```
##########################################################
   SHA-3 Derived Functions
        cSHAKE
        KMAC
        TupleHash
        ParallelHash
##########################################################

TupleHashXOF:
        Sample #1

Security Strength: 128-bits

Number of Tuples: 2

Tuple 1
        00 01 02

Tuple 2
        10 11 12 13 14 15

Requested output length is 256-bits

S (as a character string) is
        "(null)"
--------------------------------------------------------
Encoded X[1]
        01 18 00 01 02
Encoded X[2]
        01 30 10 11 12 13 14 15
Encoded N
        01 48 54 75 70 6C 65 48 61 73 68
Encoded S
        01 00
bytepad data
        01 A8 01 48 54 75 70 6C 65 48 61 73 68 01 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
--------------------------------------------------------
About to Absorb data
State (in bytes)
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
```

Data to be absorbed

```
01 A8 01 48 54 75 70 6C 65 48 61 73 68 01 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
```

Xor'd state (in bytes)

```
01 A8 01 48 54 75 70 6C 65 48 61 73 68 01 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
```

After Permutation

```
19 EE 26 92 79 BC E2 ED EB 0E F8 9E 4B F8 84 AF
DD AD F9 62 00 C6 C4 AC 6D D7 9F BD 11 CF B7 D1
5F 27 0D DA 8A 35 9B 05 48 BE 64 A7 57 D6 FC 33
29 BC 3C FD DE 4B 94 C4 47 E3 9C 9F 28 C9 01 0F
17 69 B5 BA 61 3F 1F 10 AA C6 AD 40 11 C5 7E 48
09 93 74 F9 27 4E C6 6C C0 13 0D D2 50 61 12 66
9B F8 F8 46 36 89 21 E9 5D CE 53 41 13 8E 06 F5
10 3F AB F5 52 8C F0 7C DF CE 8D E8 D9 D4 B4 D0
EE 68 24 9E 17 71 57 90 EB D3 11 52 C9 5C BC 62
D6 B0 E4 95 D2 1A 1A 20 47 42 1F D3 58 BD 45 BE
```

```
        62 72 DD 3B 7D 4B B9 D3 A6 02 8A C6 9F 64 FE B3
        43 1B D3 78 D4 C4 5F 6A 5A 43 58 2A F6 94 FE FF
        CA 44 68 B9 5C 3E F0 9E
about to call last of the absorb phase
----------------------------------------------------------
About to Absorb data
State (in bytes)
        19 EE 26 92 79 BC E2 ED EB 0E F8 9E 4B F8 84 AF
        DD AD F9 62 00 C6 C4 AC 6D D7 9F BD 11 CF B7 D1
        5F 27 0D DA 8A 35 9B 05 48 BE 64 A7 57 D6 FC 33
        29 BC 3C FD DE 4B 94 C4 47 E3 9C 9F 28 C9 01 0F
        17 69 B5 BA 61 3F 1F 10 AA C6 AD 40 11 C5 7E 48
        09 93 74 F9 27 4E C6 6C C0 13 0D D2 50 61 12 66
        9B F8 F8 46 36 89 21 E9 5D CE 53 41 13 8E 06 F5
        10 3F AB F5 52 8C F0 7C DF CE 8D E8 D9 D4 B4 D0
        EE 68 24 9E 17 71 57 90 EB D3 11 52 C9 5C BC 62
        D6 B0 E4 95 D2 1A 1A 20 47 42 1F D3 58 BD 45 BE
        62 72 DD 3B 7D 4B B9 D3 A6 02 8A C6 9F 64 FE B3
        43 1B D3 78 D4 C4 5F 6A 5A 43 58 2A F6 94 FE FF
        CA 44 68 B9 5C 3E F0 9E
Data to be absorbed
        01 18 00 01 02 01 30 10 11 12 13 14 15 00 01 04
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
Xor'd state (in bytes)
        18 F6 26 93 7B BD D2 FD FA 1C EB 8A 5E F8 85 AB
        DD AD F9 62 00 C6 C4 AC 6D D7 9F BD 11 CF B7 D1
        5F 27 0D DA 8A 35 9B 05 48 BE 64 A7 57 D6 FC 33
        29 BC 3C FD DE 4B 94 C4 47 E3 9C 9F 28 C9 01 0F
        17 69 B5 BA 61 3F 1F 10 AA C6 AD 40 11 C5 7E 48
        09 93 74 F9 27 4E C6 6C C0 13 0D D2 50 61 12 66
        9B F8 F8 46 36 89 21 E9 5D CE 53 41 13 8E 06 F5
        10 3F AB F5 52 8C F0 7C DF CE 8D E8 D9 D4 B4 D0
        EE 68 24 9E 17 71 57 90 EB D3 11 52 C9 5C BC 62
        D6 B0 E4 95 D2 1A 1A 20 47 42 1F D3 58 BD 45 BE
        62 72 DD 3B 7D 4B B9 53 A6 02 8A C6 9F 64 FE B3
        43 1B D3 78 D4 C4 5F 6A 5A 43 58 2A F6 94 FE FF
        CA 44 68 B9 5C 3E F0 9E

After Permutation
        2F 10 3C D7 C3 23 20 35 34 95 C6 8D E1 A8 12 92
```

```
        45 C6 32 5F 6F 2A 3D 60 8D 92 17 9C 96 E6 84 88
        3A FA 64 C0 9E EC 71 C6 36 52 71 56 34 E7 C0 E5
        EF 27 8C 0D E6 62 80 4A 28 4A 9F 7E 84 7F 37 B9
        26 22 D7 EB 55 18 9A 3F 05 47 88 82 7E 82 A8 BC
        E3 6A FC DD 20 5C 2D 6D 0D 4B E0 4F 1D 7F 56 BC
        57 CD D6 EC 30 7B 08 8C D9 76 4E 95 FA C7 76 FA
        1C 2B 1C 09 18 AA D1 C4 16 2E A8 7A B9 7E 52 6D
        24 D1 35 9E 39 4D 21 3A C4 74 6B E4 81 EC F0 1C
        14 08 05 C9 13 BC 5F A5 F0 6E F6 81 67 03 9F A7
        4B C3 BA 90 5F 67 EB 44 06 E4 54 8C 77 24 64 76
        C9 52 FE E0 00 DE DF 5A 30 76 C5 6C 7E A7 B5 AA
        E6 38 D1 DF 85 1B 71 A8
Outval is
        2F 10 3C D7 C3 23 20 35 34 95 C6 8D E1 A8 12 92
        45 C6 32 5F 6F 2A 3D 60 8D 92 17 9C 96 E6 84 88

============================================================

TupleHashXOF:
        Sample #2

Security Strength: 128-bits

Number of Tuples: 2

Tuple 1
        00 01 02

Tuple 2
        10 11 12 13 14 15

Requested output length is 256-bits

S (as a character string) is
        "My Tuple App"
----------------------------------------------------------
Encoded X[1]
        01 18 00 01 02
Encoded X[2]
        01 30 10 11 12 13 14 15
Encoded N
        01 48 54 75 70 6C 65 48 61 73 68
Encoded S
        01 60 4D 79 20 54 75 70 6C 65 20 41 70 70
bytepad data
        01 A8 01 48 54 75 70 6C 65 48 61 73 68 01 60 4D
        79 20 54 75 70 6C 65 20 41 70 70 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00
------------------------------------------------------------
About to Absorb data
State (in bytes)
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00
Data to be absorbed
          01 A8 01 48 54 75 70 6C 65 48 61 73 68 01 60 4D
          79 20 54 75 70 6C 65 20 41 70 70 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00
Xor'd state (in bytes)
          01 A8 01 48 54 75 70 6C 65 48 61 73 68 01 60 4D
          79 20 54 75 70 6C 65 20 41 70 70 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00

After Permutation
```

```
        6F 92 C7 41 FD F3 22 6F A1 AC EB F5 AB D1 81 C3
        AE 04 2B 5E C6 03 92 D3 16 B5 CC F5 6C 1E A4 B1
        16 22 57 38 89 A7 7B BE B1 9D F1 3D 24 89 86 39
        09 E7 EB EF 03 56 8A 96 39 C4 EC 06 A8 9E D4 02
        6E 10 90 83 86 D4 D5 AD B2 00 84 89 36 F6 F2 66
        A6 B0 93 0B 7B D2 52 13 C6 53 42 20 E5 25 92 21
        9F 83 D0 A9 44 0C 70 4A F3 4D 3C 7A 33 B1 91 1D
        51 FB EE 20 1C CC 57 F2 41 BC 2E AE C2 BF D0 A2
        DB A5 0E D4 A9 84 E7 AA C1 B2 B7 E5 1C 93 5A 9E
        7A F8 00 93 5B 6F FA 0E 8A DE 7B EA C7 11 29 AF
        BE C3 40 47 B1 8D CA 84 D3 47 9A 47 E7 43 52 36
        7E 9B AE 6C 7C 97 BB 55 54 3F 2F 09 F7 76 FC E8
        05 CC E4 F6 85 3F 2B 17
about to call last of the absorb phase
------------------------------------------------------------
About to Absorb data
State (in bytes)
        6F 92 C7 41 FD F3 22 6F A1 AC EB F5 AB D1 81 C3
        AE 04 2B 5E C6 03 92 D3 16 B5 CC F5 6C 1E A4 B1
        16 22 57 38 89 A7 7B BE B1 9D F1 3D 24 89 86 39
        09 E7 EB EF 03 56 8A 96 39 C4 EC 06 A8 9E D4 02
        6E 10 90 83 86 D4 D5 AD B2 00 84 89 36 F6 F2 66
        A6 B0 93 0B 7B D2 52 13 C6 53 42 20 E5 25 92 21
        9F 83 D0 A9 44 0C 70 4A F3 4D 3C 7A 33 B1 91 1D
        51 FB EE 20 1C CC 57 F2 41 BC 2E AE C2 BF D0 A2
        DB A5 0E D4 A9 84 E7 AA C1 B2 B7 E5 1C 93 5A 9E
        7A F8 00 93 5B 6F FA 0E 8A DE 7B EA C7 11 29 AF
        BE C3 40 47 B1 8D CA 84 D3 47 9A 47 E7 43 52 36
        7E 9B AE 6C 7C 97 BB 55 54 3F 2F 09 F7 76 FC E8
        05 CC E4 F6 85 3F 2B 17
Data to be absorbed
        01 18 00 01 02 01 30 10 11 12 13 14 15 00 01 04
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
Xor'd state (in bytes)
        6E 8A C7 40 FF F2 12 7F B0 BE F8 E1 BE D1 80 C7
        AE 04 2B 5E C6 03 92 D3 16 B5 CC F5 6C 1E A4 B1
        16 22 57 38 89 A7 7B BE B1 9D F1 3D 24 89 86 39
        09 E7 EB EF 03 56 8A 96 39 C4 EC 06 A8 9E D4 02
        6E 10 90 83 86 D4 D5 AD B2 00 84 89 36 F6 F2 66
        A6 B0 93 0B 7B D2 52 13 C6 53 42 20 E5 25 92 21
```

```
        9F 83 D0 A9 44 0C 70 4A F3 4D 3C 7A 33 B1 91 1D
        51 FB EE 20 1C CC 57 F2 41 BC 2E AE C2 BF D0 A2
        DB A5 0E D4 A9 84 E7 AA C1 B2 B7 E5 1C 93 5A 9E
        7A F8 00 93 5B 6F FA 0E 8A DE 7B EA C7 11 29 AF
        BE C3 40 47 B1 8D CA 04 D3 47 9A 47 E7 43 52 36
        7E 9B AE 6C 7C 97 BB 55 54 3F 2F 09 F7 76 FC E8
        05 CC E4 F6 85 3F 2B 17

After Permutation
        3F C8 AD 69 45 31 28 29 28 59 A1 8B 6C 67 D7 AD
        85 F0 1B 32 81 5E 22 CE 83 9C 49 EC 37 4E 9B 9A
        41 3B EA BD 8F 84 CD 94 9C 52 FE 39 47 83 5F FD
        07 D3 55 6F 48 9F 87 82 54 34 9A 0E 07 55 94 34
        3E 5B EF BC 81 FB 96 C5 59 21 59 8B 64 1E A9 08
        42 87 37 40 C0 09 92 CD 6F B4 90 02 4E 14 D2 2D
        55 8E 8D 44 70 0F 1C FD A1 11 D9 02 AE DB 08 8D
        08 17 31 04 11 AB D9 CC 52 C6 70 16 EB 1A 11 02
        D0 8E 49 69 1C 52 07 15 A8 78 24 97 F2 72 AF 96
        8E 00 2D 43 26 61 42 DA 73 00 CB 29 08 E2 11 B2
        CA B5 77 09 46 57 C7 C7 78 63 01 10 E6 EA DF 1F
        5C 74 A1 44 85 DB 28 CC 7E F3 2D CF 8F 1E 10 7A
        4A FC 82 80 A0 90 E1 2E
Outval is
        3F C8 AD 69 45 31 28 29 28 59 A1 8B 6C 67 D7 AD
        85 F0 1B 32 81 5E 22 CE 83 9C 49 EC 37 4E 9B 9A

=================================================================

TupleHashXOF:
        Sample #3

Security Strength: 128-bits

Number of Tuples: 3

Tuple 1
        00 01 02

Tuple 2
        10 11 12 13 14 15

Tuple 3
        20 21 22 23 24 25 26 27 28

Requested output length is 256-bits

S (as a character string) is
        "My Tuple App"
----------------------------------------------------------------
Encoded X[1]
        01 18 00 01 02
```

```
Encoded X[2]
        01 30 10 11 12 13 14 15
Encoded X[3]
        01 48 20 21 22 23 24 25 26 27 28
Encoded N
        01 48 54 75 70 6C 65 48 61 73 68
Encoded S
        01 60 4D 79 20 54 75 70 6C 65 20 41 70 70
bytepad data
        01 A8 01 48 54 75 70 6C 65 48 61 73 68 01 60 4D
        79 20 54 75 70 6C 65 20 41 70 70 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
----------------------------------------------------------
About to Absorb data
State (in bytes)
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
Data to be absorbed
        01 A8 01 48 54 75 70 6C 65 48 61 73 68 01 60 4D
        79 20 54 75 70 6C 65 20 41 70 70 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
Xor'd state (in bytes)
```

```
        01 A8 01 48 54 75 70 6C 65 48 61 73 68 01 60 4D
        79 20 54 75 70 6C 65 20 41 70 70 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00

After Permutation
        6F 92 C7 41 FD F3 22 6F A1 AC EB F5 AB D1 81 C3
        AE 04 2B 5E C6 03 92 D3 16 B5 CC F5 6C 1E A4 B1
        16 22 57 38 89 A7 7B BE B1 9D F1 3D 24 89 86 39
        09 E7 EB EF 03 56 8A 96 39 C4 EC 06 A8 9E D4 02
        6E 10 90 83 86 D4 D5 AD B2 00 84 89 36 F6 F2 66
        A6 B0 93 0B 7B D2 52 13 C6 53 42 20 E5 25 92 21
        9F 83 D0 A9 44 0C 70 4A F3 4D 3C 7A 33 B1 91 1D
        51 FB EE 20 1C CC 57 F2 41 BC 2E AE C2 BF D0 A2
        DB A5 0E D4 A9 84 E7 AA C1 B2 B7 E5 1C 93 5A 9E
        7A F8 00 93 5B 6F FA 0E 8A DE 7B EA C7 11 29 AF
        BE C3 40 47 B1 8D CA 84 D3 47 9A 47 E7 43 52 36
        7E 9B AE 6C 7C 97 BB 55 54 3F 2F 09 F7 76 FC E8
        05 CC E4 F6 85 3F 2B 17
about to call last of the absorb phase
------------------------------------------------------------
About to Absorb data
State (in bytes)
        6F 92 C7 41 FD F3 22 6F A1 AC EB F5 AB D1 81 C3
        AE 04 2B 5E C6 03 92 D3 16 B5 CC F5 6C 1E A4 B1
        16 22 57 38 89 A7 7B BE B1 9D F1 3D 24 89 86 39
        09 E7 EB EF 03 56 8A 96 39 C4 EC 06 A8 9E D4 02
        6E 10 90 83 86 D4 D5 AD B2 00 84 89 36 F6 F2 66
        A6 B0 93 0B 7B D2 52 13 C6 53 42 20 E5 25 92 21
        9F 83 D0 A9 44 0C 70 4A F3 4D 3C 7A 33 B1 91 1D
        51 FB EE 20 1C CC 57 F2 41 BC 2E AE C2 BF D0 A2
        DB A5 0E D4 A9 84 E7 AA C1 B2 B7 E5 1C 93 5A 9E
        7A F8 00 93 5B 6F FA 0E 8A DE 7B EA C7 11 29 AF
        BE C3 40 47 B1 8D CA 84 D3 47 9A 47 E7 43 52 36
        7E 9B AE 6C 7C 97 BB 55 54 3F 2F 09 F7 76 FC E8
        05 CC E4 F6 85 3F 2B 17
Data to be absorbed
        01 18 00 01 02 01 30 10 11 12 13 14 15 01 48 20
        21 22 23 24 25 26 27 28 00 01 04 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
```

Xor'd state (in bytes)

```
        6E 8A C7 40 FF F2 12 7F B0 BE F8 E1 BE D0 C9 E3
        8F 26 08 7A E3 25 B5 FB 16 B4 C8 F5 6C 1E A4 B1
        16 22 57 38 89 A7 7B BE B1 9D F1 3D 24 89 86 39
        09 E7 EB EF 03 56 8A 96 39 C4 EC 06 A8 9E D4 02
        6E 10 90 83 86 D4 D5 AD B2 00 84 89 36 F6 F2 66
        A6 B0 93 0B 7B D2 52 13 C6 53 42 20 E5 25 92 21
        9F 83 D0 A9 44 0C 70 4A F3 4D 3C 7A 33 B1 91 1D
        51 FB EE 20 1C CC 57 F2 41 BC 2E AE C2 BF D0 A2
        DB A5 0E D4 A9 84 E7 AA C1 B2 B7 E5 1C 93 5A 9E
        7A F8 00 93 5B 6F FA 0E 8A DE 7B EA C7 11 29 AF
        BE C3 40 47 B1 8D CA 04 D3 47 9A 47 E7 43 52 36
        7E 9B AE 6C 7C 97 BB 55 54 3F 2F 09 F7 76 FC E8
        05 CC E4 F6 85 3F 2B 17
```

After Permutation

```
        90 0F E1 6C AD 09 8D 28 E7 4D 63 2E D8 52 F9 9D
        AA B7 F7 DF 4D 99 E7 75 65 78 85 B4 BF 76 D6 F8
        07 4B 9C 2E AF 01 28 95 C2 6B E8 60 1E FE 02 90
        8F 7B D4 19 AC 13 A5 0D 75 4B 9C A3 89 29 AC 3C
        51 45 86 C4 E7 B8 67 45 97 A1 16 7B BD F7 74 4A
        8D 8F 2A 56 77 44 17 5A 84 B0 7E D2 F9 06 39 9B
        AA 60 D4 0A 2A 6E B0 3C 08 40 AB 8F 6B B9 2C 86
        47 AD C5 0D 18 3C A4 6A D3 29 C6 FB F7 3B 26 C9
        26 6F 1A 89 25 57 9E F5 17 29 69 2F 56 D1 95 A1
        FE E9 7D 73 71 3F D5 5B 31 8A 73 AB CA 03 58 B6
        6A 47 11 2C 25 65 55 B6 21 47 FD F7 79 25 E6 FA
        34 87 35 4F 64 5E 6F 68 C3 51 2B 7B 49 7A 9A A8
        8C F3 5E 5A 76 3D 31 4F
```

Outval is

```
        90 0F E1 6C AD 09 8D 28 E7 4D 63 2E D8 52 F9 9D
        AA B7 F7 DF 4D 99 E7 75 65 78 85 B4 BF 76 D6 F8
```

===

TupleHashXOF:

Sample #4

Security Strength: 256-bits

Number of Tuples: 2

Tuple 1

```
        00 01 02

Tuple 2
        10 11 12 13 14 15

Requested output length is 512-bits

S (as a character string) is
        "(null)"
----------------------------------------------------------
Encoded X[1]
        01 18 00 01 02
Encoded X[2]
        01 30 10 11 12 13 14 15
Encoded N
        01 48 54 75 70 6C 65 48 61 73 68
Encoded S
        01 00
bytepad data
        01 88 01 48 54 75 70 6C 65 48 61 73 68 01 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
----------------------------------------------------------
About to Absorb data
State (in bytes)
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
Data to be absorbed
        01 88 01 48 54 75 70 6C 65 48 61 73 68 01 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
Xor'd state (in bytes)
        01 88 01 48 54 75 70 6C 65 48 61 73 68 01 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00

After Permutation
        B4 53 E2 7F 89 F4 DD 43 11 02 47 7E A9 1F 15 CF
        C8 AC 83 90 41 26 B7 05 1A 4D D1 DA 41 66 5F B5
        22 41 B5 5F 8F B4 63 23 94 88 74 86 AD C2 A6 EC
        49 6D 5A 58 0A 7A F0 AA 76 B5 40 3E 35 67 2E 1C
        BC A7 78 D7 E6 69 7B AC CD 9D 25 77 9A E7 E6 2C
        41 AD FA 64 A8 48 1F 56 81 19 EA 5A 32 2A AA 0C
        F6 EB 75 57 42 60 BB 99 67 A3 E2 67 AC D4 F5 C2
        28 B4 30 54 B9 FD C4 9A 06 59 2C 5B CD 4D E6 A2
        44 09 C6 30 DC 72 9C 9A 71 65 05 1F D2 D5 E6 A9
        C5 E7 4F 99 69 DE 51 E9 50 16 48 8E DA 08 E1 D8
        96 18 52 33 C0 57 67 D9 15 D0 E7 E3 A7 71 76 0E
        7A 02 01 2D 5F EE A8 22 57 8E D2 0A 7E 74 4C 9C
        5B 01 31 26 A8 B0 66 B4
about to call last of the absorb phase
----------------------------------------------------------
About to Absorb data
State (in bytes)
        B4 53 E2 7F 89 F4 DD 43 11 02 47 7E A9 1F 15 CF
        C8 AC 83 90 41 26 B7 05 1A 4D D1 DA 41 66 5F B5
        22 41 B5 5F 8F B4 63 23 94 88 74 86 AD C2 A6 EC
        49 6D 5A 58 0A 7A F0 AA 76 B5 40 3E 35 67 2E 1C
        BC A7 78 D7 E6 69 7B AC CD 9D 25 77 9A E7 E6 2C
        41 AD FA 64 A8 48 1F 56 81 19 EA 5A 32 2A AA 0C
        F6 EB 75 57 42 60 BB 99 67 A3 E2 67 AC D4 F5 C2
        28 B4 30 54 B9 FD C4 9A 06 59 2C 5B CD 4D E6 A2
        44 09 C6 30 DC 72 9C 9A 71 65 05 1F D2 D5 E6 A9
        C5 E7 4F 99 69 DE 51 E9 50 16 48 8E DA 08 E1 D8
        96 18 52 33 C0 57 67 D9 15 D0 E7 E3 A7 71 76 0E
```

```
        7A 02 01 2D 5F EE A8 22 57 8E D2 0A 7E 74 4C 9C
        5B 01 31 26 A8 B0 66 B4
Data to be absorbed
        01 18 00 01 02 01 30 10 11 12 13 14 15 00 01 04
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
Xor'd state (in bytes)
        B5 4B E2 7E 8B F5 ED 53 00 10 54 6A BC 1F 14 CB
        C8 AC 83 90 41 26 B7 05 1A 4D D1 DA 41 66 5F B5
        22 41 B5 5F 8F B4 63 23 94 88 74 86 AD C2 A6 EC
        49 6D 5A 58 0A 7A F0 AA 76 B5 40 3E 35 67 2E 1C
        BC A7 78 D7 E6 69 7B AC CD 9D 25 77 9A E7 E6 2C
        41 AD FA 64 A8 48 1F 56 81 19 EA 5A 32 2A AA 0C
        F6 EB 75 57 42 60 BB 99 67 A3 E2 67 AC D4 F5 C2
        28 B4 30 54 B9 FD C4 9A 06 59 2C 5B CD 4D E6 A2
        44 09 C6 30 DC 72 9C 1A 71 65 05 1F D2 D5 E6 A9
        C5 E7 4F 99 69 DE 51 E9 50 16 48 8E DA 08 E1 D8
        96 18 52 33 C0 57 67 D9 15 D0 E7 E3 A7 71 76 0E
        7A 02 01 2D 5F EE A8 22 57 8E D2 0A 7E 74 4C 9C
        5B 01 31 26 A8 B0 66 B4

After Permutation
        03 DE D4 61 0E D6 45 0A 1E 3F 8B C4 49 51 D1 4F
        BC 38 4A B0 EF E5 7B 00 0D F6 B6 DF 5A AE 7C D5
        68 E7 73 77 DA F1 3F 37 EC 75 CF 5F C5 98 B6 84
        1D 51 DD 20 7C 99 1C D4 5D 21 0B A6 0A C5 2E B9
        DA 7D 23 08 05 98 6D 65 89 10 F7 12 4A D1 F3 5A
        1D C4 31 35 92 CE BD EC D5 1B 10 0B B5 53 64 C2
        E6 3F AC 75 84 9E FC BF 31 34 44 6E 2C CB 09 6D
        9D ED F0 74 FD 7B FB 34 1A 6D 95 44 9F 4A F6 3F
        2F 96 81 03 2A 2F 16 58 DE B1 B9 88 38 41 70 96
        9A 35 C7 E9 0A F7 48 7E 30 11 67 06 95 6D B4 DE
        E6 59 BB 52 5F 8E B1 00 55 FB 2C 58 03 31 04 1D
        E1 B5 6A 8A 2B 69 14 10 0B 88 CC 15 F3 93 C2 E5
        05 A8 D0 13 B6 A6 BC 59
Outval is
        03 DE D4 61 0E D6 45 0A 1E 3F 8B C4 49 51 D1 4F
        BC 38 4A B0 EF E5 7B 00 0D F6 B6 DF 5A AE 7C D5
        68 E7 73 77 DA F1 3F 37 EC 75 CF 5F C5 98 B6 84
        1D 51 DD 20 7C 99 1C D4 5D 21 0B A6 0A C5 2E B9
```

```
================================================================

TupleHashXOF:
        Sample #5

Security Strength: 256-bits

Number of Tuples: 2

Tuple 1
        00 01 02

Tuple 2
        10 11 12 13 14 15

Requested output length is 512-bits

S (as a character string) is
        "My Tuple App"
----------------------------------------------------------
Encoded X[1]
        01 18 00 01 02
Encoded X[2]
        01 30 10 11 12 13 14 15
Encoded N
        01 48 54 75 70 6C 65 48 61 73 68
Encoded S
        01 60 4D 79 20 54 75 70 6C 65 20 41 70 70
bytepad data
        01 88 01 48 54 75 70 6C 65 48 61 73 68 01 60 4D
        79 20 54 75 70 6C 65 20 41 70 70 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
----------------------------------------------------------
About to Absorb data
State (in bytes)
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
Data to be absorbed
        01 88 01 48 54 75 70 6C 65 48 61 73 68 01 60 4D
        79 20 54 75 70 6C 65 20 41 70 70 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
Xor'd state (in bytes)
        01 88 01 48 54 75 70 6C 65 48 61 73 68 01 60 4D
        79 20 54 75 70 6C 65 20 41 70 70 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00

After Permutation
        4E 7C C8 AC 2E 83 E3 88 4C 43 37 EC 42 5E 1C 9B
        02 9F 24 F7 50 37 44 01 73 B3 B2 E9 88 F7 D8 95
        34 78 47 27 BA 02 6D 16 3F E1 23 BD 74 58 75 F6
        5F 81 94 87 75 4A CA BC C5 60 9B 58 55 2E 02 75
        24 E0 D2 C0 D0 CD 3C 3D 29 D1 26 BD 50 AA DC 86
        CB E1 17 49 87 4B FC 47 9E 38 9A 8A EE 33 19 37
        2A C5 43 68 EC 7A 55 E0 91 25 7E C8 D3 C8 AC D4
        ED CA 61 97 A6 D5 C1 2D 53 F4 AD 05 5D 2E 13 32
        DF 96 5E ED C6 4F 36 C1 1C B8 DD 4B A9 FD FB EF
        B1 D2 DF D5 2A E6 0A 75 B8 F7 42 05 25 61 71 8F
        E5 E3 A9 C7 54 83 F2 F2 74 F0 D0 03 D6 72 EF 64
        DB F8 6F 0E E4 31 63 29 3C DA F6 E5 FE CD 80 47
        52 E3 C5 1B 25 AA D6 81
about to call last of the absorb phase
------------------------------------------------------------
About to Absorb data
State (in bytes)
        4E 7C C8 AC 2E 83 E3 88 4C 43 37 EC 42 5E 1C 9B
```

```
02 9F 24 F7 50 37 44 01 73 B3 B2 E9 88 F7 D8 95
34 78 47 27 BA 02 6D 16 3F E1 23 BD 74 58 75 F6
5F 81 94 87 75 4A CA BC C5 60 9B 58 55 2E 02 75
24 E0 D2 C0 D0 CD 3C 3D 29 D1 26 BD 50 AA DC 86
CB E1 17 49 87 4B FC 47 9E 38 9A 8A EE 33 19 37
2A C5 43 68 EC 7A 55 E0 91 25 7E C8 D3 C8 AC D4
ED CA 61 97 A6 D5 C1 2D 53 F4 AD 05 5D 2E 13 32
DF 96 5E ED C6 4F 36 C1 1C B8 DD 4B A9 FD FB EF
B1 D2 DF D5 2A E6 0A 75 B8 F7 42 05 25 61 71 8F
E5 E3 A9 C7 54 83 F2 F2 74 F0 D0 03 D6 72 EF 64
DB F8 6F 0E E4 31 63 29 3C DA F6 E5 FE CD 80 47
52 E3 C5 1B 25 AA D6 81
```

Data to be absorbed

```
01 18 00 01 02 01 30 10 11 12 13 14 15 00 01 04
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
```

Xor'd state (in bytes)

```
4F 64 C8 AD 2C 82 D3 98 5D 51 24 F8 57 5E 1D 9F
02 9F 24 F7 50 37 44 01 73 B3 B2 E9 88 F7 D8 95
34 78 47 27 BA 02 6D 16 3F E1 23 BD 74 58 75 F6
5F 81 94 87 75 4A CA BC C5 60 9B 58 55 2E 02 75
24 E0 D2 C0 D0 CD 3C 3D 29 D1 26 BD 50 AA DC 86
CB E1 17 49 87 4B FC 47 9E 38 9A 8A EE 33 19 37
2A C5 43 68 EC 7A 55 E0 91 25 7E C8 D3 C8 AC D4
ED CA 61 97 A6 D5 C1 2D 53 F4 AD 05 5D 2E 13 32
DF 96 5E ED C6 4F 36 41 1C B8 DD 4B A9 FD FB EF
B1 D2 DF D5 2A E6 0A 75 B8 F7 42 05 25 61 71 8F
E5 E3 A9 C7 54 83 F2 F2 74 F0 D0 03 D6 72 EF 64
DB F8 6F 0E E4 31 63 29 3C DA F6 E5 FE CD 80 47
52 E3 C5 1B 25 AA D6 81
```

After Permutation

```
64 83 CB 3C 99 52 EB 20 E8 30 AF 47 85 85 1F C5
97 EE 3B F9 3B B7 60 2C 0E F6 A6 5D 74 1A EC A7
E6 3C 3B 12 89 81 AA 05 C6 D2 74 38 C7 9D 27 54
BB 1B 71 91 F1 25 D6 62 0F CA 12 CE 65 8B 24 42
F3 FA 29 3C B6 E7 3E 23 25 89 F0 08 1E B7 65 F9
5E CC FB E5 3F F9 A3 BC A8 9B 43 85 BF 93 23 CD
24 02 A4 80 95 8D C3 9C C9 C8 6B 7D 4D 22 C7 16
4E 44 DA E6 E1 70 D9 82 8D 13 21 F4 73 E2 A5 4C
1F 1A 11 3A 15 3D ED B6 47 41 33 63 B5 D2 47 9E
```

```
        FF 5B B5 18 FB DE 98 54 8B 93 11 74 1E 91 05 D1
        33 E4 1B 3A 2A 59 1E C1 1E 01 6F 35 81 34 2C 1A
        62 63 F3 7C D9 53 49 A1 A3 40 4B 77 C6 BE 39 EA
        F6 0D F4 C4 4B 1A BC B9
Outval is
        64 83 CB 3C 99 52 EB 20 E8 30 AF 47 85 85 1F C5
        97 EE 3B F9 3B B7 60 2C 0E F6 A6 5D 74 1A EC A7
        E6 3C 3B 12 89 81 AA 05 C6 D2 74 38 C7 9D 27 54
        BB 1B 71 91 F1 25 D6 62 0F CA 12 CE 65 8B 24 42

============================================================

TupleHashXOF:
        Sample #6

Security Strength: 256-bits

Number of Tuples: 3

Tuple 1
        00 01 02

Tuple 2
        10 11 12 13 14 15

Tuple 3
        20 21 22 23 24 25 26 27 28

Requested output length is 512-bits

S (as a character string) is
        "My Tuple App"
------------------------------------------------------------
Encoded X[1]
        01 18 00 01 02
Encoded X[2]
        01 30 10 11 12 13 14 15
Encoded X[3]
        01 48 20 21 22 23 24 25 26 27 28
Encoded N
        01 48 54 75 70 6C 65 48 61 73 68
Encoded S
        01 60 4D 79 20 54 75 70 6C 65 20 41 70 70
bytepad data
        01 88 01 48 54 75 70 6C 65 48 61 73 68 01 60 4D
        79 20 54 75 70 6C 65 20 41 70 70 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
------------------------------------------------------------
About to Absorb data
State (in bytes)
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
Data to be absorbed
        01 88 01 48 54 75 70 6C 65 48 61 73 68 01 60 4D
        79 20 54 75 70 6C 65 20 41 70 70 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
Xor'd state (in bytes)
        01 88 01 48 54 75 70 6C 65 48 61 73 68 01 60 4D
        79 20 54 75 70 6C 65 20 41 70 70 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00

After Permutation
        4E 7C C8 AC 2E 83 E3 88 4C 43 37 EC 42 5E 1C 9B
        02 9F 24 F7 50 37 44 01 73 B3 B2 E9 88 F7 D8 95
        34 78 47 27 BA 02 6D 16 3F E1 23 BD 74 58 75 F6
```

```
    5F 81 94 87 75 4A CA BC C5 60 9B 58 55 2E 02 75
    24 E0 D2 C0 D0 CD 3C 3D 29 D1 26 BD 50 AA DC 86
    CB E1 17 49 87 4B FC 47 9E 38 9A 8A EE 33 19 37
    2A C5 43 68 EC 7A 55 E0 91 25 7E C8 D3 C8 AC D4
    ED CA 61 97 A6 D5 C1 2D 53 F4 AD 05 5D 2E 13 32
    DF 96 5E ED C6 4F 36 C1 1C B8 DD 4B A9 FD FB EF
    B1 D2 DF D5 2A E6 0A 75 B8 F7 42 05 25 61 71 8F
    E5 E3 A9 C7 54 83 F2 F2 74 F0 D0 03 D6 72 EF 64
    DB F8 6F 0E E4 31 63 29 3C DA F6 E5 FE CD 80 47
    52 E3 C5 1B 25 AA D6 81
about to call last of the absorb phase
--------------------------------------------------------
About to Absorb data
State (in bytes)
    4E 7C C8 AC 2E 83 E3 88 4C 43 37 EC 42 5E 1C 9B
    02 9F 24 F7 50 37 44 01 73 B3 B2 E9 88 F7 D8 95
    34 78 47 27 BA 02 6D 16 3F E1 23 BD 74 58 75 F6
    5F 81 94 87 75 4A CA BC C5 60 9B 58 55 2E 02 75
    24 E0 D2 C0 D0 CD 3C 3D 29 D1 26 BD 50 AA DC 86
    CB E1 17 49 87 4B FC 47 9E 38 9A 8A EE 33 19 37
    2A C5 43 68 EC 7A 55 E0 91 25 7E C8 D3 C8 AC D4
    ED CA 61 97 A6 D5 C1 2D 53 F4 AD 05 5D 2E 13 32
    DF 96 5E ED C6 4F 36 C1 1C B8 DD 4B A9 FD FB EF
    B1 D2 DF D5 2A E6 0A 75 B8 F7 42 05 25 61 71 8F
    E5 E3 A9 C7 54 83 F2 F2 74 F0 D0 03 D6 72 EF 64
    DB F8 6F 0E E4 31 63 29 3C DA F6 E5 FE CD 80 47
    52 E3 C5 1B 25 AA D6 81
Data to be absorbed
    01 18 00 01 02 01 30 10 11 12 13 14 15 01 48 20
    21 22 23 24 25 26 27 28 00 01 04 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00
Xor'd state (in bytes)
    4F 64 C8 AD 2C 82 D3 98 5D 51 24 F8 57 5F 54 BB
    23 BD 07 D3 75 11 63 29 73 B2 B6 E9 88 F7 D8 95
    34 78 47 27 BA 02 6D 16 3F E1 23 BD 74 58 75 F6
    5F 81 94 87 75 4A CA BC C5 60 9B 58 55 2E 02 75
    24 E0 D2 C0 D0 CD 3C 3D 29 D1 26 BD 50 AA DC 86
    CB E1 17 49 87 4B FC 47 9E 38 9A 8A EE 33 19 37
    2A C5 43 68 EC 7A 55 E0 91 25 7E C8 D3 C8 AC D4
    ED CA 61 97 A6 D5 C1 2D 53 F4 AD 05 5D 2E 13 32
    DF 96 5E ED C6 4F 36 41 1C B8 DD 4B A9 FD FB EF
```

```
        B1 D2 DF D5 2A E6 0A 75 B8 F7 42 05 25 61 71 8F
        E5 E3 A9 C7 54 83 F2 F2 74 F0 D0 03 D6 72 EF 64
        DB F8 6F 0E E4 31 63 29 3C DA F6 E5 FE CD 80 47
        52 E3 C5 1B 25 AA D6 81

After Permutation
        0C 59 B1 14 64 F2 33 6C 34 66 3E D5 1B 2B 95 0B
        EC 74 36 10 85 6F 36 C2 8D 1D 08 8D 8A 24 46 28
        4D D0 98 30 A6 A1 78 DC 75 23 76 19 9F AE 93 5D
        86 CF DE E5 91 3D 49 22 DF D3 69 B6 6A 53 C8 97
        D8 BC DF 4E FE 75 82 41 65 06 B8 16 DD 1A 50 4D
        36 17 CD C7 AA 3C 93 FD 4E E0 4E 15 FF 6D A6 D2
        34 79 71 0D BD C0 1C 65 EE BE 2B F0 3C EA AD 4D
        1E ED 99 6A BF B9 BE 93 9B 9F D7 73 F5 A2 59 59
        28 54 6A E2 57 10 C4 33 FD 3B A8 4E 1B EC D5 4C
        E3 70 AB 7F 50 A8 54 88 7A F8 65 D9 FB 85 6D 0B
        50 4E DC EF 60 A4 8A B6 6C 57 3A 16 D0 69 CC 96
        70 5E 24 81 78 A7 3C 24 DA EC 95 57 76 C7 F3 32
        11 73 E3 A9 7B 7B 96 B1
Outval is
        0C 59 B1 14 64 F2 33 6C 34 66 3E D5 1B 2B 95 0B
        EC 74 36 10 85 6F 36 C2 8D 1D 08 8D 8A 24 46 28
        4D D0 98 30 A6 A1 78 DC 75 23 76 19 9F AE 93 5D
        86 CF DE E5 91 3D 49 22 DF D3 69 B6 6A 53 C8 97

============================================================
```