step 4.vii
                A is    0 5 8 1 6 8 2 8 0
        Step 4.viii
                B is    5 0 4 1 4 9 8 6 5

Round #7
        Step 4.i
                m is <9>
```

```
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 149, 0, 0, 0, 0, 0, 0, 0, 0,
33, 233, 91, 93 ]
        Step 4.iii
                S is        392D7C8E 411024A9 F95E273D 1EAAA7A1
        Step 4.iv
                y is  760021754077002434236326205179587890 25
        Step 4.v
                c is  41650875
        Step 4.vi
                C is    5 7 8 0 5 6 1 4 0
        Step 4.vii
                A is    5 0 4 1 4 9 8 6 5
        Step 4.viii
                B is    5 7 8 0 5 6 1 4 0
Step 5
        A || B is    5 0 4 1 4 9 8 6 5 5 7 8 0 5 6 1 4 0

CT is 504149865578056140
--------------------------------------------------------------

FF3.Decrypt()

X is    5 0 4 1 4 9 8 6 5 5 7 8 0 5 6 1 4 0
Tweak is 9A 76 8A 92 F6 0E 12 D8

Step 1
        u is <9>, and v is <9>
Step 2
        A is    5 0 4 1 4 9 8 6 5
        B is    5 7 8 0 5 6 1 4 0
Step 3
        T_L is      9A768A92
        T_R is      F60E12D8

Round #7
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 149, 0, 0, 0, 0, 0, 0, 0, 0,
33, 233, 91, 93 ]
        Step 4.iii
                S is        392D7C8E 411024A9 F95E273D 1EAAA7A1
        Step 4.iv
                y is  760021754077002434236326205179587890 25
        Step 4.v
                c is  82861850
        Step 4.vi
```

```
                C is    0 5 8 1 6 8 2 8 0
        Step 4.vii
                B is    5 0 4 1 4 9 8 6 5
        Step 4.viii
                A is    0 5 8 1 6 8 2 8 0

Round #6
        Step 4.i
                m is <9>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 222, 0, 0, 0, 0, 0, 0, 0, 0, 4,
240, 95, 26 ]
        Step 4.iii
                S is        8F6DFF1E 2E5D7CB8 B38A59F4 92D57C69
        Step 4.iv
                y is  190650738160466402174230538935067835497
        Step 4.v
                c is  501105908
        Step 4.vi
                C is    8 0 9 5 0 1 1 0 5
        Step 4.vii
                B is    0 5 8 1 6 8 2 8 0
        Step 4.viii
                A is    8 0 9 5 0 1 1 0 5

Round #5
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 151, 0, 0, 0, 0, 0, 0, 0, 0,
29, 222, 68, 244 ]
        Step 4.iii
                S is        38217D7E CE328B7A 939A76E8 A585B1E2
        Step 4.iv
                y is  746106589080508884347218876483726013l4
        Step 4.v
                c is  710260536
        Step 4.vi
                C is    6 3 5 0 6 2 0 1 7
        Step 4.vii
                B is    8 0 9 5 0 1 1 0 5
        Step 4.viii
                A is    6 3 5 0 6 2 0 1 7

Round #4
        Step 4.i
                m is <9>
                W is        F60E12D8
```

```
        Step 4.ii
                P is  [ 246, 14, 18, 220, 0, 0, 0, 0, 0, 0, 0, 0, 42,
85, 183, 56 ]
        Step 4.iii
                S is         7F049BD4 2B5A4CCF 37785442 11794345
        Step 4.iv
                y is  168835885235394495670661813540019061573
        Step 4.v
                c is  482044335
        Step 4.vi
                C is    5 3 3 4 4 0 2 8 4
        Step 4.vii
                B is    6 3 5 0 6 2 0 1 7
        Step 4.viii
                A is    5 3 3 4 4 0 2 8 4

Round #3
        Step 4.i
                m is <9>
                W is         9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 145, 0, 0, 0, 0, 0, 0, 0, 0,
28, 187, 105, 175 ]
        Step 4.iii
                S is         784896F6 DE0EBF2A 93E57E84 C6DA81F4
        Step 4.iv
                y is  159884266788296438496533435534213284340
        Step 4.v
                c is  496976196
        Step 4.vi
                C is    6 9 1 6 7 9 6 9 4
        Step 4.vii
                B is    5 3 3 4 4 0 2 8 4
        Step 4.viii
                A is    6 9 1 6 7 9 6 9 4

Round #2
        Step 4.i
                m is <9>
                W is         F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 218, 0, 0, 0, 0, 0, 0, 0, 0, 29,
159, 65, 68 ]
        Step 4.iii
                S is         D1D1AE87 F70BEC81 CD4BA39A 31B1197F
        Step 4.iv
                y is  27889738107401138371039892420598386521 5
        Step 4.v
                c is  498179120
        Step 4.vi
```

```
                C is    0 2 1 9 7 1 8 9 4
        Step 4.vii
                B is    6 9 1 6 7 9 6 9 4
        Step 4.viii
                A is    0 2 1 9 7 1 8 9 4

Round #1
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 147, 0, 0, 0, 0, 0, 0, 0, 0,
29, 177, 156, 48 ]
        Step 4.iii
                S is        02F7D2B5 801AD3E3 B28A8FCE 53E9C777
        Step 4.iv
                y is  394522700158863005073497285249687743l
        Step 4.v
                c is  98765
        Step 4.vi
                C is    5 6 7 8 9 0 0 0 0
        Step 4.vii
                B is    0 2 1 9 7 1 8 9 4
        Step 4.viii
                A is    5 6 7 8 9 0 0 0 0

Round #0
        Step 4.i
                m is <9>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 216, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 129, 205 ]
        Step 4.iii
                S is        F89ADB25 F087FAEA 471670EC A1EAA126
        Step 4.iv
                y is  330452601524459504934593210673066058022
        Step 4.v
                c is  432121098
        Step 4.vi
                C is    8 9 0 1 2 1 2 3 4
        Step 4.vii
                B is    5 6 7 8 9 0 0 0 0
        Step 4.viii
                A is    8 9 0 1 2 1 2 3 4
Step 5
        A || B is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0

PTout is <890121234567890000>
============================================================
```

Sample #13

FF3-AES256

Key is EF 43 59 D8 D5 80 AA 4F 7F 03 6D 6F 04 FC 6A 94 2B 7E 15 16 28
AE D2 A6 AB F7 15 88 09 CF 4F 3C
Radix = 10
---

PT is <8901212345678900000789000000>

FF3.Encrypt()

X is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0 0 0 7 8 9 0 0 0 0 0 0
Tweak is D8 E7 92 0A FA 33 0A 73

Step 1
        u is <15>, and v is <14>
Step 2
        A is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0
        B is    0 0 0 0 0 7 8 9 0 0 0 0 0 0 0
Step 3
        T_L is      D8E7920A
        T_R is      FA330A73

Round #0
        Step 4.i
                m is <15>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 115, 0, 0, 0, 0, 0, 0, 0, 0, 5,
226, 10, 224 ]
        Step 4.iii
                S is        1CA0A131 ACE24F6F AF919128 EFBBC451
        Step 4.iv
                y is  380524207829743820314583240227807406 89
        Step 4.v
                c is  422788212861787
        Step 4.vi
                C is    7 8 7 1 6 8 2 1 2 8 8 7 2 2 4
        Step 4.vii
                A is    0 0 0 0 0 7 8 9 0 0 0 0 0 0 0
        Step 4.viii
                B is    7 8 7 1 6 8 2 1 2 8 8 7 2 2 4

Round #1
        Step 4.i
                m is <14>

```
                W is         D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 11, 0, 0, 0, 0, 0, 1, 128,
134, 13, 62, 43, 91 ]
        Step 4.iii
                S is         E17D2D2B A38BE048 76E0AF58 3FBD8C8B
        Step 4.iv
                y is  29972625232478123373208794980278688474 7
        Step 4.v
                c is  49802885584747
        Step 4.vi
                C is    7 4 7 4 8 5 5 8 8 2 0 8 9 4
        Step 4.vii
                A is    7 8 7 1 6 8 2 1 2 8 8 7 2 2 4
        Step 4.viii
                B is    7 4 7 4 8 5 5 8 8 2 0 8 9 4

Round #2
        Step 4.i
                m is <15>
                W is         FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 113, 0, 0, 0, 0, 0, 0, 45, 75,
163, 77, 215, 107 ]
        Step 4.iii
                S is         5CFEBDC9 AA4E62B5 709B020F 40D2280C
        Step 4.iv
                y is  123611668367263076080087660689913686028
        Step 4.v
                c is  83478126547815
        Step 4.vi
                C is    5 1 8 7 4 5 6 2 1 8 7 4 3 8 0
        Step 4.vii
                A is    7 4 7 4 8 5 5 8 8 2 0 8 9 4
        Step 4.viii
                B is    5 1 8 7 4 5 6 2 1 8 7 4 3 8 0

Round #3
        Step 4.i
                m is <14>
                W is         D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 9, 0, 0, 0, 0, 0, 0, 75, 236,
68, 20, 83, 103 ]
        Step 4.iii
                S is         9E45C8E5 F94B3ED5 3B2937F8 C77F84EA
        Step 4.iv
                y is  21038036651957829072791566312546497457 0
        Step 4.v
                c is  12928350559317
```

```
        Step 4.vi
                C is    7 1 3 9 5 5 0 5 3 8 2 9 2 1
        Step 4.vii
                A is    5 1 8 7 4 5 6 2 1 8 7 4 3 8 0
        Step 4.viii
                B is    7 1 3 9 5 5 0 5 3 8 2 9 2 1

Round #4
        Step 4.i
                m is <15>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 119, 0, 0, 0, 0, 0, 0, 11, 194,
29, 190, 28, 85 ]
        Step 4.iii
                S is        636AF5DB BD32920F DED869B6 6A78785F
        Step 4.iv
                y is  1321489416495856513347252418664857908l5
        Step 4.v
                c is  325344612338630
        Step 4.vi
                C is    0 3 6 8 3 3 2 1 6 4 4 3 5 2 3
        Step 4.vii
                A is    7 1 3 9 5 5 0 5 3 8 2 9 2 1
        Step 4.viii
                B is    0 3 6 8 3 3 2 1 6 4 4 3 5 2 3

Round #5
        Step 4.i
                m is <14>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 15, 0, 0, 0, 0, 0, 1, 39, 230,
50, 12, 75, 198 ]
        Step 4.iii
                S is        2D2513E1 4D44F96C 5D5B9CD7 2B2BF026
        Step 4.iv
                y is  600077780101197685743480621163020247l2
        Step 4.v
                c is  75044652584059
        Step 4.vi
                C is    9 5 0 4 8 5 2 5 6 4 4 0 5 7
        Step 4.vii
                A is    0 3 6 8 3 3 2 1 6 4 4 3 5 2 3
        Step 4.viii
                B is    9 5 0 4 8 5 2 5 6 4 4 0 5 7

Round #6
        Step 4.i
                m is <15>
```

```
                W is         FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 117, 0, 0, 0, 0, 0, 0, 68, 64,
177, 220, 12, 123 ]
        Step 4.iii
                S is         A5825F89 AD211F0C 60395A13 20303DCE
        Step 4.iv
                y is  219999555632872205856537204408622005710
        Step 4.v
                c is  529753234344340
        Step 4.vi
                C is    0 4 3 4 4 3 4 3 2 3 5 7 9 2 5
        Step 4.vii
                A is    9 5 0 4 8 5 2 5 6 4 4 0 5 7
        Step 4.viii
                B is    0 4 3 4 4 3 4 3 2 3 5 7 9 2 5

Round #7
        Step 4.i
                m is <14>
                W is         D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 13, 0, 0, 0, 0, 0, 1, 225,
206, 201, 90, 9, 148 ]
        Step 4.iii
                S is         BFC08DC8 6A6EA6C2 0644E02C 3AA1A02C
        Step 4.iv
                y is  254882343890083416740878724577991172140
        Step 4.v
                c is  99622643756199
        Step 4.vi
                C is    9 9 1 6 5 7 3 4 6 2 2 6 9 9
        Step 4.vii
                A is    0 4 3 4 4 3 4 3 2 3 5 7 9 2 5
        Step 4.viii
                B is    9 9 1 6 5 7 3 4 6 2 2 6 9 9
Step 5
        A || B is    0 4 3 4 4 3 4 3 2 3 5 7 9 2 5 9 9 1 6 5 7 3 4 6 2
2 6 9 9

CT is 043443432357925991657346226 99
----------------------------------------------------------

FF3.Decrypt()

X is    0 4 3 4 4 3 4 3 2 3 5 7 9 2 5 9 9 1 6 5 7 3 4 6 2 2 6 9 9
Tweak is D8 E7 92 0A FA 33 0A 73

Step 1
        u is <15>, and v is <14>
```

```
Step 2
        A is    0 4 3 4 4 3 4 3 2 3 5 7 9 2 5
        B is    9 9 1 6 5 7 3 4 6 2 2 6 9 9
Step 3
        T_L is      D8E7920A
        T_R is      FA330A73

Round #7
        Step 4.i
                m is <14>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 13, 0, 0, 0, 0, 0, 1, 225,
206, 201, 90, 9, 148 ]
        Step 4.iii
                S is        BFC08DC8 6A6EA6C2 0644E02C 3AA1A02C
        Step 4.iv
                y is  254882343890083416740878724577991172140
        Step 4.v
                c is  75044652584059
        Step 4.vi
                C is    9 5 0 4 8 5 2 5 6 4 4 0 5 7
        Step 4.vii
                B is    0 4 3 4 4 3 4 3 2 3 5 7 9 2 5
        Step 4.viii
                A is    9 5 0 4 8 5 2 5 6 4 4 0 5 7

Round #6
        Step 4.i
                m is <15>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 117, 0, 0, 0, 0, 0, 0, 68, 64,
177, 220, 12, 123 ]
        Step 4.iii
                S is        A5825F89 AD211F0C 60395A13 20303DCE
        Step 4.iv
                y is  219995555632872205856537204408622005710
        Step 4.v
                c is  325344612338630
        Step 4.vi
                C is    0 3 6 8 3 3 2 1 6 4 4 3 5 2 3
        Step 4.vii
                B is    9 5 0 4 8 5 2 5 6 4 4 0 5 7
        Step 4.viii
                A is    0 3 6 8 3 3 2 1 6 4 4 3 5 2 3

Round #5
        Step 4.i
                m is <14>
```

```
                W is         D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 15, 0, 0, 0, 0, 0, 1, 39, 230,
50, 12, 75, 198 ]
        Step 4.iii
                S is         2D2513E1 4D44F96C 5D5B9CD7 2B2BF026
        Step 4.iv
                y is  60007778010119768574348062116302024742
        Step 4.v
                c is  12928350559317
        Step 4.vi
                C is    7 1 3 9 5 5 0 5 3 8 2 9 2 1
        Step 4.vii
                B is    0 3 6 8 3 3 2 1 6 4 4 3 5 2 3
        Step 4.viii
                A is    7 1 3 9 5 5 0 5 3 8 2 9 2 1

Round #4
        Step 4.i
                m is <15>
                W is         FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 119, 0, 0, 0, 0, 0, 0, 11, 194,
29, 190, 28, 85 ]
        Step 4.iii
                S is         636AF5DB BD32920F DED869B6 6A78785F
        Step 4.iv
                y is  13214894164958565133472524186648579081 5
        Step 4.v
                c is  83478126547815
        Step 4.vi
                C is    5 1 8 7 4 5 6 2 1 8 7 4 3 8 0
        Step 4.vii
                B is    7 1 3 9 5 5 0 5 3 8 2 9 2 1
        Step 4.viii
                A is    5 1 8 7 4 5 6 2 1 8 7 4 3 8 0

Round #3
        Step 4.i
                m is <14>
                W is         D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 9, 0, 0, 0, 0, 0, 0, 75, 236,
68, 20, 83, 103 ]
        Step 4.iii
                S is         9E45C8E5 F94B3ED5 3B2937F8 C77F84EA
        Step 4.iv
                y is  21038036651957829072791566312546497457 0
        Step 4.v
                c is  49802885584747
```

```
        Step 4.vi
                C is    7 4 7 4 8 5 5 8 8 2 0 8 9 4
        Step 4.vii
                B is    5 1 8 7 4 5 6 2 1 8 7 4 3 8 0
        Step 4.viii
                A is    7 4 7 4 8 5 5 8 8 2 0 8 9 4

Round #2
        Step 4.i
                m is <15>
                W is        FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 113, 0, 0, 0, 0, 0, 0, 45, 75,
163, 77, 215, 107 ]
        Step 4.iii
                S is        5CFEBDC9 AA4E62B5 709B020F 40D2280C
        Step 4.iv
                y is  123611668367263076080087660689913686028
        Step 4.v
                c is  422788212861787
        Step 4.vi
                C is    7 8 7 1 6 8 2 1 2 8 8 7 2 2 4
        Step 4.vii
                B is    7 4 7 4 8 5 5 8 8 2 0 8 9 4
        Step 4.viii
                A is    7 8 7 1 6 8 2 1 2 8 8 7 2 2 4

Round #1
        Step 4.i
                m is <14>
                W is        D8E7920A
        Step 4.ii
                P is  [ 216, 231, 146, 11, 0, 0, 0, 0, 0, 1, 128,
134, 13, 62, 43, 91 ]
        Step 4.iii
                S is        E17D2D2B A38BE048 76E0AF58 3FBD8C8B
        Step 4.iv
                y is  299726252324781233732087949802786884747
        Step 4.v
                c is  98700000
        Step 4.vi
                C is    0 0 0 0 0 7 8 9 0 0 0 0 0 0
        Step 4.vii
                B is    7 8 7 1 6 8 2 1 2 8 8 7 2 2 4
        Step 4.viii
                A is    0 0 0 0 0 7 8 9 0 0 0 0 0 0

Round #0
        Step 4.i
                m is <15>
```

```
                W is         FA330A73
        Step 4.ii
                P is  [ 250, 51, 10, 115, 0, 0, 0, 0, 0, 0, 0, 0, 5,
226, 10, 224 ]
        Step 4.iii
                S is         1CA0A131 ACE24F6F AF919128 EFBBC451
        Step 4.iv
                y is  380524207829743820314583240227807406 89
        Step 4.v
                c is  98765432121098
        Step 4.vi
                C is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0
        Step 4.vii
                B is    0 0 0 0 0 7 8 9 0 0 0 0 0 0
        Step 4.viii
                A is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0
Step 5
        A || B is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0 0 0 7 8 9 0 0
0 0 0 0

PTout is <8901212345678900000789000000>
============================================================

Sample #14

FF3-AES256

Key is EF 43 59 D8 D5 80 AA 4F 7F 03 6D 6F 04 FC 6A 94 2B 7E 15 16 28
AE D2 A6 AB F7 15 88 09 CF 4F 3C
Radix = 10
------------------------------------------------------------


PT is <8901212345678900000789000000>

FF3.Encrypt()

X is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0 0 0 7 8 9 0 0 0 0 0 0
Tweak is 00 00 00 00 00 00 00 00

Step 1
        u is <15>, and v is <14>
Step 2
        A is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0
        B is    0 0 0 0 0 7 8 9 0 0 0 0 0 0
Step 3
        T_L is      00000000
        T_R is      00000000

Round #0
```

```
        Step 4.i
                m is <15>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 226,
10, 224 ]
        Step 4.iii
                S is         3089AAF8 05E8802E DF3F0E34 95E389BD
        Step 4.iv
                y is  64517756127340658772823157152566970813
        Step 4.v
                c is  255917999091911
        Step 4.vi
                C is    1 1 9 1 9 0 9 9 9 7 1 9 5 5 2
        Step 4.vii
                A is    0 0 0 0 0 7 8 9 0 0 0 0 0 0 0
        Step 4.viii
                B is    1 1 9 1 9 0 9 9 9 7 1 9 5 5 2

Round #1
        Step 4.i
                m is <14>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 232, 193, 141,
109, 112, 199 ]
        Step 4.iii
                S is         E291B8FC 72BF8948 B28219E0 1E12E1C7
        Step 4.iv
                y is  30116216205625540704078472784997429293 5
        Step 4.v
                c is  27850072992935
        Step 4.vi
                C is    5 3 9 2 9 9 2 7 0 0 5 8 7 2
        Step 4.vii
                A is    1 1 9 1 9 0 9 9 9 7 1 9 5 5 2
        Step 4.viii
                B is    5 3 9 2 9 9 2 7 0 0 5 8 7 2

Round #2
        Step 4.i
                m is <15>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 25, 84, 89,
181, 44, 167 ]
        Step 4.iii
                S is         A54C85BA 15900F03 9DB9B0FA 57FFAC39
        Step 4.iv
                y is  21971994616934862068070519808496918 0217
```

```
        Step 4.v
                c is  454002968272128
        Step 4.vi
                C is    8 2 1 2 7 2 8 6 9 2 0 0 4 5 4
        Step 4.vii
                A is    5 3 9 2 9 9 2 7 0 0 5 8 7 2
        Step 4.viii
                B is    8 2 1 2 7 2 8 6 9 2 0 0 4 5 4

Round #3
        Step 4.i
                m is <14>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 3, 0, 0, 0, 0, 0, 1, 156, 233, 205,
166, 157, 0 ]
        Step 4.iii
                S is         09FA0B23 9752F4F7 F40F35EE 46AD8634
        Step 4.iv
                y is  132613521030218031624788125554991119 88
        Step 4.v
                c is  40405572104923
        Step 4.vi
                C is    3 2 9 4 0 1 2 7 5 5 0 4 0 4
        Step 4.vii
                A is    8 2 1 2 7 2 8 6 9 2 0 0 4 5 4
        Step 4.viii
                B is    3 2 9 4 0 1 2 7 5 5 0 4 0 4

Round #4
        Step 4.i
                m is <15>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 36, 191, 167,
197, 178, 219 ]
        Step 4.iii
                S is         86016AB1 7AC8AD4A 141A7AD1 AA9858B9
        Step 4.iv
                y is  178123907728839788596627596433386133689
        Step 4.v
                c is  50436354405817
        Step 4.vi
                C is    7 1 8 5 0 4 4 5 3 6 3 4 0 5 0
        Step 4.vii
                A is    3 2 9 4 0 1 2 7 5 5 0 4 0 4
        Step 4.viii
                B is    7 1 8 5 0 4 4 5 3 6 3 4 0 5 0

Round #5
```

```
        Step 4.i
                m is <14>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 5, 0, 0, 0, 0, 0, 0, 45, 223, 32,
252, 245, 185 ]
        Step 4.iii
                S is         5F988400 BF92CC5C 0C07E28D 902C4B77
        Step 4.iv
                y is  127068566059421088852164781931615767415
        Step 4.v
                c is  22337187872338
        Step 4.vi
                C is    8 3 3 2 7 8 7 8 1 7 3 3 2 2
        Step 4.vii
                A is    7 1 8 5 0 4 4 5 3 6 3 4 0 5 0
        Step 4.viii
                B is    8 3 3 2 7 8 7 8 1 7 3 3 2 2

Round #6
        Step 4.i
                m is <15>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 6, 0, 0, 0, 0, 0, 0, 20, 80, 200,
37, 254, 82 ]
        Step 4.iii
                S is         617066EA E6D1776E 9ECD6EDB D1AC4E02
        Step 4.iv
                y is  129518740255897122931707996963638889986
        Step 4.v
                c is  47399993295803
        Step 4.vi
                C is    3 0 8 5 9 2 3 9 9 9 9 3 7 4 0
        Step 4.vii
                A is    8 3 3 2 7 8 7 8 1 7 3 3 2 2
        Step 4.viii
                B is    3 0 8 5 9 2 3 9 9 9 9 3 7 4 0

Round #7
        Step 4.i
                m is <14>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 7, 0, 0, 0, 0, 0, 0, 43, 28, 43,
195, 67, 187 ]
        Step 4.iii
                S is         6F6EA064 EBF91FEC 61669AAF 55DD2B49
        Step 4.iv
                y is  148118713367947479216073700518368455497
```

```
        Step 4.v
                c is  22855556327835
        Step 4.vi
                C is    5 3 8 7 2 3 6 5 5 5 5 8 2 2
        Step 4.vii
                A is    3 0 8 5 9 2 3 9 9 9 9 3 7 4 0
        Step 4.viii
                B is    5 3 8 7 2 3 6 5 5 5 5 8 2 2
Step 5
        A || B is    3 0 8 5 9 2 3 9 9 9 9 3 7 4 0 5 3 8 7 2 3 6 5 5 5
5 8 2 2

CT is 308592399993740538723655555822
--------------------------------------------------------------

FF3.Decrypt()

X is    3 0 8 5 9 2 3 9 9 9 9 3 7 4 0 5 3 8 7 2 3 6 5 5 5 5 8 2 2
Tweak is 00 00 00 00 00 00 00 00

Step 1
        u is <15>, and v is <14>
Step 2
        A is    3 0 8 5 9 2 3 9 9 9 9 3 7 4 0
        B is    5 3 8 7 2 3 6 5 5 5 5 8 2 2
Step 3
        T_L is      00000000
        T_R is      00000000

Round #7
        Step 4.i
                m is <14>
                W is        00000000
        Step 4.ii
                P is  [ 0, 0, 0, 7, 0, 0, 0, 0, 0, 0, 43, 28, 43,
195, 67, 187 ]
        Step 4.iii
                S is        6F6EA064 EBF91FEC 61669AAF 55DD2B49
        Step 4.iv
                y is  148118713367947479216073700518368455497
        Step 4.v
                c is  22337187872338
        Step 4.vi
                C is    8 3 3 2 7 8 7 8 1 7 3 3 2 2
        Step 4.vii
                B is    3 0 8 5 9 2 3 9 9 9 9 3 7 4 0
        Step 4.viii
                A is    8 3 3 2 7 8 7 8 1 7 3 3 2 2

Round #6
```

```
        Step 4.i
                m is <15>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 6, 0, 0, 0, 0, 0, 0, 20, 80, 200,
37, 254, 82 ]
        Step 4.iii
                S is         617066EA E6D1776E 9ECD6EDB D1AC4E02
        Step 4.iv
                y is  129518740255897122931707996963638889986
        Step 4.v
                c is  50436354405817
        Step 4.vi
                C is    7 1 8 5 0 4 4 5 3 6 3 4 0 5 0
        Step 4.vii
                B is    8 3 3 2 7 8 7 8 1 7 3 3 2 2
        Step 4.viii
                A is    7 1 8 5 0 4 4 5 3 6 3 4 0 5 0

Round #5
        Step 4.i
                m is <14>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 5, 0, 0, 0, 0, 0, 0, 45, 223, 32,
252, 245, 185 ]
        Step 4.iii
                S is         5F988400 BF92CC5C 0C07E28D 902C4B77
        Step 4.iv
                y is  127068566059421088852164781931615767415
        Step 4.v
                c is  40405572104923
        Step 4.vi
                C is    3 2 9 4 0 1 2 7 5 5 0 4 0 4
        Step 4.vii
                B is    7 1 8 5 0 4 4 5 3 6 3 4 0 5 0
        Step 4.viii
                A is    3 2 9 4 0 1 2 7 5 5 0 4 0 4

Round #4
        Step 4.i
                m is <15>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 36, 191, 167,
197, 178, 219 ]
        Step 4.iii
                S is         86016AB1 7AC8AD4A 141A7AD1 AA9858B9
        Step 4.iv
                y is  178123907728839788596627596433386133689
```

```
        Step 4.v
                c is  454002968272128
        Step 4.vi
                C is    8 2 1 2 7 2 8 6 9 2 0 0 4 5 4
        Step 4.vii
                B is    3 2 9 4 0 1 2 7 5 5 0 4 0 4
        Step 4.viii
                A is    8 2 1 2 7 2 8 6 9 2 0 0 4 5 4

Round #3
        Step 4.i
                m is <14>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 3, 0, 0, 0, 0, 0, 1, 156, 233, 205,
166, 157, 0 ]
        Step 4.iii
                S is         09FA0B23 9752F4F7 F40F35EE 46AD8634
        Step 4.iv
                y is  132613521030218031624788125554991119 88
        Step 4.v
                c is  27850072992935
        Step 4.vi
                C is    5 3 9 2 9 9 2 7 0 0 5 8 7 2
        Step 4.vii
                B is    8 2 1 2 7 2 8 6 9 2 0 0 4 5 4
        Step 4.viii
                A is    5 3 9 2 9 9 2 7 0 0 5 8 7 2

Round #2
        Step 4.i
                m is <15>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 25, 84, 89,
181, 44, 167 ]
        Step 4.iii
                S is         A54C85BA 15900F03 9DB9B0FA 57FFAC39
        Step 4.iv
                y is  219719946169348620680705198084969180217
        Step 4.v
                c is  255917999091911
        Step 4.vi
                C is    1 1 9 1 9 0 9 9 9 7 1 9 5 5 2
        Step 4.vii
                B is    5 3 9 2 9 9 2 7 0 0 5 8 7 2
        Step 4.viii
                A is    1 1 9 1 9 0 9 9 9 7 1 9 5 5 2

Round #1
```

```
        Step 4.i
                m is <14>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 232, 193, 141,
109, 112, 199 ]
        Step 4.iii
                S is         E291B8FC 72BF8948 B28219E0 1E12E1C7
        Step 4.iv
                y is  301162162056255407040784727849974292935
        Step 4.v
                c is  98700000
        Step 4.vi
                C is    0 0 0 0 0 7 8 9 0 0 0 0 0 0 0
        Step 4.vii
                B is    1 1 9 1 9 0 9 9 9 7 1 9 5 5 2
        Step 4.viii
                A is    0 0 0 0 0 7 8 9 0 0 0 0 0 0 0

Round #0
        Step 4.i
                m is <15>
                W is         00000000
        Step 4.ii
                P is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 226,
10, 224 ]
        Step 4.iii
                S is         3089AAF8 05E8802E DF3F0E34 95E389BD
        Step 4.iv
                y is  645177561273406587728231571525669708l3
        Step 4.v
                c is  98765432121098
        Step 4.vi
                C is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0
        Step 4.vii
                B is    0 0 0 0 0 7 8 9 0 0 0 0 0 0 0
        Step 4.viii
                A is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0
Step 5
        A || B is    8 9 0 1 2 1 2 3 4 5 6 7 8 9 0 0 0 0 0 0 7 8 9 0 0
0 0 0 0

PTout is <8901212345678900000789000000>
============================================================

Sample #15

FF3-AES256

Key is EF 43 59 D8 D5 80 AA 4F 7F 03 6D 6F 04 FC 6A 94 2B 7E 15 16 28
```

```
AE D2 A6 AB F7 15 88 09 CF 4F 3C
Radix = 26
------------------------------------------------------------


PT is <0123456789abcdefghi>

FF3.Encrypt()

X is    0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
Tweak is 9A 76 8A 92 F6 0E 12 D8

Step 1
        u is <10>, and v is <9>
Step 2
        A is    0 1 2 3 4 5 6 7 8 9
        B is    10 11 12 13 14 15 16 17 18
Step 3
        T_L is      9A768A92
        T_R is      F60E12D8

Round #0
        Step 4.i
                m is <10>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 216, 0, 0, 0, 0, 0, 0, 3, 140,
43, 56, 187, 32 ]
        Step 4.iii
                S is        8542984C E5A41E6E 907F6CE5 15B6BBA5
        Step 4.iv
                y is  177133104050727690651736763581255302053
        Step 4.v
                c is  129555143637599
        Step 4.vi
                C is    17 17 5 4 4 16 6 10 22 23
        Step 4.vii
                A is    10 11 12 13 14 15 16 17 18
        Step 4.viii
                B is    17 17 5 4 4 16 6 10 22 23

Round #1
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 147, 0, 0, 0, 0, 0, 0, 117,
212, 104, 80, 186, 95 ]
        Step 4.iii
                S is        329A01CE 96FFE0E0 8BC5F813 D3A2710A
```

```
        Step 4.iv
                y is  67261050155603328199546072631479529738
        Step 4.v
                c is  871754233898
        Step 4.vi
                C is    2 2 19 17 12 25 13 4 4
        Step 4.vii
                A is    17 17 5 4 4 16 6 10 22 23
        Step 4.viii
                B is    2 2 19 17 12 25 13 4 4

Round #2
        Step 4.i
                m is <10>
                W is         F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 218, 0, 0, 0, 0, 0, 0, 0, 202,
248, 153, 248, 42 ]
        Step 4.iii
                S is         A365B038 949BD36A E157F79B 53F72FEE
        Step 4.iv
                y is  21719215948251281171311946513934288075O
        Step 4.v
                c is  83716232153677
        Step 4.vi
                C is    19 25 24 10 20 4 2 23 10 15
        Step 4.vii
                A is    2 2 19 17 12 25 13 4 4
        Step 4.viii
                B is    19 25 24 10 20 4 2 23 10 15

Round #3
        Step 4.i
                m is <9>
                W is         9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 145, 0, 0, 0, 0, 0, 0, 76, 35,
180, 71, 138, 77 ]
        Step 4.iii
                S is         0D19DFC8 E5F3DABA 57A91ECB 5135E0FF
        Step 4.iv
                y is  17414310260808263350393465868716990719
        Step 4.v
                c is  5091042542889
        Step 4.vi
                C is    17 0 2 24 7 9 22 9 24
        Step 4.vii
                A is    19 25 24 10 20 4 2 23 10 15
        Step 4.viii
                B is    17 0 2 24 7 9 22 9 24
```

```
Round #4
        Step 4.i
                m is <10>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 220, 0, 0, 0, 0, 0, 0, 4, 161,
89, 200, 69, 41 ]
        Step 4.iii
                S is        BBB75B2A 9FB414C7 0F9754A2 3485781F
        Step 4.iv
                y is  249517674613173720918623446156871825439
        Step 4.v
                c is  28684272725612
        Step 4.vi
                C is    10 25 6 14 11 17 8 9 7 5
        Step 4.vii
                A is    17 0 2 24 7 9 22 9 24
        Step 4.viii
                B is    10 25 6 14 11 17 8 9 7 5

Round #5
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 151, 0, 0, 0, 0, 0, 0, 26, 22,
147, 226, 238, 108 ]
        Step 4.iii
                S is        38E572DD 32907DE8 08DF77B6 13140F67
        Step 4.iv
                y is  756281334643274267375797223346124921 35
        Step 4.v
                c is  1202313115280
        Step 4.vi
                C is    4 4 21 6 2 1 18 19 5
        Step 4.vii
                A is    10 25 6 14 11 17 8 9 7 5
        Step 4.viii
                B is    4 4 21 6 2 1 18 19 5

Round #6
        Step 4.i
                m is <10>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 222, 0, 0, 0, 0, 0, 0, 1, 23,
239, 114, 54, 144 ]
        Step 4.iii
                S is        1A13CF4B EE19F652 49F4D696 AE7091C9
```

```
        Step 4.iv
                y is  346627860053089375891315518588741595 61
        Step 4.v
                c is  58387536581685
        Step 4.vi
                C is    25 0 11 2 16 24 13 15 19 10
        Step 4.vii
                A is    4 4 21 6 2 1 18 19 5
        Step 4.viii
                B is    25 0 11 2 16 24 13 15 19 10

Round #7
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 149, 0, 0, 0, 0, 0, 0, 53, 26,
104, 96, 148, 53 ]
        Step 4.iii
                S is        8B19B4C7 14626C7E A8C1266E 20BB5083
        Step 4.iv
                y is  184896165442008361942401016373693862019
        Step 4.v
                c is  1701024361747
        Step 4.vi
                C is    9 11 17 11 7 11 20 3 8
        Step 4.vii
                A is    25 0 11 2 16 24 13 15 19 10
        Step 4.viii
                B is    9 11 17 11 7 11 20 3 8
Step 5
        A || B is    25 0 11 2 16 24 13 15 19 10 9 11 17 11 7 11 20 3
8

CT is p0b2godfja9bhb7bk38
----------------------------------------------------------------

FF3.Decrypt()

X is    25 0 11 2 16 24 13 15 19 10 9 11 17 11 7 11 20 3 8
Tweak is 9A 76 8A 92 F6 0E 12 D8

Step 1
        u is <10>, and v is <9>
Step 2
        A is    25 0 11 2 16 24 13 15 19 10
        B is    9 11 17 11 7 11 20 3 8
Step 3
        T_L is      9A768A92
        T_R is      F60E12D8
```

```
Round #7
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 149, 0, 0, 0, 0, 0, 0, 53, 26,
104, 96, 148, 53 ]
        Step 4.iii
                S is        8B19B4C7 14626C7E A8C1266E 20BB5083
        Step 4.iv
                y is  184896165442008361942401016373693862019
        Step 4.v
                c is  1202313115280
        Step 4.vi
                C is    4 4 21 6 2 1 18 19 5
        Step 4.vii
                B is    25 0 11 2 16 24 13 15 19 10
        Step 4.viii
                A is    4 4 21 6 2 1 18 19 5

Round #6
        Step 4.i
                m is <10>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 222, 0, 0, 0, 0, 0, 0, 1, 23,
239, 114, 54, 144 ]
        Step 4.iii
                S is        1A13CF4B EE19F652 49F4D696 AE7091C9
        Step 4.iv
                y is  346627860053089375891315518588741595 61
        Step 4.v
                c is  28684272725612
        Step 4.vi
                C is    10 25 6 14 11 17 8 9 7 5
        Step 4.vii
                B is    4 4 21 6 2 1 18 19 5
        Step 4.viii
                A is    10 25 6 14 11 17 8 9 7 5

Round #5
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 151, 0, 0, 0, 0, 0, 0, 26, 22,
147, 226, 238, 108 ]
        Step 4.iii
                S is        38E572DD 32907DE8 08DF77B6 13140F67
```

```
        Step 4.iv
                y is  756281334643274267375797223346124921 35
        Step 4.v
                c is  5091042542889
        Step 4.vi
                C is    17 0 2 24 7 9 22 9 24
        Step 4.vii
                B is    10 25 6 14 11 17 8 9 7 5
        Step 4.viii
                A is    17 0 2 24 7 9 22 9 24

Round #4
        Step 4.i
                m is <10>
                W is         F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 220, 0, 0, 0, 0, 0, 0, 4, 161,
89, 200, 69, 41 ]
        Step 4.iii
                S is         BBB75B2A 9FB414C7 0F9754A2 3485781F
        Step 4.iv
                y is  249517674613173720918623446156871825439
        Step 4.v
                c is  83716232153677
        Step 4.vi
                C is    19 25 24 10 20 4 2 23 10 15
        Step 4.vii
                B is    17 0 2 24 7 9 22 9 24
        Step 4.viii
                A is    19 25 24 10 20 4 2 23 10 15

Round #3
        Step 4.i
                m is <9>
                W is         9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 145, 0, 0, 0, 0, 0, 0, 76, 35,
180, 71, 138, 77 ]
        Step 4.iii
                S is         0D19DFC8 E5F3DABA 57A91ECB 5135E0FF
        Step 4.iv
                y is  174143102608082633503934658687169907 19
        Step 4.v
                c is  871754233898
        Step 4.vi
                C is    2 2 19 17 12 25 13 4 4
        Step 4.vii
                B is    19 25 24 10 20 4 2 23 10 15
        Step 4.viii
                A is    2 2 19 17 12 25 13 4 4
```

```
Round #2
        Step 4.i
                m is <10>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 218, 0, 0, 0, 0, 0, 0, 0, 202,
248, 153, 248, 42 ]
        Step 4.iii
                S is        A365B038 949BD36A E157F79B 53F72FEE
        Step 4.iv
                y is  217192159482512811713119465139342880750
        Step 4.v
                c is  129555143637599
        Step 4.vi
                C is    17 17 5 4 4 16 6 10 22 23
        Step 4.vii
                B is    2 2 19 17 12 25 13 4 4
        Step 4.viii
                A is    17 17 5 4 4 16 6 10 22 23

Round #1
        Step 4.i
                m is <9>
                W is        9A768A92
        Step 4.ii
                P is  [ 154, 118, 138, 147, 0, 0, 0, 0, 0, 0, 117,
212, 104, 80, 186, 95 ]
        Step 4.iii
                S is        329A01CE 96FFE0E0 8BC5F813 D3A2710A
        Step 4.iv
                y is  67261050155603328199546072631479529738
        Step 4.v
                c is  3900555442976
        Step 4.vi
                C is    10 11 12 13 14 15 16 17 18
        Step 4.vii
                B is    17 17 5 4 4 16 6 10 22 23
        Step 4.viii
                A is    10 11 12 13 14 15 16 17 18

Round #0
        Step 4.i
                m is <10>
                W is        F60E12D8
        Step 4.ii
                P is  [ 246, 14, 18, 216, 0, 0, 0, 0, 0, 0, 3, 140,
43, 56, 187, 32 ]
        Step 4.iii
                S is        8542984C E5A41E6E 907F6CE5 15B6BBA5
```

```
        Step 4.iv
                y is  177133104050727690651736763581255302053
        Step 4.v
                c is  50594287082170
        Step 4.vi
                C is    0 1 2 3 4 5 6 7 8 9
        Step 4.vii
                B is    10 11 12 13 14 15 16 17 18
        Step 4.viii
                A is    0 1 2 3 4 5 6 7 8 9
Step 5
        A || B is    0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18

PTout is <0123456789abcdefghi>
##############################################################
```