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

TupleHash:
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 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 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

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

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 01 00 02
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 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 F9 84 AD
D9 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
C5 D8 78 6C 1A FB 9B 82 11 1A B3 4B 65 B2 C0 04

8F A6 4E 6D 48 E2 63 26 4C E1 70 7D 3F FC 8E D1
B9 A8 D3 D5 27 55 51 4E 92 F5 04 9B 12 08 7A 54
35 CA 60 19 6E 5E DE AE F4 A1 02 CA 43 22 D1 0D
05 13 31 DC B1 AC AF 82 96 C7 F6 1A 04 70 56 32
03 46 87 87 D0 4B 44 23 A0 3C F7 DA FF 14 4C 40
EA 0C 7C FA B1 AA A9 EF BC FB 5E 49 36 95 B6 89
A1 2E C2 78 2A AD 8C A5 E3 39 AA EA BA B9 42 B5
6B C9 7B 0C 26 B1 39 9A E0 0D 13 2B 85 19 0E 27
2E 3F B3 0E 09 BB FB 8F 0C 06 12 57 ED 12 65 59
6F A2 BF 41 9A 65 B9 40 8E 85 41 64 9B 3B 63 B2
CC A3 AF AB 77 33 B7 E6 58 D7 B0 A8 14 5A 13 8B
BA C8 99 9E B1 E2 92 9E

Outval is

C5 D8 78 6C 1A FB 9B 82 11 1A B3 4B 65 B2 C0 04
8F A6 4E 6D 48 E2 63 26 4C E1 70 7D 3F FC 8E D1

==========

TupleHash:

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

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

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

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

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 00 02
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 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

Xor'd state (in bytes)

6E 8A C7 40 FF F2 12 7F B0 BE F8 E1 BE D0 81 C1
AA 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
75 CD B2 0F F4 DB 11 54 E8 41 D7 58 E2 41 60 C5
4B AE 86 EB 8C 13 E7 F5 F4 0E B3 55 88 E9 6D FB
F0 B6 E5 CF 72 90 5E DE 4F 6D CF 18 F4 82 28 16
77 91 EB FF 68 FA 8E E5 82 54 5E 4C 3C 67 7F 0F
52 39 88 7D 37 45 85 74 23 BB A0 8D 44 87 B7 EC
54 CE F0 3B 5A 28 65 9E 72 02 14 F1 5E 6B B1 8D
48 93 90 97 F7 8E 88 8D 18 AF AF 5F 52 04 8E A8
BD AF 15 C8 B9 25 73 F8 FA A1 28 7F 8F 7F 86 74
6D B7 89 8D CB 64 14 5D 66 B6 2E A2 00 54 30 A8
FE 5E 82 FA 5D 8C 16 7F 4E 78 25 59 E6 3D 6A CD
88 36 90 15 D5 4F E0 39 B6 48 59 37 D5 F1 9B F8
00 2B 70 45 58 26 D7 04 9C 31 2E 16 8E F5 E4 0F
94 77 8A 8E AD A0 E5 DB
Outval is
75 CD B2 0F F4 DB 11 54 E8 41 D7 58 E2 41 60 C5
4B AE 86 EB 8C 13 E7 F5 F4 0E B3 55 88 E9 6D FB

==========

TupleHash:
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

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

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 01 00 02 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 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 17 B5 CE F1 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

E6 0F 20 2C 89 A2 63 1E DA 8D 4C 58 8C A5 FD 07
F3 9E 51 51 99 8D EC CF 97 3A DB 38 04 BB 6E 84
05 AA 5B FC 8B 91 96 0F CD 3E 88 5B AF 4A 87 02
BF D1 F3 4B 7F C2 65 55 CB EC 80 93 45 20 A5 9B
DA B7 0A FA 86 93 B9 65 73 76 E1 D7 10 D1 5D F9
DA FC DB 4C 54 5B 60 73 21 22 28 5D E6 17 EA AB
B1 5B BD 7E 83 21 AF 6A 97 56 72 73 8E DC 12 12
BD E2 76 1E 80 DB 42 BC 85 48 CA 2F 04 9A 5B DD
52 65 3E C9 FA D6 FC A2 9C F0 A9 8D BC 97 42 4C
1C 98 5C 5E CB E7 E4 1D DD 2F E3 C2 5F 94 0E 98
C5 D1 B6 5A CB DA 2F 4B 41 3F DF 0A 9C B9 4B 1B
D5 15 40 F7 CC 57 26 2F 05 7D 60 D7 9C DA 6D 49
35 D8 05 31 F7 08 1A 26

Outval is

E6 0F 20 2C 89 A2 63 1E DA 8D 4C 58 8C A5 FD 07
F3 9E 51 51 99 8D EC CF 97 3A DB 38 04 BB 6E 84

==========

TupleHash:

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 02 00 02
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 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

Xor'd state (in bytes)

B5 4B E2 7E 8B F5 ED 53 00 10 54 6A BC 1D 15 CD
CC 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

CF B7 05 8C AC A5 E6 68 F8 1A 12 A2 0A 21 95 CE
97 A9 25 F1 DB A3 E7 44 9A 56 F8 22 01 EC 60 73
11 AC 26 96 B1 AB 5E A2 35 2D F1 42 3B DE 7B D4
BB 78 C9 AE D1 A8 53 C7 86 72 F9 EB 23 BB E1 94
07 64 45 F4 6F F5 16 45 BB 1A 68 71 25 FD F7 2C
C6 DA EF 5B EC 52 2E F2 EB A9 7B F4 07 4F 65 2E
AA E0 84 B2 D8 C0 70 4B BA 7D CC 41 42 1F 4C CC
1F EB 2F 9C B4 EC 79 C3 63 D5 04 47 9B 9E 70 6B
36 38 48 49 DF 19 9A A0 82 E2 81 19 A2 F3 7F CE
64 F7 69 67 AC 54 01 50 D0 71 73 66 36 19 EF 5D
F7 9E CF 4A E7 2E 12 2E DF 2B E1 08 4D 7A 60 EE
E2 1A AA A0 49 50 FD C0 14 BD 6A 1E D4 9A EB 2F
B0 D6 E7 B0 36 3B EC C6

Outval is

CF B7 05 8C AC A5 E6 68 F8 1A 12 A2 0A 21 95 CE
97 A9 25 F1 DB A3 E7 44 9A 56 F8 22 01 EC 60 73
11 AC 26 96 B1 AB 5E A2 35 2D F1 42 3B DE 7B D4
BB 78 C9 AE D1 A8 53 C7 86 72 F9 EB 23 BB E1 94

==

TupleHash:
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 02 00 02
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 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

Xor'd state (in bytes)

4F 64 C8 AD 2C 82 D3 98 5D 51 24 F8 57 5C 1C 99
06 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

14 7C 21 91 D5 ED 7E FD 98 DB D9 6D 7A B5 A1 16
92 57 6F 5F E2 A5 06 5F 3E 33 DE 6B BA 9F 3A A1
C4 E9 A0 68 A2 89 C6 1C 95 AA B3 0A EE 1E 41 0B
0B 60 7D E3 62 0E 24 A4 E3 BF 98 52 A1 D4 36 7E
1C 0E 46 8F 5B F4 D2 3B BE 9E 38 86 AA 9F CD 17
16 7D 4E 0E 1F 48 3D 22 63 17 18 E4 FD 6A 4F 05
58 98 E9 E1 03 A9 AD E5 1B CF 60 50 F2 4A CF D1
F6 39 EF 4B 20 51 CC 24 18 6A BA 0B A4 12 F0 AD
C8 81 58 55 61 D3 61 B5 82 15 B7 F6 3E CC C2 47

50 FC D0 D8 54 38 DC 62 8E 6B 3B 6C DB E2 BB AF
77 A3 43 52 77 78 E1 D6 7A FA 4B A9 06 FA F7 FB
60 13 A6 9C 8E 0E 4E 19 94 C2 B5 3E 6D E1 0B DB
E7 92 0C 8C 61 4E 20 64
Outval is
14 7C 21 91 D5 ED 7E FD 98 DB D9 6D 7A B5 A1 16
92 57 6F 5F E2 A5 06 5F 3E 33 DE 6B BA 9F 3A A1
C4 E9 A0 68 A2 89 C6 1C 95 AA B3 0A EE 1E 41 0B
0B 60 7D E3 62 0E 24 A4 E3 BF 98 52 A1 D4 36 7E

==========

TupleHash:
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

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 02 00 02 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 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

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 71 B3 B0 ED 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

45 00 0B E6 3F 9B 6B FD 89 F5 47 17 67 0F 69 A9
BC 76 35 91 A4 F0 5C 50 D6 88 91 A7 44 BC C6 E7
D6 D5 B5 E8 2C 01 8D A9 99 ED 35 B0 BB 49 C9 67
8E 52 6A BD 8E 85 C1 3E D2 54 02 1D B9 E7 90 CE
8D 0A 70 07 57 F9 95 4B 85 55 49 B0 A9 B1 51 32
08 72 5F 4D D5 9B 7C 3B DF 07 0D 3A 0E 06 2C 48
4B 08 1A 38 B9 BF 9F 6D 09 9D 4B DC 00 1E 92 45
C9 E4 B1 31 F8 C3 02 EC 38 25 89 92 73 DC 6A 10
7E E8 11 9E 8C D4 73 C0 F5 CE 04 A6 71 77 BD 92
76 4C 6E 72 E7 63 3E 47 D2 57 51 2A 0E D5 CA F1
57 ED 52 6B B2 58 61 DD 28 DB B3 AF D8 E1 18 82
10 53 0C 81 89 CC B8 F6 42 C3 F9 3F D5 FD 1A 04
3A 38 3B 26 59 8E 6F 1A

Outval is

45 00 0B E6 3F 9B 6B FD 89 F5 47 17 67 0F 69 A9
BC 76 35 91 A4 F0 5C 50 D6 88 91 A7 44 BC C6 E7
D6 D5 B5 E8 2C 01 8D A9 99 ED 35 B0 BB 49 C9 67
8E 52 6A BD 8E 85 C1 3E D2 54 02 1D B9 E7 90 CE

==========