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

ParallelHashXOF:
Sample #1

Security Strength: 128-bits

Length of data is 192-bits
Data is
00 01 02 03 04 05 06 07 10 11 12 13 14 15 16 17
20 21 22 23 24 25 26 27

Block size (B) is 8

Requested output length is 256-bits

S (as a character string) is
"(null)"

Encoded B
01 08
about to call last of the absorb phase

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
00 01 02 03 04 05 06 07 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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)

00 01 02 03 04 05 06 07 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

After Permutation

2E A7 A0 60 1B 9C 5C B4 1E 46 9F 85 40 77 C1 E3
3A AC 94 D3 9C E4 61 63 42 9A BC AC FA 99 2B BC
42 4A B6 89 BB 01 23 E0 DC 3E 0D 84 37 6A 56 61
6C A0 D2 F7 83 2F 6A 7F AC DD FB C0 D9 D6 17 5A
E7 AC 86 17 2D 43 F5 76 E6 AF 5B AA 80 DB 29 FC
07 9C B7 37 AA E6 CF 82 EA 69 AC 6D 00 5E 07 2D
41 FF 84 CA 47 77 2D FF 4A 08 C2 E2 9A 5D 69 A5
64 72 8B F5 66 9E D8 14 6A 9F DC 4E DB 5E 58 C9
62 14 0D 59 1F A6 BF 52 0B F0 88 92 6B 91 9F 79
71 61 6F C4 AA 4B 74 65 21 AC CE C8 E0 7B 9A 36
BA 71 81 76 18 A6 8C E1 23 17 CE ED 27 A2 7D 9C
ED 1F B9 FB A5 77 03 F7 D8 EE 18 DF 6B 3E 7A 5E
4A DD 80 27 02 65 00 13

about to call last of the absorb phase

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

10 11 12 13 14 15 16 17 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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)

10 11 12 13 14 15 16 17 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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

After Permutation

49 86 7B 4E 0D 7B A3 44 07 8E ED E9 BD 7E 84 21
67 9D ED 28 2A 0E 50 CE E8 F1 18 36 1C 08 75 95
A6 AF 48 A1 8A 74 56 4E 5B 76 26 E6 92 C5 5A A3
D6 F3 FB F0 30 6B 7E F0 D5 40 28 F7 AC F3 1F D1
0C F5 65 49 99 F6 06 65 37 67 53 91 28 41 71 90
76 AE 49 5C B0 77 E2 C6 0E C0 E1 37 4D B5 34 60
7F A4 2E 6A 94 30 F2 A5 D8 C7 1E 07 18 7B 61 2B
A0 3E 20 60 17 3C A8 32 FC 86 D4 7A 6D A7 58 07
4C E7 C6 07 B3 04 C0 79 E5 7F 93 EC B1 D4 C5 46
DA CD 8A CB F9 7D D2 A7 AE 18 2F 14 0F E9 8F 62
67 91 26 F7 34 9E 21 EB 4D DA 29 2D 7C 7A CE BD
1E EA E5 CC F7 63 28 42 ED F7 90 CC C5 06 B1 D1
0D 4E 82 71 D6 95 1F 7A

about to call last of the absorb phase

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

20 21 22 23 24 25 26 27 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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)

20 21 22 23 24 25 26 27 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

After Permutation

E6 89 84 75 8E E8 3E 4B 3F 43 7C 58 62 5D A0 CD
E3 EE 6B 06 BF 30 F0 F6 3D FF 39 15 A5 51 8F C8
CC 5A E2 EB 09 BF BA 5E 88 31 00 E2 85 5A F8 E1
EF C5 60 86 33 1F 5F 5D 57 BF 55 D9 EF 05 E0 C9
84 36 57 9E AB FD 9B 77 60 57 CB 1E 58 C2 F5 8E
52 F8 A4 11 24 23 D3 6D C1 6F 75 BF 8E DD 2B 3F
2D 34 95 9F E4 D3 5D 65 85 76 C6 E4 6D 81 64 F7
CA 66 52 91 96 6F 76 A0 B3 E6 AA A7 E0 43 54 4A
40 C0 4B 36 A8 01 13 5D 2D EA C3 D5 F6 91 89 F7
79 C8 27 45 6B C0 28 34 C3 C3 57 C7 08 3E 52 23

74 38 84 DE E1 F1 99 3C 0A 51 E6 8C A1 69 8E 9B
9D 11 F7 CF AE 94 C5 DB C9 CD CC 5A AE B7 55 51
96 A5 93 9E 1D D0 06 51

Encoded n

03 01

Encoded L

00 01

Length of newX is <816>

newX is

01 08 2E A7 A0 60 1B 9C 5C B4 1E 46 9F 85 40 77
C1 E3 3A AC 94 D3 9C E4 61 63 42 9A BC AC FA 99
2B BC 49 86 7B 4E 0D 7B A3 44 07 8E ED E9 BD 7E
84 21 67 9D ED 28 2A 0E 50 CE E8 F1 18 36 1C 08
75 95 E6 89 84 75 8E E8 3E 4B 3F 43 7C 58 62 5D
A0 CD E3 EE 6B 06 BF 30 F0 F6 3D FF 39 15 A5 51
8F C8 03 01 00 01

Encoded N

01 60 50 61 72 61 6C 6C 65 6C 48 61 73 68

Encoded S

01 00

bytepad data

01 A8 01 60 50 61 72 61 6C 6C 65 6C 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

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

Data to be absorbed

01 A8 01 60 50 61 72 61 6C 6C 65 6C 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 00 00 00 00 00
00 00 00 00 00 00 00 00

Xor'd state (in bytes)

01 A8 01 60 50 61 72 61 6C 6C 65 6C 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

After Permutation

23 85 01 4D D6 CF E5 32 F4 A5 71 C7 26 BD 4F B4
D7 DB 5A F7 3A D6 F1 2A DF 4C 4E D7 EF FE A9 85
41 B2 2C C9 BE 91 98 C5 8C 7D 48 35 80 0C 3B 3A
6E 58 CE DF 4A 20 B1 69 65 3E DB 68 F6 C3 AC E5
B8 95 04 71 3A B1 CF 78 5A 0C 88 7C 07 A8 C6 95
ED D1 EC 8C BF 43 47 F4 D0 AC 84 5C BC 32 6E 52
D6 7A E1 D6 BC F1 68 D1 19 FA 4C 8B 5B 43 16 1D
E8 50 40 5C B7 35 6C B9 F8 F3 D2 12 C8 FB C2 C9
F9 2D 0C 32 7C F3 F3 8E B6 C8 3B 3B 51 90 3E 29
26 44 75 23 EA 46 F3 F2 A3 58 59 2F EB 84 F6 E9
09 38 FA AD E3 23 09 D9 CD 8C 36 01 17 46 37 1D
D7 2D 6E E3 C2 C7 64 D4 48 E7 99 06 BD 43 EB D4
82 0E 51 34 4E 3C 1F E2

about to call last of the absorb phase

About to Absorb data

State (in bytes)

23 85 01 4D D6 CF E5 32 F4 A5 71 C7 26 BD 4F B4
D7 DB 5A F7 3A D6 F1 2A DF 4C 4E D7 EF FE A9 85
41 B2 2C C9 BE 91 98 C5 8C 7D 48 35 80 0C 3B 3A
6E 58 CE DF 4A 20 B1 69 65 3E DB 68 F6 C3 AC E5
B8 95 04 71 3A B1 CF 78 5A 0C 88 7C 07 A8 C6 95
ED D1 EC 8C BF 43 47 F4 D0 AC 84 5C BC 32 6E 52
D6 7A E1 D6 BC F1 68 D1 19 FA 4C 8B 5B 43 16 1D

E8 50 40 5C B7 35 6C B9 F8 F3 D2 12 C8 FB C2 C9
F9 2D 0C 32 7C F3 F3 8E B6 C8 3B 3B 51 90 3E 29
26 44 75 23 EA 46 F3 F2 A3 58 59 2F EB 84 F6 E9
09 38 FA AD E3 23 09 D9 CD 8C 36 01 17 46 37 1D
D7 2D 6E E3 C2 C7 64 D4 48 E7 99 06 BD 43 EB D4
82 0E 51 34 4E 3C 1F E2

Data to be absorbed

01 08 2E A7 A0 60 1B 9C 5C B4 1E 46 9F 85 40 77
C1 E3 3A AC 94 D3 9C E4 61 63 42 9A BC AC FA 99
2B BC 49 86 7B 4E 0D 7B A3 44 07 8E ED E9 BD 7E
84 21 67 9D ED 28 2A 0E 50 CE E8 F1 18 36 1C 08
75 95 E6 89 84 75 8E E8 3E 4B 3F 43 7C 58 62 5D
A0 CD E3 EE 6B 06 BF 30 F0 F6 3D FF 39 15 A5 51
8F C8 03 01 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 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)

22 8D 2F EA 76 AF FE AE A8 11 6F 81 B9 38 0F C3
16 38 60 5B AE 05 6D CE BE 2F 0C 4D 53 52 53 1C
6A 0E 65 4F C5 DF 95 BE 2F 39 4F BB 6D E5 86 44
EA 79 A9 42 A7 08 9B 67 35 F0 33 99 EE F5 B0 ED
CD 00 E2 F8 BE C4 41 90 64 47 B7 3F 7B F0 A4 C8
4D 1C 0F 62 D4 45 F8 C4 20 5A B9 A3 85 27 CB 03
59 B2 E2 D7 BC F0 6C D1 19 FA 4C 8B 5B 43 16 1D
E8 50 40 5C B7 35 6C B9 F8 F3 D2 12 C8 FB C2 C9
F9 2D 0C 32 7C F3 F3 8E B6 C8 3B 3B 51 90 3E 29
26 44 75 23 EA 46 F3 F2 A3 58 59 2F EB 84 F6 E9
09 38 FA AD E3 23 09 59 CD 8C 36 01 17 46 37 1D
D7 2D 6E E3 C2 C7 64 D4 48 E7 99 06 BD 43 EB D4
82 0E 51 34 4E 3C 1F E2

After Permutation

FE 47 D6 61 E4 9F FE 5B 7D 99 99 22 C0 62 35 67
50 CA F5 52 98 5B 8E 8C E6 66 7F 27 27 C3 C8 D3
2F 03 4D 79 10 11 F4 8A 50 B4 3D 30 6E 75 BC 05
AF 44 46 82 B3 47 FE 73 97 BF 5E 19 62 43 D1 AA
4A D9 32 C4 00 ED 46 62 90 E2 29 51 AF 6F F3 C4
FA A8 86 CA B4 5B 7D 07 FB 45 1A DE 9E 93 70 4B
E7 0B B7 42 04 C4 CA 09 99 D4 9F 9F 5F C7 39 76
7F 99 43 63 04 4F 06 64 96 9D D1 55 FB D2 84 D1
45 F6 23 31 EC 51 32 54 4B 95 84 8B A0 B7 A5 E1
13 8E E7 7B C5 17 C3 9A 2A B5 C5 A8 2C CD 63 BE
48 99 64 02 13 B8 68 64 64 75 E8 03 1A 2D 84 E3
BB A4 CE 7F 59 DD D4 C7 E5 4A CC B8 9D 0E 19 B7
11 77 2C 97 C2 07 78 D4

Outval is

FE 47 D6 61 E4 9F FE 5B 7D 99 99 22 C0 62 35 67

50 CA F5 52 98 5B 8E 8C E6 66 7F 27 27 C3 C8 D3

==========

ParallelHashXOF:
Sample #2

Security Strength: 128-bits

Length of data is 192-bits
Data is
00 01 02 03 04 05 06 07 10 11 12 13 14 15 16 17
20 21 22 23 24 25 26 27

Block size (B) is 8

Requested output length is 256-bits

S (as a character string) is
"Parallel Data"

Encoded B
01 08
about to call last of the absorb phase

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
00 01 02 03 04 05 06 07 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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)

00 01 02 03 04 05 06 07 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

After Permutation

2E A7 A0 60 1B 9C 5C B4 1E 46 9F 85 40 77 C1 E3
3A AC 94 D3 9C E4 61 63 42 9A BC AC FA 99 2B BC
42 4A B6 89 BB 01 23 E0 DC 3E 0D 84 37 6A 56 61
6C A0 D2 F7 83 2F 6A 7F AC DD FB C0 D9 D6 17 5A
E7 AC 86 17 2D 43 F5 76 E6 AF 5B AA 80 DB 29 FC
07 9C B7 37 AA E6 CF 82 EA 69 AC 6D 00 5E 07 2D
41 FF 84 CA 47 77 2D FF 4A 08 C2 E2 9A 5D 69 A5
64 72 8B F5 66 9E D8 14 6A 9F DC 4E DB 5E 58 C9
62 14 0D 59 1F A6 BF 52 0B F0 88 92 6B 91 9F 79
71 61 6F C4 AA 4B 74 65 21 AC CE C8 E0 7B 9A 36
BA 71 81 76 18 A6 8C E1 23 17 CE ED 27 A2 7D 9C
ED 1F B9 FB A5 77 03 F7 D8 EE 18 DF 6B 3E 7A 5E
4A DD 80 27 02 65 00 13

about to call last of the absorb phase

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

10 11 12 13 14 15 16 17 1F 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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)

10 11 12 13 14 15 16 17 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

After Permutation

49 86 7B 4E 0D 7B A3 44 07 8E ED E9 BD 7E 84 21
67 9D ED 28 2A 0E 50 CE E8 F1 18 36 1C 08 75 95
A6 AF 48 A1 8A 74 56 4E 5B 76 26 E6 92 C5 5A A3
D6 F3 FB F0 30 6B 7E F0 D5 40 28 F7 AC F3 1F D1
0C F5 65 49 99 F6 06 65 37 67 53 91 28 41 71 90
76 AE 49 5C B0 77 E2 C6 0E C0 E1 37 4D B5 34 60
7F A4 2E 6A 94 30 F2 A5 D8 C7 1E 07 18 7B 61 2B
A0 3E 20 60 17 3C A8 32 FC 86 D4 7A 6D A7 58 07
4C E7 C6 07 B3 04 C0 79 E5 7F 93 EC B1 D4 C5 46
DA CD 8A CB F9 7D D2 A7 AE 18 2F 14 0F E9 8F 62
67 91 26 F7 34 9E 21 EB 4D DA 29 2D 7C 7A CE BD
1E EA E5 CC F7 63 28 42 ED F7 90 CC C5 06 B1 D1
0D 4E 82 71 D6 95 1F 7A

about to call last of the absorb phase

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

20 21 22 23 24 25 26 27 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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)

20 21 22 23 24 25 26 27 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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

After Permutation

E6 89 84 75 8E E8 3E 4B 3F 43 7C 58 62 5D A0 CD
E3 EE 6B 06 BF 30 F0 F6 3D FF 39 15 A5 51 8F C8
CC 5A E2 EB 09 BF BA 5E 88 31 00 E2 85 5A F8 E1
EF C5 60 86 33 1F 5F 5D 57 BF 55 D9 EF 05 E0 C9
84 36 57 9E AB FD 9B 77 60 57 CB 1E 58 C2 F5 8E
52 F8 A4 11 24 23 D3 6D C1 6F 75 BF 8E DD 2B 3F
2D 34 95 9F E4 D3 5D 65 85 76 C6 E4 6D 81 64 F7
CA 66 52 91 96 6F 76 A0 B3 E6 AA A7 E0 43 54 4A
40 C0 4B 36 A8 01 13 5D 2D EA C3 D5 F6 91 89 F7
79 C8 27 45 6B C0 28 34 C3 C3 57 C7 08 3E 52 23
74 38 84 DE E1 F1 99 3C 0A 51 E6 8C A1 69 8E 9B
9D 11 F7 CF AE 94 C5 DB C9 CD CC 5A AE B7 55 51
96 A5 93 9E 1D D0 06 51

Encoded n

03 01
Encoded L
00 01
Length of newX is <816>
newX is
01 08 2E A7 A0 60 1B 9C 5C B4 1E 46 9F 85 40 77
C1 E3 3A AC 94 D3 9C E4 61 63 42 9A BC AC FA 99
2B BC 49 86 7B 4E 0D 7B A3 44 07 8E ED E9 BD 7E
84 21 67 9D ED 28 2A 0E 50 CE E8 F1 18 36 1C 08
75 95 E6 89 84 75 8E E8 3E 4B 3F 43 7C 58 62 5D
A0 CD E3 EE 6B 06 BF 30 F0 F6 3D FF 39 15 A5 51
8F C8 03 01 00 01
Encoded N
01 60 50 61 72 61 6C 6C 65 6C 48 61 73 68
Encoded S
01 68 50 61 72 61 6C 6C 65 6C 20 44 61 74 61
bytepad data
01 A8 01 60 50 61 72 61 6C 6C 65 6C 48 61 73 68
01 68 50 61 72 61 6C 6C 65 6C 20 44 61 74 61 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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 60 50 61 72 61 6C 6C 65 6C 48 61 73 68
01 68 50 61 72 61 6C 6C 65 6C 20 44 61 74 61 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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 60 50 61 72 61 6C 6C 65 6C 48 61 73 68
01 68 50 61 72 61 6C 6C 65 6C 20 44 61 74 61 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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

9E 2F 09 BE D5 1D 75 A2 32 D2 14 95 32 4F 60 E3
26 E0 DF AE ED 09 D6 61 AF A8 94 67 BE B0 24 07
7A C2 88 B1 87 EA AF 06 C1 D6 B5 5C D2 8D 7D 80
4C 48 99 28 30 EF 3B FF 91 88 66 EB 08 BF EA 6F
0A 7B 05 76 7C 54 B7 B5 01 46 FE D2 37 24 55 2E
CE A3 89 3B 57 B2 20 A8 CD DC 04 9C 68 F9 FE EE
71 87 46 11 5D 35 EE D5 E4 72 2C 6C 9F B5 0B F7
43 B5 38 47 5C 57 AC 05 0B 86 83 CF 97 E1 AA 41
72 08 50 20 B3 E5 0C B5 5B BA 2E A8 7C 6D 18 A3
BB DC CB 35 A0 5F B0 04 4F 80 C3 DE 53 B4 42 38
75 D6 D0 8F 9E A9 A8 CC 72 D7 4D A3 F3 E0 06 05
B8 10 7B 0C F8 D3 75 8C 09 3C 60 57 55 A4 70 F3
43 BD 8F 4A 7C D9 DD 25

about to call last of the absorb phase

About to Absorb data

State (in bytes)

9E 2F 09 BE D5 1D 75 A2 32 D2 14 95 32 4F 60 E3
26 E0 DF AE ED 09 D6 61 AF A8 94 67 BE B0 24 07
7A C2 88 B1 87 EA AF 06 C1 D6 B5 5C D2 8D 7D 80
4C 48 99 28 30 EF 3B FF 91 88 66 EB 08 BF EA 6F
0A 7B 05 76 7C 54 B7 B5 01 46 FE D2 37 24 55 2E
CE A3 89 3B 57 B2 20 A8 CD DC 04 9C 68 F9 FE EE
71 87 46 11 5D 35 EE D5 E4 72 2C 6C 9F B5 0B F7
43 B5 38 47 5C 57 AC 05 0B 86 83 CF 97 E1 AA 41
72 08 50 20 B3 E5 0C B5 5B BA 2E A8 7C 6D 18 A3
BB DC CB 35 A0 5F B0 04 4F 80 C3 DE 53 B4 42 38
75 D6 D0 8F 9E A9 A8 CC 72 D7 4D A3 F3 E0 06 05

B8 10 7B 0C F8 D3 75 8C 09 3C 60 57 55 A4 70 F3
43 BD 8F 4A 7C D9 DD 25

Data to be absorbed

01 08 2E A7 A0 60 1B 9C 5C B4 1E 46 9F 85 40 77
C1 E3 3A AC 94 D3 9C E4 61 63 42 9A BC AC FA 99
2B BC 49 86 7B 4E 0D 7B A3 44 07 8E ED E9 BD 7E
84 21 67 9D ED 28 2A 0E 50 CE E8 F1 18 36 1C 08
75 95 E6 89 84 75 8E E8 3E 4B 3F 43 7C 58 62 5D
A0 CD E3 EE 6B 06 BF 30 F0 F6 3D FF 39 15 A5 51
8F C8 03 01 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 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)

9F 27 27 19 75 7D 6E 3E 6E 66 0A D3 AD CA 20 94
E7 03 E5 02 79 DA 4A 85 CE CB D6 FD 02 1C DE 9E
51 7E C1 37 FC A4 A2 7D 62 92 B2 D2 3F 64 C0 FE
C8 69 FE B5 DD C7 11 F1 C1 46 8E 1A 10 89 F6 67
7F EE E3 FF F8 21 39 5D 3F 0D C1 91 4B 7C 37 73
6E 6E 6A D5 3C B4 9F 98 3D 2A 39 63 51 EC 5B BF
FE 4F 45 10 5D 34 EA D5 E4 72 2C 6C 9F B5 0B F7
43 B5 38 47 5C 57 AC 05 0B 86 83 CF 97 E1 AA 41
72 08 50 20 B3 E5 0C B5 5B BA 2E A8 7C 6D 18 A3
BB DC CB 35 A0 5F B0 04 4F 80 C3 DE 53 B4 42 38
75 D6 D0 8F 9E A9 A8 4C 72 D7 4D A3 F3 E0 06 05
B8 10 7B 0C F8 D3 75 8C 09 3C 60 57 55 A4 70 F3
43 BD 8F 4A 7C D9 DD 25

After Permutation

EA 2A 79 31 40 82 0F 7A 12 8B 8E B7 0A 94 39 F9
32 57 C6 E6 E7 9B 4A 54 0D 29 1D 6D AE 70 98 D7
44 10 63 9C 70 E5 B7 25 5B E1 1D CC B6 03 1F D3
AE 17 24 13 C9 7B CD FC 2F A8 50 44 45 84 48 30
28 72 8A BC 6D 77 FF 37 E4 66 4E B7 75 3C DF 94
9E 53 92 20 2C 80 7E E9 3A 9B 82 A4 5B F3 F4 AC
D5 BD 02 37 E0 61 D3 62 D9 70 CB 4C 3B 31 9E FE
54 2C 42 92 6F 2F D4 2B C1 C1 3E 47 DE 7E FA B7
FB 77 78 94 49 41 CE 82 14 87 19 93 DF B1 34 33
7C 47 E1 24 CD 80 50 E8 14 2E 8E A1 C4 15 12 82
7D 04 89 23 40 72 23 D7 E0 5B 92 9E 50 86 52 C4
32 87 91 BA 07 0C 08 2B 4F 9B 79 3C EF 09 68 83
2C 2E 56 7D 26 B1 2E BF

Outval is

EA 2A 79 31 40 82 0F 7A 12 8B 8E B7 0A 94 39 F9
32 57 C6 E6 E7 9B 4A 54 0D 29 1D 6D AE 70 98 D7

==========

ParallelHashXOF:
Sample #3

Security Strength: 128-bits

Length of data is 576-bits
Data is
00 01 02 03 04 05 06 07 08 09 0A 0B 10 11 12 13
14 15 16 17 18 19 1A 1B 20 21 22 23 24 25 26 27
28 29 2A 2B 30 31 32 33 34 35 36 37 38 39 3A 3B
40 41 42 43 44 45 46 47 48 49 4A 4B 50 51 52 53
54 55 56 57 58 59 5A 5B

Block size (B) is 12

Requested output length is 256-bits

S (as a character string) is
"Parallel Data"

Encoded B
01 0C
about to call last of the absorb phase

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
00 01 02 03 04 05 06 07 08 09 0A 0B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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)
00 01 02 03 04 05 06 07 08 09 0A 0B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

After Permutation
15 BC 36 A4 F1 17 F4 FD AB 53 64 D5 DA 67 8C 2E
35 CE 09 50 A5 7C 1A 23 5E CC 83 0E CE 29 EC EE
44 6D A6 38 8D 23 93 1B 8A 43 4C 67 D1 2C 0A 57
1C 3D 34 0A 65 63 5D A0 B9 2E 95 76 78 D9 FF CA
FE EB 86 54 75 0E 90 0F 81 F8 39 ED A9 5E 50 8D
EC B1 40 05 FA D8 C9 60 CB 45 2D 90 0D 25 62 E0
A1 74 14 F8 A0 8F 78 01 98 E7 23 85 67 FE 60 DF
D6 85 75 DE 62 3D 69 44 E6 37 00 92 C7 76 0A D5
E8 47 D7 98 F4 70 07 7B CE 2D 50 D4 37 67 A9 E9
2D 71 7C 42 D6 79 5D 17 96 45 DF 3E FD D5 30 F6
C9 C9 F8 04 C8 18 7D 71 70 5F 80 D6 8A F4 F7 AB
3D 89 1D 91 59 A4 3B C7 34 C3 94 1A D1 59 D5 4F
98 0E 2C 81 C7 09 F6 66
about to call last of the absorb phase

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
10 11 12 13 14 15 16 17 18 19 1A 1B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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)

10 11 12 13 14 15 16 17 18 19 1A 1B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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

After Permutation

FC 59 81 3E E8 4F 8E B9 B6 D7 4A 4A 2D 05 BB 8D
1E D7 4A 72 D2 81 F9 6A D1 F7 A0 6B FA 71 C2 45
0A 39 39 B5 19 21 A8 9A 1B 39 AD 0B 86 34 3A EF
15 87 46 23 68 22 9C D8 A9 1F 9B 74 9E 44 39 9D
76 C9 B6 B8 7E 13 42 DF 34 5B 3A 67 3B 57 AF 55
7D A3 FF 16 C4 CF 23 DF 39 6E 8E 2D D4 7F 07 79
99 00 E7 90 3A B7 D1 15 19 36 88 D9 F4 A4 C7 2F
C8 42 35 F0 D0 66 64 45 3A 55 EF 54 45 7E A1 4D
CD E4 26 E2 E6 89 A6 43 36 4B 5B 8F 5A B6 C2 91
27 6E E6 D1 13 B0 42 4F 4E FA 8B F0 3D 46 1F 28
0A 88 C6 C2 67 48 04 3D 2A D4 49 61 CB C7 DD 6B
A4 8C A3 B1 01 88 ED 18 F5 11 DF C8 B4 61 18 B3
83 79 FC 0C 99 C4 91 96

about to call last of the absorb phase

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

Data to be absorbed

20 21 22 23 24 25 26 27 28 29 2A 2B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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)

20 21 22 23 24 25 26 27 28 29 2A 2B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

After Permutation

E3 12 64 13 EC F2 E8 45 43 B2 85 80 32 FD 71 2C
26 6C 20 28 B1 F0 59 02 58 1B 40 14 D1 9A 15 CF
99 1D 82 F6 30 C7 26 2B 49 D8 54 C0 CC EB 8F D5
B0 7C 5D C6 C2 82 6A A4 E8 56 57 7C 9B 8E 3C B8
FC DA 32 BE AF 3C 07 5B 44 BD 64 C4 55 D6 00 23
81 95 CD BC 6B 6B 52 42 8A A6 3B F2 2C C1 49 DD
D9 8F 3B E4 EE 46 1E 8C E1 B3 1D C2 27 A0 76 35
A7 EE 12 B1 43 06 A2 AD 87 A0 17 DD A0 59 7B A9
15 E8 EF 69 CF F2 42 2D D1 AC 8B 90 22 CD 29 BA
0E B9 DD 64 37 85 17 AF EB E5 E7 1B 7E 09 57 CC
4F 63 84 3B 1F 2E 1D D5 38 A2 7C 7C 19 6A D2 B3
FF 15 33 0A 91 3C 69 B2 86 B9 8B 45 F5 04 1E 87
5F 34 D3 32 46 3B 4D CF

about to call last of the absorb phase

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

```
30 31 32 33 34 35 36 37 38 39 3A 3B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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)

```
30 31 32 33 34 35 36 37 38 39 3A 3B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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
```

After Permutation

```
F3 38 F2 D9 E9 91 CD 5E 41 E9 96 87 3B CF 6A F6
B3 C0 8B C0 38 6E E2 24 20 27 BC BD 58 5A 9D 32
21 30 AB C8 AC 83 4D B0 F7 5D 88 AC E9 42 EA 71
9A 13 2D 30 4E 40 E8 09 0C FB F1 24 8B 81 B6 9F
92 A8 32 01 4A B4 EA 5D 5E FF E0 91 6E 0C FF 93
E0 82 EF D8 49 BB 4D CA 63 AD 3F B7 29 0F BF F3
```

18 D3 22 59 3F EA B4 2D EC E8 39 B2 38 81 E8 32
B2 DB 80 04 C6 89 E4 47 AF 85 73 10 D3 6A 5D 61
99 23 7F 8D 51 4B 50 31 51 1D DE BB 6F 12 21 71
FF 06 81 3A 48 2D 24 B5 A4 34 1A 4E C3 58 33 D1
0D 77 82 4A 97 66 45 45 8D 91 1D 60 7A 2A 24 0C
CF 79 B0 42 3E 7F A4 B8 52 2C 14 E7 92 C7 7C 0D
C7 AD CA 84 44 F7 DC 87

about to call last of the absorb phase

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

40 41 42 43 44 45 46 47 48 49 4A 4B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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)

40 41 42 43 44 45 46 47 48 49 4A 4B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

After Permutation
FA B1 A0 DA A8 A3 52 8C 7F BA 60 C8 57 47 91 87
60 E1 46 69 F0 2D 96 F9 C5 3D 71 E9 8A A5 CD D5
E8 0B 15 F6 0E 7E 00 E1 5B 81 44 F8 60 50 D2 BA
3A D6 28 01 DE CD 95 DF 5A CF 14 FA 2E 80 DD 98
08 BE F8 FD 07 5A 69 4A AA CE 90 DB DB B5 52 92
59 B8 88 44 91 10 BA 3E CD 1C 37 DD 69 19 9E 72
24 1F DA AF 00 A8 8B A9 76 C3 0D 94 FF F2 10 98
82 7D DC 97 1B D9 DE F7 A1 49 81 B3 C9 3C B9 A4
34 2E 7B 25 35 99 A3 1F 5B 2F F1 5F E3 EC DA B8
D4 17 AC 91 12 3B 37 48 6C 42 2D 2F 3D 4F 82 A3
13 B2 D6 4B 0E 9C A0 54 29 18 36 5C 47 BA FD 85
57 1D 5B 9C 75 94 8B 11 F0 81 BD D9 20 3A 2A 5D
77 4F E8 B5 05 C8 71 82
about to call last of the absorb phase

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
50 51 52 53 54 55 56 57 58 59 5A 5B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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)
50 51 52 53 54 55 56 57 58 59 5A 5B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

After Permutation
60 A1 F3 3D FA FE 48 E4 83 09 0D 46 A0 53 34 B3
44 BB 8F AF 3A 11 C9 3E 2A 0E C7 CC CC FF 28 E5
CF 09 91 6E CC 40 B3 D6 9D 9E 4E EC 4A FB 0E DF
F0 5D FF 1E F4 BF 2C 1B 89 55 28 C0 8C 1B BB 26
6A A5 B1 7A 71 4C D0 46 E2 1D C8 8E 82 13 67 33
6C 10 B4 F0 03 FD E4 D8 1F A0 5D 45 E3 DE 61 17
39 53 42 08 5D 35 60 1D A1 11 4F 13 13 E0 C5 3A
5A D6 2B EE 10 DE 2F F8 A9 F3 5C 29 A0 43 28 03
60 93 C0 47 30 76 87 0E 4F A9 F6 62 08 69 41 D5
95 9B B4 FE 7D 07 5A 4C 43 45 A2 F5 A3 68 3A 76
FD 01 80 F8 CE E2 AC CC 77 25 C3 99 F4 CC 93 D6
C5 50 BA 08 55 42 94 0F 08 B6 81 68 D2 63 2C F6
52 FE 7B 83 FC 69 98 9D
Encoded n
06 01
Encoded L
00 01
Length of newX is <1584>
newX is
01 0C 15 BC 36 A4 F1 17 F4 FD AB 53 64 D5 DA 67
8C 2E 35 CE 09 50 A5 7C 1A 23 5E CC 83 0E CE 29
EC EE FC 59 81 3E E8 4F 8E B9 B6 D7 4A 4A 2D 05
BB 8D 1E D7 4A 72 D2 81 F9 6A D1 F7 A0 6B FA 71
C2 45 E3 12 64 13 EC F2 E8 45 43 B2 85 80 32 FD
71 2C 26 6C 20 28 B1 F0 59 02 58 1B 40 14 D1 9A
15 CF F3 38 F2 D9 E9 91 CD 5E 41 E9 96 87 3B CF
6A F6 B3 C0 8B C0 38 6E E2 24 20 27 BC BD 58 5A
9D 32 FA B1 A0 DA A8 A3 52 8C 7F BA 60 C8 57 47
91 87 60 E1 46 69 F0 2D 96 F9 C5 3D 71 E9 8A A5
CD D5 60 A1 F3 3D FA FE 48 E4 83 09 0D 46 A0 53
34 B3 44 BB 8F AF 3A 11 C9 3E 2A 0E C7 CC CC FF
28 E5 06 01 00 01
Encoded N
01 60 50 61 72 61 6C 6C 65 6C 48 61 73 68
Encoded S
01 68 50 61 72 61 6C 6C 65 6C 20 44 61 74 61
bytepad data
01 A8 01 60 50 61 72 61 6C 6C 65 6C 48 61 73 68
01 68 50 61 72 61 6C 6C 65 6C 20 44 61 74 61 00

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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 60 50 61 72 61 6C 6C 65 6C 48 61 73 68
01 68 50 61 72 61 6C 6C 65 6C 20 44 61 74 61 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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 60 50 61 72 61 6C 6C 65 6C 48 61 73 68
01 68 50 61 72 61 6C 6C 65 6C 20 44 61 74 61 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

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
9E 2F 09 BE D5 1D 75 A2 32 D2 14 95 32 4F 60 E3
26 E0 DF AE ED 09 D6 61 AF A8 94 67 BE B0 24 07
7A C2 88 B1 87 EA AF 06 C1 D6 B5 5C D2 8D 7D 80
4C 48 99 28 30 EF 3B FF 91 88 66 EB 08 BF EA 6F
0A 7B 05 76 7C 54 B7 B5 01 46 FE D2 37 24 55 2E
CE A3 89 3B 57 B2 20 A8 CD DC 04 9C 68 F9 FE EE
71 87 46 11 5D 35 EE D5 E4 72 2C 6C 9F B5 0B F7
43 B5 38 47 5C 57 AC 05 0B 86 83 CF 97 E1 AA 41
72 08 50 20 B3 E5 0C B5 5B BA 2E A8 7C 6D 18 A3
BB DC CB 35 A0 5F B0 04 4F 80 C3 DE 53 B4 42 38
75 D6 D0 8F 9E A9 A8 CC 72 D7 4D A3 F3 E0 06 05
B8 10 7B 0C F8 D3 75 8C 09 3C 60 57 55 A4 70 F3
43 BD 8F 4A 7C D9 DD 25

About to Absorb data
State (in bytes)
9E 2F 09 BE D5 1D 75 A2 32 D2 14 95 32 4F 60 E3
26 E0 DF AE ED 09 D6 61 AF A8 94 67 BE B0 24 07
7A C2 88 B1 87 EA AF 06 C1 D6 B5 5C D2 8D 7D 80
4C 48 99 28 30 EF 3B FF 91 88 66 EB 08 BF EA 6F
0A 7B 05 76 7C 54 B7 B5 01 46 FE D2 37 24 55 2E
CE A3 89 3B 57 B2 20 A8 CD DC 04 9C 68 F9 FE EE
71 87 46 11 5D 35 EE D5 E4 72 2C 6C 9F B5 0B F7
43 B5 38 47 5C 57 AC 05 0B 86 83 CF 97 E1 AA 41
72 08 50 20 B3 E5 0C B5 5B BA 2E A8 7C 6D 18 A3
BB DC CB 35 A0 5F B0 04 4F 80 C3 DE 53 B4 42 38
75 D6 D0 8F 9E A9 A8 CC 72 D7 4D A3 F3 E0 06 05
B8 10 7B 0C F8 D3 75 8C 09 3C 60 57 55 A4 70 F3
43 BD 8F 4A 7C D9 DD 25
Data to be absorbed
01 0C 15 BC 36 A4 F1 17 F4 FD AB 53 64 D5 DA 67
8C 2E 35 CE 09 50 A5 7C 1A 23 5E CC 83 0E CE 29
EC EE FC 59 81 3E E8 4F 8E B9 B6 D7 4A 4A 2D 05
BB 8D 1E D7 4A 72 D2 81 F9 6A D1 F7 A0 6B FA 71
C2 45 E3 12 64 13 EC F2 E8 45 43 B2 85 80 32 FD
71 2C 26 6C 20 28 B1 F0 59 02 58 1B 40 14 D1 9A
15 CF F3 38 F2 D9 E9 91 CD 5E 41 E9 96 87 3B CF
6A F6 B3 C0 8B C0 38 6E E2 24 20 27 BC BD 58 5A
9D 32 FA B1 A0 DA A8 A3 52 8C 7F BA 60 C8 57 47
91 87 60 E1 46 69 F0 2D 96 F9 C5 3D 71 E9 8A A5
CD D5 60 A1 F3 3D FA FE 00 00 00 00 00 00 00 00
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)
9F 23 1C 02 E3 B9 84 B5 C6 2F BF C6 56 9A BA 84
AA CE EA 60 E4 59 73 1D B5 8B CA AB 3D BE EA 2E
96 2C 74 E8 06 D4 47 49 4F 6F 03 8B 98 C7 50 85

F7 C5 87 FF 7A 9D E9 7E 68 E2 B7 1C A8 D4 10 1E
C8 3E E6 64 18 47 5B 47 E9 03 BD 60 B2 A4 67 D3
BF 8F AF 57 77 9A 91 58 94 DE 5C 87 28 ED 2F 74
64 48 B5 29 AF EC 07 44 29 2C 6D 85 09 32 30 38
29 43 8B 87 D7 97 94 6B E9 A2 A3 E8 2B 5C F2 1B
EF 3A AA 91 13 3F A4 16 09 36 51 12 1C A5 4F E4
2A 5B AB D4 E6 36 40 29 D9 79 06 E3 22 5D C8 9D
B8 03 B0 2E 6D 94 52 32 72 D7 4D A3 F3 E0 06 05
B8 10 7B 0C F8 D3 75 8C 09 3C 60 57 55 A4 70 F3
43 BD 8F 4A 7C D9 DD 25

After Permutation
61 C6 F7 78 46 ED 4F 16 EA 62 6D 73 89 24 B6 07
80 66 45 2B CD 85 5D 92 44 A6 69 F9 BB 53 C7 88
C7 1E 70 30 51 77 34 9C DA E2 6F AF 51 EE DC 66
D9 95 1A B9 34 C2 C1 F5 9A 78 EB 23 75 86 24 FC
D0 AB C4 53 62 1E D1 4E D5 DD 6D E8 80 A8 DF 72
BC 57 8A A6 26 D9 98 6C AF E0 CF 5B 5E 18 23 52
0D 11 E4 D4 0F 6C A4 D7 22 94 29 47 44 3F 9E 8C
39 51 56 5A CD 35 0E DA 92 55 85 6B C9 D3 E9 0A
CD 98 4D 01 E4 00 AC 2C 63 2E D3 F8 CF 18 13 A9
80 1D 8B B2 17 14 5E 18 18 B8 11 89 62 C2 D6 CB
3A A1 64 1D 4F E9 51 BB 39 C1 AA 33 47 9A DB AB
67 2B C4 25 B4 83 65 2A 16 3B F9 C3 51 76 01 4C
E2 F3 2F 8C 83 5D A5 CA
about to call last of the absorb phase

About to Absorb data
State (in bytes)
61 C6 F7 78 46 ED 4F 16 EA 62 6D 73 89 24 B6 07
80 66 45 2B CD 85 5D 92 44 A6 69 F9 BB 53 C7 88
C7 1E 70 30 51 77 34 9C DA E2 6F AF 51 EE DC 66
D9 95 1A B9 34 C2 C1 F5 9A 78 EB 23 75 86 24 FC
D0 AB C4 53 62 1E D1 4E D5 DD 6D E8 80 A8 DF 72
BC 57 8A A6 26 D9 98 6C AF E0 CF 5B 5E 18 23 52
0D 11 E4 D4 0F 6C A4 D7 22 94 29 47 44 3F 9E 8C
39 51 56 5A CD 35 0E DA 92 55 85 6B C9 D3 E9 0A
CD 98 4D 01 E4 00 AC 2C 63 2E D3 F8 CF 18 13 A9
80 1D 8B B2 17 14 5E 18 18 B8 11 89 62 C2 D6 CB
3A A1 64 1D 4F E9 51 BB 39 C1 AA 33 47 9A DB AB
67 2B C4 25 B4 83 65 2A 16 3B F9 C3 51 76 01 4C
E2 F3 2F 8C 83 5D A5 CA
Data to be absorbed
48 E4 83 09 0D 46 A0 53 34 B3 44 BB 8F AF 3A 11
C9 3E 2A 0E C7 CC CC FF 28 E5 06 01 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 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)

29 22 74 71 4B AB EF 45 DE D1 29 C8 06 8B 8C 16
49 58 6F 25 0A 49 91 6D 6C 43 6F F8 BB 52 C3 88
C7 1E 70 30 51 77 34 9C DA E2 6F AF 51 EE DC 66
D9 95 1A B9 34 C2 C1 F5 9A 78 EB 23 75 86 24 FC
D0 AB C4 53 62 1E D1 4E D5 DD 6D E8 80 A8 DF 72
BC 57 8A A6 26 D9 98 6C AF E0 CF 5B 5E 18 23 52
0D 11 E4 D4 0F 6C A4 D7 22 94 29 47 44 3F 9E 8C
39 51 56 5A CD 35 0E DA 92 55 85 6B C9 D3 E9 0A
CD 98 4D 01 E4 00 AC 2C 63 2E D3 F8 CF 18 13 A9
80 1D 8B B2 17 14 5E 18 18 B8 11 89 62 C2 D6 CB
3A A1 64 1D 4F E9 51 3B 39 C1 AA 33 47 9A DB AB
67 2B C4 25 B4 83 65 2A 16 3B F9 C3 51 76 01 4C
E2 F3 2F 8C 83 5D A5 CA

After Permutation

01 27 AD 97 72 AB 90 46 91 98 7F CC 4A 24 88 8F
34 1F A0 DB 21 45 E8 72 D4 EF D2 55 37 66 02 F0
13 C7 39 E6 A3 86 14 62 86 00 B3 C3 36 E7 A6 2D
51 1E 31 CC 41 FD 04 5A BB 45 47 B4 B5 D0 EF DD
45 F8 A3 78 2E C0 0F 22 DF FE 31 A9 73 91 EB 8C
BB FE 5D 8F 59 BA 15 3A 10 C7 8E 7C 6F F5 F9 9D
0A A7 13 E0 78 86 6E 30 76 93 56 7D 99 43 71 EC
DF 1D A0 63 23 C1 41 7A 4C 05 B9 0E 16 3C AD 4C
AB B8 58 4B E4 E8 D4 57 2E 3E 5D 2C 97 A0 E3 D3
3D 96 50 90 E2 E0 F5 BA 2E 64 33 3F 19 EC 12 FA
57 6F BB D7 E0 C8 98 AB C6 80 38 D2 12 35 2C 1F
BE FD A0 43 19 88 83 55 88 D0 EC 16 2A B3 94 AE
1F B7 AC 33 21 0E C6 A3

Outval is

01 27 AD 97 72 AB 90 46 91 98 7F CC 4A 24 88 8F
34 1F A0 DB 21 45 E8 72 D4 EF D2 55 37 66 02 F0

==========

ParallelHashXOF:

Sample #1

Security Strength: 256-bits

Length of data is 192-bits

Data is

00 01 02 03 04 05 06 07 10 11 12 13 14 15 16 17
20 21 22 23 24 25 26 27

Block size (B) is 8

Requested output length is 512-bits

S (as a character string) is
"(null)"

Encoded B
01 08
about to call last of the absorb phase

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
00 01 02 03 04 05 06 07 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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)
00 01 02 03 04 05 06 07 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

After Permutation
B4 4D AE 93 F2 36 0C 49 14 FA 99 9F 3A ED 53 90
1D 47 A1 B6 14 10 9E 4B FB E8 A5 95 D5 DD 50 58
14 2C 63 B0 B5 48 E2 96 C3 7F 89 72 67 7B 7F AF
0C 22 BF 85 BF 9C 89 1C 1B 91 F6 91 84 D8 B6 DE
9A 32 B1 5E 28 99 12 CA 73 1A 12 5C 15 FA 69 40
3C B3 11 58 F7 D6 15 9A E3 E2 07 78 B5 9A 6F 43
EE 3E 27 34 7D 5E C2 38 B7 C3 A2 98 12 40 64 87
96 2C 23 9A 40 BC F9 C4 1E B2 85 CA A4 CD 27 0E
F7 CC AB 33 46 05 21 6D 20 5F 44 9F 30 B4 BF 3D
53 06 6C 1B 81 C0 6D 08 10 2C F5 31 44 51 CD C0
A1 E1 DF F9 17 72 A4 E0 3D 3A CF 72 65 7C 74 D7
32 E3 90 95 34 3B D4 62 CF EC 5F 7D 8E B2 17 79
6E 07 C6 B2 61 05 32 B7
about to call last of the absorb phase

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
10 11 12 13 14 15 16 17 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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)
10 11 12 13 14 15 16 17 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

After Permutation

05 AE 49 D9 17 05 EE 53 5B E9 AF 26 8F 66 E6 C2
A2 2A 89 BE 4A EC DF A1 F6 6F 4D 04 97 3F 29 FB
DC 05 E8 C3 01 0B E3 22 C3 07 77 CA 0D 8C A6 67
A3 03 82 B6 9A 49 A1 57 27 4A A4 62 D5 9C C8 E1
87 5E 0C C3 20 45 C0 92 04 AA C2 A6 AF 02 D3 AA
8C 28 C9 49 F9 C6 09 31 89 A0 7F 27 DE 0D B3 02
E5 4D E1 AE 28 FB D4 05 D0 38 30 02 7B AD 36 4C
4A 93 EE AE 1B BD 5B F5 86 7F EF 6F 05 71 0A 9E
CA FA A2 20 54 A6 46 57 43 81 C9 C2 D8 2B F5 50
2C 4A 6E D5 6E F4 68 BF 6C 12 5C EF 71 34 73 13
E0 6C A7 2F F2 BE 0D 61 41 77 20 D6 C5 13 28 A3
E0 1A 87 1D DF B7 75 94 47 0E 83 E9 36 0A 77 1E
87 47 2F 45 E9 28 58 CA

about to call last of the absorb phase

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

Data to be absorbed

20 21 22 23 24 25 26 27 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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)

20 21 22 23 24 25 26 27 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

After Permutation

81 BD FC 2D 48 E0 97 89 68 B3 1C E7 85 FE 36 C7
CC 6B 41 30 23 4F D6 7C 51 DA 5D FB 7C 81 68 7A
28 06 12 3D 2D ED 47 E4 CD E9 61 A4 48 EA 8D 5E
91 B3 96 2E EA 48 BD B7 F2 C8 94 FA 52 00 D3 AC
06 6A C1 E5 25 12 DC 6B B6 8F 42 3E F4 F4 C9 4E
E5 3D DF E1 AB A1 DC 26 02 21 0B 4D 99 88 52 4C
06 AC 85 74 C7 65 23 F9 A6 69 31 16 9C 8A 02 6E
C3 A9 83 1D 65 E6 46 C7 9D FF 99 20 D1 A6 D6 75
F8 4B A7 20 38 CA 2E ED C1 69 B2 42 DA 66 2B A8
26 60 C7 34 9E 3C 1F 15 95 47 C5 AC C0 B5 4A D7
B7 C8 7B F8 69 09 3A FB D4 CA 2C 4D 1E 7B 1C 9D
5C 31 C7 BC CB C4 C4 9C 56 4E 6C 2B 07 49 2A 6E
01 97 01 1A EE 27 74 BB

Encoded n

03 01

Encoded L

00 01

Length of newX is <1584>

newX is

01 08 B4 4D AE 93 F2 36 0C 49 14 FA 99 9F 3A ED
53 90 1D 47 A1 B6 14 10 9E 4B FB E8 A5 95 D5 DD
50 58 14 2C 63 B0 B5 48 E2 96 C3 7F 89 72 67 7B
7F AF 0C 22 BF 85 BF 9C 89 1C 1B 91 F6 91 84 D8
B6 DE 05 AE 49 D9 17 05 EE 53 5B E9 AF 26 8F 66
E6 C2 A2 2A 89 BE 4A EC DF A1 F6 6F 4D 04 97 3F
29 FB DC 05 E8 C3 01 0B E3 22 C3 07 77 CA 0D 8C
A6 67 A3 03 82 B6 9A 49 A1 57 27 4A A4 62 D5 9C
C8 E1 81 BD FC 2D 48 E0 97 89 68 B3 1C E7 85 FE
36 C7 CC 6B 41 30 23 4F D6 7C 51 DA 5D FB 7C 81

68 7A 28 06 12 3D 2D ED 47 E4 CD E9 61 A4 48 EA
8D 5E 91 B3 96 2E EA 48 BD B7 F2 C8 94 FA 52 00
D3 AC 03 01 00 01

Encoded N

01 60 50 61 72 61 6C 6C 65 6C 48 61 73 68

Encoded S

01 00

bytepad data

01 88 01 60 50 61 72 61 6C 6C 65 6C 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

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

Data to be absorbed

01 88 01 60 50 61 72 61 6C 6C 65 6C 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 00 00 00 00 00

Xor'd state (in bytes)

01 88 01 60 50 61 72 61 6C 6C 65 6C 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 00 00 00 00 00
00 00 00 00 00 00 00

After Permutation

70 BA DC 22 9E 10 00 1C 0C BA 38 8D 6F F6 80 B3
F2 FC B8 27 FF EC 61 CA B2 E2 E9 27 0C 6C A2 77
B8 CE F8 C8 09 0D 32 9D 77 C6 16 94 CD 1C 4F 50
3C 5D B2 75 DF 70 9B 0A EC 08 53 98 F7 2B E0 0C
D0 94 E0 34 BD 8C 9F C4 EC A9 81 1B C2 EC 08 5A
82 2E 07 9E BB 39 EC D8 A0 B1 12 77 73 36 EB 5A
A3 A1 F1 ED 17 6B B1 95 B3 71 AC 52 0F 04 CA C1
16 7A B7 0C AD 33 4F 00 06 F3 1A 10 0C 5D B1 A5
AE C0 6F 6A 1C DA 33 5A C0 A6 25 D5 F5 25 8D E9
79 FE F3 96 07 00 A5 DE 64 D8 E6 F7 95 4E D1 93
87 EB 7B AC A9 46 9C B9 B3 E3 3B 17 50 D2 82 5D
1C CD 1E 2D 97 97 A5 B8 BB 1D 1A C1 55 F7 8F 29
17 A1 2D 3B 21 3D 23 33

About to Absorb data

State (in bytes)

70 BA DC 22 9E 10 00 1C 0C BA 38 8D 6F F6 80 B3
F2 FC B8 27 FF EC 61 CA B2 E2 E9 27 0C 6C A2 77
B8 CE F8 C8 09 0D 32 9D 77 C6 16 94 CD 1C 4F 50
3C 5D B2 75 DF 70 9B 0A EC 08 53 98 F7 2B E0 0C
D0 94 E0 34 BD 8C 9F C4 EC A9 81 1B C2 EC 08 5A
82 2E 07 9E BB 39 EC D8 A0 B1 12 77 73 36 EB 5A
A3 A1 F1 ED 17 6B B1 95 B3 71 AC 52 0F 04 CA C1
16 7A B7 0C AD 33 4F 00 06 F3 1A 10 0C 5D B1 A5
AE C0 6F 6A 1C DA 33 5A C0 A6 25 D5 F5 25 8D E9
79 FE F3 96 07 00 A5 DE 64 D8 E6 F7 95 4E D1 93
87 EB 7B AC A9 46 9C B9 B3 E3 3B 17 50 D2 82 5D
1C CD 1E 2D 97 97 A5 B8 BB 1D 1A C1 55 F7 8F 29
17 A1 2D 3B 21 3D 23 33

Data to be absorbed

01 08 B4 4D AE 93 F2 36 0C 49 14 FA 99 9F 3A ED
53 90 1D 47 A1 B6 14 10 9E 4B FB E8 A5 95 D5 DD
50 58 14 2C 63 B0 B5 48 E2 96 C3 7F 89 72 67 7B
7F AF 0C 22 BF 85 BF 9C 89 1C 1B 91 F6 91 84 D8
B6 DE 05 AE 49 D9 17 05 EE 53 5B E9 AF 26 8F 66
E6 C2 A2 2A 89 BE 4A EC DF A1 F6 6F 4D 04 97 3F
29 FB DC 05 E8 C3 01 0B E3 22 C3 07 77 CA 0D 8C
A6 67 A3 03 82 B6 9A 49 A1 57 27 4A A4 62 D5 9C
C8 E1 81 BD FC 2D 48 E0 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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)

71 B2 68 6F 30 83 F2 2A 00 F3 2C 77 F6 69 BA 5E
A1 6C A5 60 5E 5A 75 DA 2C A9 12 CF A9 F9 77 AA
E8 96 EC E4 6A BD 87 D5 95 50 D5 EB 44 6E 28 2B
43 F2 BE 57 60 F5 24 96 65 14 48 09 01 BA 64 D4
66 4A E5 9A F4 55 88 C1 02 FA DA F2 6D CA 87 3C
64 EC A5 B4 32 87 A6 34 7F 10 E4 18 3E 32 7C 65
8A 5A 2D E8 FF A8 B0 9E 50 53 6F 55 78 CE C7 4D
B0 1D 14 0F 2F 85 D5 49 A7 A4 3D 5A A8 3F 64 39
66 21 EE D7 E0 F7 7B BA C0 A6 25 D5 F5 25 8D E9
79 FE F3 96 07 00 A5 DE 64 D8 E6 F7 95 4E D1 93
87 EB 7B AC A9 46 9C B9 B3 E3 3B 17 50 D2 82 5D
1C CD 1E 2D 97 97 A5 B8 BB 1D 1A C1 55 F7 8F 29
17 A1 2D 3B 21 3D 23 33

After Permutation

74 9D 13 B1 82 99 16 82 E5 1D 05 18 0E 40 50 15
28 8C 0B 7E 86 6E B0 F6 AD 44 F1 22 D6 A9 E1 A9
FE 31 AB 60 D5 8F 2B 32 52 B3 51 CD 59 BB B9 87
33 A7 D0 47 98 1C C1 F2 27 7E B8 19 CD 47 92 71
09 9D 05 31 E4 FF 54 3E 2A EC E4 62 71 71 E9 F0
E5 E2 6B C5 20 35 F1 D4 B3 2C 32 CE 91 71 35 84
30 C6 0F 52 BC 15 C0 CB B9 0C 2B BA A9 9A 50 B2
FA 25 F6 AF CE 38 92 17 59 E6 5A 93 98 82 E3 50
6C 68 E1 D2 A2 30 DA 10 47 E6 3E E3 D9 44 6D 82
E5 FD B6 E2 4A 1A B7 DF 0E D6 26 CD 69 B2 7A EF
FA 22 6E 1F AF 34 39 02 A8 B0 38 08 DE 5A FF D3
E1 E1 87 D2 15 E8 A8 8B 33 48 58 B0 09 C3 8E FC
0D 0B 46 CA 50 59 38 22

about to call last of the absorb phase

About to Absorb data

State (in bytes)

74 9D 13 B1 82 99 16 82 E5 1D 05 18 0E 40 50 15
28 8C 0B 7E 86 6E B0 F6 AD 44 F1 22 D6 A9 E1 A9
FE 31 AB 60 D5 8F 2B 32 52 B3 51 CD 59 BB B9 87
33 A7 D0 47 98 1C C1 F2 27 7E B8 19 CD 47 92 71
09 9D 05 31 E4 FF 54 3E 2A EC E4 62 71 71 E9 F0
E5 E2 6B C5 20 35 F1 D4 B3 2C 32 CE 91 71 35 84
30 C6 0F 52 BC 15 C0 CB B9 0C 2B BA A9 9A 50 B2
FA 25 F6 AF CE 38 92 17 59 E6 5A 93 98 82 E3 50
6C 68 E1 D2 A2 30 DA 10 47 E6 3E E3 D9 44 6D 82
E5 FD B6 E2 4A 1A B7 DF 0E D6 26 CD 69 B2 7A EF
FA 22 6E 1F AF 34 39 02 A8 B0 38 08 DE 5A FF D3
E1 E1 87 D2 15 E8 A8 8B 33 48 58 B0 09 C3 8E FC
0D 0B 46 CA 50 59 38 22

Data to be absorbed

97 89 68 B3 1C E7 85 FE 36 C7 CC 6B 41 30 23 4F
D6 7C 51 DA 5D FB 7C 81 68 7A 28 06 12 3D 2D ED
47 E4 CD E9 61 A4 48 EA 8D 5E 91 B3 96 2E EA 48
BD B7 F2 C8 94 FA 52 00 D3 AC 03 01 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 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)

E3 14 7B 02 9E 7E 93 7C D3 DA C9 73 4F 70 73 5A
FE F0 5A A4 DB 95 CC 77 C5 3E D9 24 C4 94 CC 44
B9 D5 66 89 B4 2B 63 D8 DF ED C0 7E CF 95 53 CF
8E 10 22 8F 0C E6 93 F2 F4 D2 BB 18 CD 46 96 71
09 9D 05 31 E4 FF 54 3E 2A EC E4 62 71 71 E9 F0
E5 E2 6B C5 20 35 F1 D4 B3 2C 32 CE 91 71 35 84
30 C6 0F 52 BC 15 C0 CB B9 0C 2B BA A9 9A 50 B2
FA 25 F6 AF CE 38 92 17 59 E6 5A 93 98 82 E3 50
6C 68 E1 D2 A2 30 DA 90 47 E6 3E E3 D9 44 6D 82
E5 FD B6 E2 4A 1A B7 DF 0E D6 26 CD 69 B2 7A EF
FA 22 6E 1F AF 34 39 02 A8 B0 38 08 DE 5A FF D3
E1 E1 87 D2 15 E8 A8 8B 33 48 58 B0 09 C3 8E FC
0D 0B 46 CA 50 59 38 22

After Permutation

C1 0A 05 27 22 61 46 84 14 4D 28 47 48 50 B4 10
75 7E 3C BA 87 65 1B A1 67 A5 CB DD FF 7F 46 66
75 FB F8 4B CA E7 37 8A C4 44 BE 68 1D 72 94 99
AF CA 66 7F B8 79 34 8B FD DA 42 78 63 C8 2F 1C
B7 F0 5E 82 10 8D 3D 41 98 4B 48 E2 0D 90 F7 9A
86 67 A9 94 8B 07 2D 5F 17 94 29 33 8E D8 8B E7
84 B8 74 65 2F 23 F7 AC 15 83 96 AA A0 C1 44 19
8C CD 47 72 8C A8 E1 11 54 0E 01 99 B0 86 9B 28
62 B0 4F B4 F2 B3 CF 0B D5 A6 C0 C0 6B 24 56 D9
DE DD 54 5F 0C 97 32 6A C3 03 71 B8 EE 92 4B 42
FF 5E FF 8F 39 37 DC D6 D4 CF 62 25 6C A4 F1 02
26 BC 4C E4 2F 4B E0 DA B0 0D 07 62 85 77 97 34
91 D0 4D 9F BE E6 ED 12

Outval is

C1 0A 05 27 22 61 46 84 14 4D 28 47 48 50 B4 10
75 7E 3C BA 87 65 1B A1 67 A5 CB DD FF 7F 46 66
75 FB F8 4B CA E7 37 8A C4 44 BE 68 1D 72 94 99
AF CA 66 7F B8 79 34 8B FD DA 42 78 63 C8 2F 1C

==========

ParallelHashXOF:

Sample #2

Security Strength: 256-bits

Length of data is 192-bits
Data is
00 01 02 03 04 05 06 07 10 11 12 13 14 15 16 17
20 21 22 23 24 25 26 27

Block size (B) is 8

Requested output length is 512-bits

S (as a character string) is
"Parallel Data"

Encoded B
01 08
about to call last of the absorb phase

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
00 01 02 03 04 05 06 07 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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)
00 01 02 03 04 05 06 07 1F 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

After Permutation
B4 4D AE 93 F2 36 0C 49 14 FA 99 9F 3A ED 53 90
1D 47 A1 B6 14 10 9E 4B FB E8 A5 95 D5 DD 50 58
14 2C 63 B0 B5 48 E2 96 C3 7F 89 72 67 7B 7F AF
0C 22 BF 85 BF 9C 89 1C 1B 91 F6 91 84 D8 B6 DE
9A 32 B1 5E 28 99 12 CA 73 1A 12 5C 15 FA 69 40
3C B3 11 58 F7 D6 15 9A E3 E2 07 78 B5 9A 6F 43
EE 3E 27 34 7D 5E C2 38 B7 C3 A2 98 12 40 64 87
96 2C 23 9A 40 BC F9 C4 1E B2 85 CA A4 CD 27 0E
F7 CC AB 33 46 05 21 6D 20 5F 44 9F 30 B4 BF 3D
53 06 6C 1B 81 C0 6D 08 10 2C F5 31 44 51 CD C0
A1 E1 DF F9 17 72 A4 E0 3D 3A CF 72 65 7C 74 D7
32 E3 90 95 34 3B D4 62 CF EC 5F 7D 8E B2 17 79
6E 07 C6 B2 61 05 32 B7
about to call last of the absorb phase

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
Data to be absorbed
10 11 12 13 14 15 16 17 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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)

10 11 12 13 14 15 16 17 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

After Permutation

05 AE 49 D9 17 05 EE 53 5B E9 AF 26 8F 66 E6 C2
A2 2A 89 BE 4A EC DF A1 F6 6F 4D 04 97 3F 29 FB
DC 05 E8 C3 01 0B E3 22 C3 07 77 CA 0D 8C A6 67
A3 03 82 B6 9A 49 A1 57 27 4A A4 62 D5 9C C8 E1
87 5E 0C C3 20 45 C0 92 04 AA C2 A6 AF 02 D3 AA
8C 28 C9 49 F9 C6 09 31 89 A0 7F 27 DE 0D B3 02
E5 4D E1 AE 28 FB D4 05 D0 38 30 02 7B AD 36 4C
4A 93 EE AE 1B BD 5B F5 86 7F EF 6F 05 71 0A 9E
CA FA A2 20 54 A6 46 57 43 81 C9 C2 D8 2B F5 50
2C 4A 6E D5 6E F4 68 BF 6C 12 5C EF 71 34 73 13
E0 6C A7 2F F2 BE 0D 61 41 77 20 D6 C5 13 28 A3
E0 1A 87 1D DF B7 75 94 47 0E 83 E9 36 0A 77 1E
87 47 2F 45 E9 28 58 CA

about to call last of the absorb phase

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

20 21 22 23 24 25 26 27 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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)

20 21 22 23 24 25 26 27 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

After Permutation

81 BD FC 2D 48 E0 97 89 68 B3 1C E7 85 FE 36 C7
CC 6B 41 30 23 4F D6 7C 51 DA 5D FB 7C 81 68 7A
28 06 12 3D 2D ED 47 E4 CD E9 61 A4 48 EA 8D 5E
91 B3 96 2E EA 48 BD B7 F2 C8 94 FA 52 00 D3 AC
06 6A C1 E5 25 12 DC 6B B6 8F 42 3E F4 F4 C9 4E
E5 3D DF E1 AB A1 DC 26 02 21 0B 4D 99 88 52 4C
06 AC 85 74 C7 65 23 F9 A6 69 31 16 9C 8A 02 6E
C3 A9 83 1D 65 E6 46 C7 9D FF 99 20 D1 A6 D6 75
F8 4B A7 20 38 CA 2E ED C1 69 B2 42 DA 66 2B A8
26 60 C7 34 9E 3C 1F 15 95 47 C5 AC C0 B5 4A D7
B7 C8 7B F8 69 09 3A FB D4 CA 2C 4D 1E 7B 1C 9D
5C 31 C7 BC CB C4 C4 9C 56 4E 6C 2B 07 49 2A 6E
01 97 01 1A EE 27 74 BB

Encoded n

03 01

Encoded L

00 01

Length of newX is <1584>

newX is

01 08 B4 4D AE 93 F2 36 0C 49 14 FA 99 9F 3A ED
53 90 1D 47 A1 B6 14 10 9E 4B FB E8 A5 95 D5 DD
50 58 14 2C 63 B0 B5 48 E2 96 C3 7F 89 72 67 7B
7F AF 0C 22 BF 85 BF 9C 89 1C 1B 91 F6 91 84 D8
B6 DE 05 AE 49 D9 17 05 EE 53 5B E9 AF 26 8F 66
E6 C2 A2 2A 89 BE 4A EC DF A1 F6 6F 4D 04 97 3F
29 FB DC 05 E8 C3 01 0B E3 22 C3 07 77 CA 0D 8C
A6 67 A3 03 82 B6 9A 49 A1 57 27 4A A4 62 D5 9C
C8 E1 81 BD FC 2D 48 E0 97 89 68 B3 1C E7 85 FE
36 C7 CC 6B 41 30 23 4F D6 7C 51 DA 5D FB 7C 81
68 7A 28 06 12 3D 2D ED 47 E4 CD E9 61 A4 48 EA
8D 5E 91 B3 96 2E EA 48 BD B7 F2 C8 94 FA 52 00
D3 AC 03 01 00 01

Encoded N

01 60 50 61 72 61 6C 6C 65 6C 48 61 73 68

Encoded S

01 68 50 61 72 61 6C 6C 65 6C 20 44 61 74 61

bytepad data

01 88 01 60 50 61 72 61 6C 6C 65 6C 48 61 73 68
01 68 50 61 72 61 6C 6C 65 6C 20 44 61 74 61 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

Data to be absorbed

01 88 01 60 50 61 72 61 6C 6C 65 6C 48 61 73 68
01 68 50 61 72 61 6C 6C 65 6C 20 44 61 74 61 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 60 50 61 72 61 6C 6C 65 6C 48 61 73 68
01 68 50 61 72 61 6C 6C 65 6C 20 44 61 74 61 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

01 33 43 40 0A 0F 02 59 DF AD 3D D3 6B 30 8E C2
0C B8 E9 DB 7E 95 58 55 4E 74 EB 2D 01 C5 58 9C
18 E8 58 FE 2B 0E 9B 73 CB 74 D1 A9 C7 F2 7C F8
5A 91 6C D0 0A E6 DE 28 92 0B B1 DA 4B 54 B5 1E
DA 70 B8 C9 44 2A 6D 59 3D AA A8 DB 7D BD EE 95
B2 F4 4A FD D0 85 1D 43 85 DD 6E 57 59 1E CB 90
E6 64 FE 27 CE 63 6A 18 35 70 C9 A5 D3 70 59 B7
88 A3 82 33 9E 6E 67 AE D5 C8 54 59 15 19 5F 92
99 58 C9 E8 FF 56 88 AF 51 3C 82 FC 18 8B 89 E3
8E 82 C5 36 E7 3A 2E 70 F0 9A 64 6B 08 4C F4 7C
B8 C0 E5 F6 4A E6 26 F2 62 57 EE E2 71 04 EC 88
5A EB 50 B7 E6 45 CA 86 65 05 9E 56 82 A8 13 9C
30 29 9A DE D0 0B 10 B0

About to Absorb data

State (in bytes)

01 33 43 40 0A 0F 02 59 DF AD 3D D3 6B 30 8E C2
0C B8 E9 DB 7E 95 58 55 4E 74 EB 2D 01 C5 58 9C
18 E8 58 FE 2B 0E 9B 73 CB 74 D1 A9 C7 F2 7C F8
5A 91 6C D0 0A E6 DE 28 92 0B B1 DA 4B 54 B5 1E
DA 70 B8 C9 44 2A 6D 59 3D AA A8 DB 7D BD EE 95
B2 F4 4A FD D0 85 1D 43 85 DD 6E 57 59 1E CB 90
E6 64 FE 27 CE 63 6A 18 35 70 C9 A5 D3 70 59 B7
88 A3 82 33 9E 6E 67 AE D5 C8 54 59 15 19 5F 92
99 58 C9 E8 FF 56 88 AF 51 3C 82 FC 18 8B 89 E3
8E 82 C5 36 E7 3A 2E 70 F0 9A 64 6B 08 4C F4 7C
B8 C0 E5 F6 4A E6 26 F2 62 57 EE E2 71 04 EC 88
5A EB 50 B7 E6 45 CA 86 65 05 9E 56 82 A8 13 9C
30 29 9A DE D0 0B 10 B0

Data to be absorbed

01 08 B4 4D AE 93 F2 36 0C 49 14 FA 99 9F 3A ED
53 90 1D 47 A1 B6 14 10 9E 4B FB E8 A5 95 D5 DD
50 58 14 2C 63 B0 B5 48 E2 96 C3 7F 89 72 67 7B
7F AF 0C 22 BF 85 BF 9C 89 1C 1B 91 F6 91 84 D8
B6 DE 05 AE 49 D9 17 05 EE 53 5B E9 AF 26 8F 66
E6 C2 A2 2A 89 BE 4A EC DF A1 F6 6F 4D 04 97 3F
29 FB DC 05 E8 C3 01 0B E3 22 C3 07 77 CA 0D 8C
A6 67 A3 03 82 B6 9A 49 A1 57 27 4A A4 62 D5 9C
C8 E1 81 BD FC 2D 48 E0 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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)

00 3B F7 0D A4 9C F0 6F D3 E4 29 29 F2 AF B4 2F
5F 28 F4 9C DF 23 4C 45 D0 3F 10 C5 A4 50 8D 41
48 B0 4C D2 48 BE 2E 3B 29 E2 12 D6 4E 80 1B 83
25 3E 60 F2 B5 63 61 B4 1B 17 AA 4B BD C5 31 C6
6C AE BD 67 0D F3 7A 5C D3 F9 F3 32 D2 9B 61 F3
54 36 E8 D7 59 3B 57 AF 5A 7C 98 38 14 1A 5C AF
CF 9F 22 22 26 A0 6B 13 D6 52 0A A2 A4 BA 54 3B
2E C4 21 30 1C D8 FD E7 74 9F 73 13 B1 7B 8A 0E
51 B9 48 55 03 7B C0 4F 51 3C 82 FC 18 8B 89 E3
8E 82 C5 36 E7 3A 2E 70 F0 9A 64 6B 08 4C F4 7C
B8 C0 E5 F6 4A E6 26 F2 62 57 EE E2 71 04 EC 88
5A EB 50 B7 E6 45 CA 86 65 05 9E 56 82 A8 13 9C
30 29 9A DE D0 0B 10 B0

After Permutation

A8 7D 60 CA 49 52 76 79 8F 16 60 C6 A7 8F AF B8
C3 8F 10 F6 C6 9B A3 A2 F9 CC 0D B0 1F F0 8A EA
BE D0 AC 33 45 B3 F5 D4 75 3A E7 AA 80 DC 12 E5
D1 32 9D C7 FA 98 FC A1 01 C6 33 1D 07 0E 6C DE
B0 45 78 41 B3 B5 FD 2F 08 19 D2 B6 D2 C7 39 B1
2C CC 27 2D 9F 30 5D 63 A6 24 3D 71 A9 40 84 9D
29 18 0A FD 57 92 1E D0 D0 48 EF 88 CE 6F B3 7E
E5 FB 32 5A 4F 34 54 25 CA 35 9A 0C 15 AE 5B AF
69 D5 4C E4 1D 63 00 C4 05 1C 8A 05 6C BD CA FC
97 90 BF 7D 67 C4 69 85 0E 5D C0 DD 3E 54 5D 3C
13 56 A7 EC AC 92 24 CE D8 05 A0 0F 1A 6B BE D9
60 B8 EF 14 57 3F DA A6 78 E8 DD 9C 12 F3 47 9F
6E AA 7B C6 8B 6D B9 CE

about to call last of the absorb phase

About to Absorb data

State (in bytes)

A8 7D 60 CA 49 52 76 79 8F 16 60 C6 A7 8F AF B8
C3 8F 10 F6 C6 9B A3 A2 F9 CC 0D B0 1F F0 8A EA
BE D0 AC 33 45 B3 F5 D4 75 3A E7 AA 80 DC 12 E5
D1 32 9D C7 FA 98 FC A1 01 C6 33 1D 07 0E 6C DE

B0 45 78 41 B3 B5 FD 2F 08 19 D2 B6 D2 C7 39 B1
2C CC 27 2D 9F 30 5D 63 A6 24 3D 71 A9 40 84 9D
29 18 0A FD 57 92 1E D0 D0 48 EF 88 CE 6F B3 7E
E5 FB 32 5A 4F 34 54 25 CA 35 9A 0C 15 AE 5B AF
69 D5 4C E4 1D 63 00 C4 05 1C 8A 05 6C BD CA FC
97 90 BF 7D 67 C4 69 85 0E 5D C0 DD 3E 54 5D 3C
13 56 A7 EC AC 92 24 CE D8 05 A0 0F 1A 6B BE D9
60 B8 EF 14 57 3F DA A6 78 E8 DD 9C 12 F3 47 9F
6E AA 7B C6 8B 6D B9 CE

Data to be absorbed

97 89 68 B3 1C E7 85 FE 36 C7 CC 6B 41 30 23 4F
D6 7C 51 DA 5D FB 7C 81 68 7A 28 06 12 3D 2D ED
47 E4 CD E9 61 A4 48 EA 8D 5E 91 B3 96 2E EA 48
BD B7 F2 C8 94 FA 52 00 D3 AC 03 01 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 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)

3F F4 08 79 55 B5 F3 87 B9 D1 AC AD E6 BF 8C F7
15 F3 41 2C 9B 60 DF 23 91 B6 25 B6 0D CD A7 07
F9 34 61 DA 24 17 BD 3E F8 64 76 19 16 F2 F8 AD
6C 85 6F 0F 6E 62 AE A1 D2 6A 30 1C 07 0F 68 DE
B0 45 78 41 B3 B5 FD 2F 08 19 D2 B6 D2 C7 39 B1
2C CC 27 2D 9F 30 5D 63 A6 24 3D 71 A9 40 84 9D
29 18 0A FD 57 92 1E D0 D0 48 EF 88 CE 6F B3 7E
E5 FB 32 5A 4F 34 54 25 CA 35 9A 0C 15 AE 5B AF
69 D5 4C E4 1D 63 00 44 05 1C 8A 05 6C BD CA FC
97 90 BF 7D 67 C4 69 85 0E 5D C0 DD 3E 54 5D 3C
13 56 A7 EC AC 92 24 CE D8 05 A0 0F 1A 6B BE D9
60 B8 EF 14 57 3F DA A6 78 E8 DD 9C 12 F3 47 9F
6E AA 7B C6 8B 6D B9 CE

After Permutation

53 8E 10 5F 1A 22 F4 4E D2 F5 CC 16 74 FB D4 0B
E8 03 D9 C9 9B F5 F8 D9 0A 2C 81 93 F3 FE 6E A7
68 E5 C1 A2 09 87 E2 C9 C6 5F EB ED 03 88 7A 51
D3 56 24 ED 12 37 75 94 B5 58 55 41 DC 37 7E FC
F2 C8 83 7D 49 76 5A 89 2E 22 C7 06 69 7B EF 14
57 EC C2 28 76 EB E7 A9 94 68 FF 00 E1 FE 3A D0
2B E5 B2 F1 D1 8D B2 74 4B 12 3F FD 85 D1 0D 4B
1F 98 7D C6 DC 82 24 19 33 4E BB 95 3C 7E BC 60
ED 86 95 76 50 92 F1 68 8B 90 09 1C 29 93 6E F4
3A 46 F5 06 4F B1 18 37 96 C3 6C 24 74 DD E6 62
CF 37 62 4F 1D 3A 21 A9 88 D4 80 69 80 9B 94 29
DF 9C 9F DD 25 F4 6C 87 83 AE E5 52 82 5D E3 68

10 92 B4 74 D3 6B 38 9F
Outval is
53 8E 10 5F 1A 22 F4 4E D2 F5 CC 16 74 FB D4 0B
E8 03 D9 C9 9B F5 F8 D9 0A 2C 81 93 F3 FE 6E A7
68 E5 C1 A2 09 87 E2 C9 C6 5F EB ED 03 88 7A 51
D3 56 24 ED 12 37 75 94 B5 58 55 41 DC 37 7E FC

==========

ParallelHashXOF:
Sample #3

Security Strength: 256-bits

Length of data is 576-bits
Data is
00 01 02 03 04 05 06 07 08 09 0A 0B 10 11 12 13
14 15 16 17 18 19 1A 1B 20 21 22 23 24 25 26 27
28 29 2A 2B 30 31 32 33 34 35 36 37 38 39 3A 3B
40 41 42 43 44 45 46 47 48 49 4A 4B 50 51 52 53
54 55 56 57 58 59 5A 5B

Block size (B) is 12

Requested output length is 512-bits

S (as a character string) is
"Parallel Data"

Encoded B
01 0C
about to call last of the absorb phase

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
00 01 02 03 04 05 06 07 08 09 0A 0B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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)

00 01 02 03 04 05 06 07 08 09 0A 0B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

After Permutation

B3 30 73 7B 7F 00 88 7F FE 79 12 4D 61 77 38 2B
92 FF DC 26 40 39 0F BB F3 85 26 8C 28 8A 9C 9A
D9 56 91 00 1C 6B F0 65 DF 3A 72 BD 5E 58 DC 35
B8 D9 04 5E EC 7B 39 E9 90 BE 97 90 C7 0D B7 A2
23 44 61 61 A0 4F 93 F5 67 6F D3 DD 6D 39 C8 C6
6D 07 CE CB 16 0E F8 E3 03 76 8C 7A 54 36 E5 E5
76 F5 13 08 F1 63 4A 98 75 AD DE B6 9D B7 1C A6
1A 45 D5 CE 91 89 93 AF C9 62 CF AC 2F 0C 62 F8
21 A0 78 48 92 B0 F5 8C 7C C5 31 61 13 D2 FA 1B
2D AB 48 63 05 98 9D A6 67 DE 3B FC B5 0E 6A 06
D3 7C 69 CB FD 79 40 67 7D 6F EB 4F 37 C0 7E 4E
8E 8C 56 E5 5B EC D0 7E D1 F3 BE 16 E8 20 5C 04
25 77 B8 8F 4B 55 80 82

about to call last of the absorb phase

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

Data to be absorbed

10 11 12 13 14 15 16 17 18 19 1A 1B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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)

10 11 12 13 14 15 16 17 18 19 1A 1B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

After Permutation

03 5D FB 3C 60 39 BC 8D E8 D2 F7 C3 C6 93 53 05
32 F2 06 EC DB 5B 87 27 D1 4E D3 21 55 86 1C 94
7E C0 7C 79 0F 2D 20 80 CC A1 43 3C 07 13 CC 87
F9 5C A8 0E 58 E1 F2 64 D2 D6 14 36 22 B1 66 26
D0 83 40 E6 EA CF 28 26 DE 9D 74 3B 22 C5 73 2C
F7 39 B6 C6 E5 3A EE 01 F4 A9 B7 0D 30 85 FF AE
63 29 A8 94 AF BA C1 96 A0 4B 2D 64 54 4D C4 E6
E1 A7 A8 CE 55 B2 80 3F 75 E5 9E 3B D3 FE 8D 07
5C 90 54 8F BC C3 FF 08 5F 1E 56 E3 33 48 D6 10
69 AC 4E 9D D7 0B 70 0E C9 B4 9C 1D D4 40 11 DB
CA FF 1A 1A 24 57 D1 C0 54 7E 86 44 CF 62 CF EB
08 40 FE 6A 4F DF AE 87 22 85 93 B7 BB 87 97 53
D0 A0 24 72 B9 F6 95 EB

about to call last of the absorb phase

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

20 21 22 23 24 25 26 27 28 29 2A 2B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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)

20 21 22 23 24 25 26 27 28 29 2A 2B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

After Permutation

9E 6C B2 AA D4 75 B3 59 72 A7 D7 E8 B3 D2 8E 47
A9 49 53 F2 60 21 38 D6 18 D6 D6 DC 4F 85 7D E3
E4 36 FC DD 96 77 37 CC 11 0D A9 77 F8 28 CD CF
F4 24 CA F8 AD B7 F3 80 5D 9A 2D 2F EE 46 4C 9A
BE 19 82 02 D9 A4 DF FF 49 3A 2A 1D BF C5 8E AE
73 90 BF F2 21 2D 49 8B 61 30 ED E4 92 B7 27 67

A1 8E 71 15 DA C6 98 D3 E2 68 A6 A7 51 41 74 AA
7D 3E A8 0F AA 75 C7 29 A8 51 B5 31 F9 0F 39 37
E6 39 07 24 A3 E6 F3 3A 8B E4 1B 7F EB 10 1C 87
32 3D DF A1 EE 8A 3F 2A 94 2F 2E E8 D5 34 BA A4
0B 23 38 64 87 7A 79 AE 71 9D FF F6 FA 34 97 4D
E7 1C 43 23 6D F3 CF A0 75 82 54 E4 A3 04 A5 B1
F3 80 D3 86 61 20 24 6F

about to call last of the absorb phase

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

30 31 32 33 34 35 36 37 38 39 3A 3B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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)

30 31 32 33 34 35 36 37 38 39 3A 3B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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
F6 32 65 84 56 94 31 55 01 6E BE A7 B4 5D 7D 48
9B 82 DA 73 A9 17 F5 DA 81 CA DD C5 38 F0 C8 F8
7F 44 9F 61 C1 F1 5E C2 67 7A 09 60 22 99 4E F7
5A 36 28 83 F9 D7 2E DA 6C EF E8 24 50 F5 CD 63
85 EF 29 88 02 86 23 DB 1F 02 0B BF 77 44 07 97
51 08 2D A7 5B 66 F7 76 DF 37 23 A5 5A D2 0B 5B
32 61 7F 65 E5 94 59 0D 4E 0B C4 68 55 86 A8 20
2E C7 82 CD D3 64 85 C6 70 D4 1E 77 54 36 9B E7
7C B9 FA C3 5B 31 E6 65 66 37 29 55 5A 94 B7 1E
AB 1D A8 58 FE 01 BE 09 90 09 85 EA 67 C4 2E E7
84 6E D6 DC 77 3A D9 FC CD 89 D0 A7 AC 14 DF E3
4E D1 63 BF 93 34 EC 55 54 10 5C BB E4 43 09 6B
F4 16 68 67 AD D9 EF DC
about to call last of the absorb phase

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
40 41 42 43 44 45 46 47 48 49 4A 4B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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)
40 41 42 43 44 45 46 47 48 49 4A 4B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

After Permutation
DC 24 D6 0D 29 65 BB 07 62 E3 98 D8 76 2D 84 70
54 DC 02 DB 89 A0 47 91 5B B6 BB 1B 13 E1 86 BD
E8 15 E8 2C 00 DE CD 7A 89 36 D2 5C D5 29 75 AF
75 25 77 D4 4B 24 C5 40 64 13 CB A0 C7 E2 BF 62
87 B6 57 E1 9B A0 B2 02 17 55 11 25 87 2B D2 FF
E8 6B 04 FA EF 2D 5F 44 DD 9F 67 9F 0C 6B BC 10
2F 5C 04 05 3D CC 76 33 02 CC 87 50 B0 FD FF 59
6D 59 F0 9D EA 5E 70 B3 B6 EE B1 08 7B A4 C5 8E
3E 79 69 2D A7 7A 74 4E 0C F8 23 51 C2 95 F8 70
11 CF 16 A0 8F 3C 78 26 C0 F5 81 43 9F E4 81 96
E9 1D 3A 2B 53 AC 19 75 08 E5 14 65 D8 34 2A 3F
1D F7 65 3C D8 AA F5 D9 1C 81 C8 BC DD DF 85 6B
5B BE C2 7E 01 D6 05 6A
about to call last of the absorb phase

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
Data to be absorbed
50 51 52 53 54 55 56 57 58 59 5A 5B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 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)

50 51 52 53 54 55 56 57 58 59 5A 5B 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

After Permutation

AB 62 AA AD 9B 66 43 3E D1 9C 73 D3 2C 45 D9 9B
4C F9 DA 67 C1 EE 07 7B 7A 0B F5 26 C8 89 3B EA
D3 4C D4 90 DD 6E 22 48 1D 7A 28 85 B4 D3 86 8D
9C D2 B3 50 E2 92 66 D0 71 B5 3E FE E4 7C 08 EC
26 1A B3 84 59 81 00 A4 48 4B 14 CF D1 E4 0F FF
4B 34 E1 90 05 26 5A D5 39 9E A5 0F D1 70 9C 2D
2D A5 7B 4B CA AC CF 23 9A 15 63 61 08 F3 58 9A
11 A1 E9 07 1F 2C 51 94 EB 06 85 59 A5 CD 55 33
47 B3 E0 AC 28 A6 62 93 9E 4B 8D 48 3F A3 2C F8
49 D3 1D F0 3A AE A2 87 82 23 DE AC 09 B1 B4 02
A2 82 3E F1 0C 75 16 EF 6E 09 93 D7 1A C6 7F 39
8A D2 39 CB 2C 20 09 18 93 89 49 0B F1 30 9A 24
4D B1 12 B5 05 25 08 E0

Encoded n

06 01

Encoded L

00 01

Length of newX is <3120>

newX is

01 0C B3 30 73 7B 7F 00 88 7F FE 79 12 4D 61 77
38 2B 92 FF DC 26 40 39 0F BB F3 85 26 8C 28 8A
9C 9A D9 56 91 00 1C 6B F0 65 DF 3A 72 BD 5E 58
DC 35 B8 D9 04 5E EC 7B 39 E9 90 BE 97 90 C7 0D
B7 A2 03 5D FB 3C 60 39 BC 8D E8 D2 F7 C3 C6 93
53 05 32 F2 06 EC DB 5B 87 27 D1 4E D3 21 55 86
1C 94 7E C0 7C 79 0F 2D 20 80 CC A1 43 3C 07 13
CC 87 F9 5C A8 0E 58 E1 F2 64 D2 D6 14 36 22 B1
66 26 9E 6C B2 AA D4 75 B3 59 72 A7 D7 E8 B3 D2
8E 47 A9 49 53 F2 60 21 38 D6 18 D6 D6 DC 4F 85
7D E3 E4 36 FC DD 96 77 37 CC 11 0D A9 77 F8 28

CD CF F4 24 CA F8 AD B7 F3 80 5D 9A 2D 2F EE 46
4C 9A F6 32 65 84 56 94 31 55 01 6E BE A7 B4 5D
7D 48 9B 82 DA 73 A9 17 F5 DA 81 CA DD C5 38 F0
C8 F8 7F 44 9F 61 C1 F1 5E C2 67 7A 09 60 22 99
4E F7 5A 36 28 83 F9 D7 2E DA 6C EF E8 24 50 F5
CD 63 DC 24 D6 0D 29 65 BB 07 62 E3 98 D8 76 2D
84 70 54 DC 02 DB 89 A0 47 91 5B B6 BB 1B 13 E1
86 BD E8 15 E8 2C 00 DE CD 7A 89 36 D2 5C D5 29
75 AF 75 25 77 D4 4B 24 C5 40 64 13 CB A0 C7 E2
BF 62 AB 62 AA AD 9B 66 43 3E D1 9C 73 D3 2C 45
D9 9B 4C F9 DA 67 C1 EE 07 7B 7A 0B F5 26 C8 89
3B EA D3 4C D4 90 DD 6E 22 48 1D 7A 28 85 B4 D3
86 8D 9C D2 B3 50 E2 92 66 D0 71 B5 3E FE E4 7C
08 EC 06 01 00 01

Encoded N

01 60 50 61 72 61 6C 6C 65 6C 48 61 73 68

Encoded S

01 68 50 61 72 61 6C 6C 65 6C 20 44 61 74 61

bytepad data

01 88 01 60 50 61 72 61 6C 6C 65 6C 48 61 73 68
01 68 50 61 72 61 6C 6C 65 6C 20 44 61 74 61 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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 60 50 61 72 61 6C 6C 65 6C 48 61 73 68
01 68 50 61 72 61 6C 6C 65 6C 20 44 61 74 61 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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 60 50 61 72 61 6C 6C 65 6C 48 61 73 68
01 68 50 61 72 61 6C 6C 65 6C 20 44 61 74 61 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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

01 33 43 40 0A 0F 02 59 DF AD 3D D3 6B 30 8E C2
0C B8 E9 DB 7E 95 58 55 4E 74 EB 2D 01 C5 58 9C
18 E8 58 FE 2B 0E 9B 73 CB 74 D1 A9 C7 F2 7C F8
5A 91 6C D0 0A E6 DE 28 92 0B B1 DA 4B 54 B5 1E
DA 70 B8 C9 44 2A 6D 59 3D AA A8 DB 7D BD EE 95
B2 F4 4A FD D0 85 1D 43 85 DD 6E 57 59 1E CB 90
E6 64 FE 27 CE 63 6A 18 35 70 C9 A5 D3 70 59 B7
88 A3 82 33 9E 6E 67 AE D5 C8 54 59 15 19 5F 92
99 58 C9 E8 FF 56 88 AF 51 3C 82 FC 18 8B 89 E3
8E 82 C5 36 E7 3A 2E 70 F0 9A 64 6B 08 4C F4 7C
B8 C0 E5 F6 4A E6 26 F2 62 57 EE E2 71 04 EC 88
5A EB 50 B7 E6 45 CA 86 65 05 9E 56 82 A8 13 9C
30 29 9A DE D0 0B 10 B0

About to Absorb data

State (in bytes)

01 33 43 40 0A 0F 02 59 DF AD 3D D3 6B 30 8E C2
0C B8 E9 DB 7E 95 58 55 4E 74 EB 2D 01 C5 58 9C
18 E8 58 FE 2B 0E 9B 73 CB 74 D1 A9 C7 F2 7C F8
5A 91 6C D0 0A E6 DE 28 92 0B B1 DA 4B 54 B5 1E
DA 70 B8 C9 44 2A 6D 59 3D AA A8 DB 7D BD EE 95
B2 F4 4A FD D0 85 1D 43 85 DD 6E 57 59 1E CB 90
E6 64 FE 27 CE 63 6A 18 35 70 C9 A5 D3 70 59 B7
88 A3 82 33 9E 6E 67 AE D5 C8 54 59 15 19 5F 92
99 58 C9 E8 FF 56 88 AF 51 3C 82 FC 18 8B 89 E3
8E 82 C5 36 E7 3A 2E 70 F0 9A 64 6B 08 4C F4 7C
B8 C0 E5 F6 4A E6 26 F2 62 57 EE E2 71 04 EC 88
5A EB 50 B7 E6 45 CA 86 65 05 9E 56 82 A8 13 9C

30 29 9A DE D0 0B 10 B0

Data to be absorbed

01 0C B3 30 73 7B 7F 00 88 7F FE 79 12 4D 61 77
38 2B 92 FF DC 26 40 39 0F BB F3 85 26 8C 28 8A
9C 9A D9 56 91 00 1C 6B F0 65 DF 3A 72 BD 5E 58
DC 35 B8 D9 04 5E EC 7B 39 E9 90 BE 97 90 C7 0D
B7 A2 03 5D FB 3C 60 39 BC 8D E8 D2 F7 C3 C6 93
53 05 32 F2 06 EC DB 5B 87 27 D1 4E D3 21 55 86
1C 94 7E C0 7C 79 0F 2D 20 80 CC A1 43 3C 07 13
CC 87 F9 5C A8 0E 58 E1 F2 64 D2 D6 14 36 22 B1
66 26 9E 6C B2 AA D4 75 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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)

00 3F F0 70 79 74 7D 59 57 D2 C3 AA 79 7D EF B5
34 93 7B 24 A2 B3 18 6C 41 CF 18 A8 27 49 70 16
84 72 81 A8 BA 0E 87 18 3B 11 0E 93 B5 4F 22 A0
86 A4 D4 09 0E B8 32 53 AB E2 21 64 DC C4 72 13
6D D2 BB 94 BF 16 0D 60 81 27 40 09 8A 7E 28 06
E1 F1 78 0F D6 69 C6 18 02 FA BF 19 8A 3F 9E 16
FA F0 80 E7 B2 1A 65 35 15 F0 05 04 90 4C 5E A4
44 24 7B 6F 36 60 3F 4F 27 AC 86 8F 01 2F 7D 23
FF 7E 57 84 4D FC 5C DA 51 3C 82 FC 18 8B 89 E3
8E 82 C5 36 E7 3A 2E 70 F0 9A 64 6B 08 4C F4 7C
B8 C0 E5 F6 4A E6 26 F2 62 57 EE E2 71 04 EC 88
5A EB 50 B7 E6 45 CA 86 65 05 9E 56 82 A8 13 9C
30 29 9A DE D0 0B 10 B0

After Permutation

C2 69 C6 47 82 73 7E AC E7 C1 19 80 F9 72 61 66
5F 83 2A 11 46 02 59 8B F2 84 E4 F9 AD 06 D8 B5
4B 56 32 16 0C A2 F0 BE 05 9A 9C 04 1F 1F C7 83
96 91 BF 6B C5 6C EF C5 45 6A 38 77 A0 69 3D E6
70 87 48 D0 9B 1D F7 24 12 7E 84 22 94 03 92 45
11 C2 35 78 8C 44 49 00 56 07 5C 3C E0 ED A3 87
FF 6E 65 8F 4C CF FB 03 03 45 79 88 7C E0 D2 60
46 81 38 B6 25 A2 2C DA 04 4A AF F0 7B 74 4D 8F
20 7E 3E 96 1B E0 10 2D 29 E4 86 7A 7A A7 2B E7
92 98 A8 A7 20 CD 22 66 B4 D6 52 88 33 87 65 AE
EF 55 AC A5 E5 55 0C 33 00 98 DA D5 5A 06 C6 B2
C5 21 7D 8A 83 DA A0 B4 F2 82 3F DD 2D 8F A5 F2
4C A6 8E 74 9D 84 60 CC

About to Absorb data

State (in bytes)

C2 69 C6 47 82 73 7E AC E7 C1 19 80 F9 72 61 66
5F 83 2A 11 46 02 59 8B F2 84 E4 F9 AD 06 D8 B5
4B 56 32 16 0C A2 F0 BE 05 9A 9C 04 1F 1F C7 83
96 91 BF 6B C5 6C EF C5 45 6A 38 77 A0 69 3D E6

70 87 48 D0 9B 1D F7 24 12 7E 84 22 94 03 92 45
11 C2 35 78 8C 44 49 00 56 07 5C 3C E0 ED A3 87
FF 6E 65 8F 4C CF FB 03 03 45 79 88 7C E0 D2 60
46 81 38 B6 25 A2 2C DA 04 4A AF F0 7B 74 4D 8F
20 7E 3E 96 1B E0 10 2D 29 E4 86 7A 7A A7 2B E7
92 98 A8 A7 20 CD 22 66 B4 D6 52 88 33 87 65 AE
EF 55 AC A5 E5 55 0C 33 00 98 DA D5 5A 06 C6 B2
C5 21 7D 8A 83 DA A0 B4 F2 82 3F DD 2D 8F A5 F2
4C A6 8E 74 9D 84 60 CC

Data to be absorbed

B3 59 72 A7 D7 E8 B3 D2 8E 47 A9 49 53 F2 60 21
38 D6 18 D6 D6 DC 4F 85 7D E3 E4 36 FC DD 96 77
37 CC 11 0D A9 77 F8 28 CD CF F4 24 CA F8 AD B7
F3 80 5D 9A 2D 2F EE 46 4C 9A F6 32 65 84 56 94
31 55 01 6E BE A7 B4 5D 7D 48 9B 82 DA 73 A9 17
F5 DA 81 CA DD C5 38 F0 C8 F8 7F 44 9F 61 C1 F1
5E C2 67 7A 09 60 22 99 4E F7 5A 36 28 83 F9 D7
2E DA 6C EF E8 24 50 F5 CD 63 DC 24 D6 0D 29 65
BB 07 62 E3 98 D8 76 2D 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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)

71 30 B4 E0 55 9B CD 7E 69 86 B0 C9 AA 80 01 47
67 55 32 C7 90 DE 16 0E 8F 67 00 CF 51 DB 4E C2
7C 9A 23 1B A5 D5 08 96 C8 55 68 20 D5 E7 6A 34
65 11 E2 F1 E8 43 01 83 09 F0 CE 45 C5 ED 6B 72
41 D2 49 BE 25 BA 43 79 6F 36 1F A0 4E 70 3B 52
E4 18 B4 B2 51 81 71 F0 9E FF 23 78 7F 8C 62 76
A1 AC 02 F5 45 AF D9 9A 4D B2 23 BE 54 63 2B B7
68 5B 54 59 CD 86 7C 2F C9 29 73 D4 AD 79 64 EA
9B 79 5C 75 83 38 66 00 29 E4 86 7A 7A A7 2B E7
92 98 A8 A7 20 CD 22 66 B4 D6 52 88 33 87 65 AE
EF 55 AC A5 E5 55 0C 33 00 98 DA D5 5A 06 C6 B2
C5 21 7D 8A 83 DA A0 B4 F2 82 3F DD 2D 8F A5 F2
4C A6 8E 74 9D 84 60 CC

After Permutation

37 17 76 AE 7C 5F 31 3B 93 2A 78 6A 7D 01 DB AE
86 EC D2 57 63 EE 15 E3 56 D6 65 9D C4 08 E4 F6
70 3B 41 73 05 3B 56 84 A2 8D 22 18 2A FF D8 41
45 C2 23 CF 39 89 C6 00 25 95 EE 15 2B E1 1B 47
A0 F6 74 32 89 6C 4E F2 B6 A5 4B 78 B5 C2 00 E4
D7 12 39 07 E7 E0 FD 23 5F CD 7D 5F 7F 38 43 5B
02 34 82 99 CC DB 71 60 4C 7D 44 0D E5 26 DB ED
20 07 C3 95 12 07 24 DD 5B 22 33 C8 2D BD 7C F0
1A BE 11 C4 59 BB 6F EF 68 A9 A6 F8 4E 99 6B B5
B2 DF D8 F9 DB 14 24 11 7D BD 41 C6 1C 07 A8 04
FF 87 92 1D B5 BD C2 AE D3 6C D3 0C 53 78 7F F7
54 D8 6F 00 2B EC C4 6F 0D 0D 5A 38 20 9F 46 A6

3B 5B B8 DB CF BB 31 06
about to call last of the absorb phase

About to Absorb data
State (in bytes)
37 17 76 AE 7C 5F 31 3B 93 2A 78 6A 7D 01 DB AE
86 EC D2 57 63 EE 15 E3 56 D6 65 9D C4 08 E4 F6
70 3B 41 73 05 3B 56 84 A2 8D 22 18 2A FF D8 41
45 C2 23 CF 39 89 C6 00 25 95 EE 15 2B E1 1B 47
A0 F6 74 32 89 6C 4E F2 B6 A5 4B 78 B5 C2 00 E4
D7 12 39 07 E7 E0 FD 23 5F CD 7D 5F 7F 38 43 5B
02 34 82 99 CC DB 71 60 4C 7D 44 0D E5 26 DB ED
20 07 C3 95 12 07 24 DD 5B 22 33 C8 2D BD 7C F0
1A BE 11 C4 59 BB 6F EF 68 A9 A6 F8 4E 99 6B B5
B2 DF D8 F9 DB 14 24 11 7D BD 41 C6 1C 07 A8 04
FF 87 92 1D B5 BD C2 AE D3 6C D3 0C 53 78 7F F7
54 D8 6F 00 2B EC C4 6F 0D 0D 5A 38 20 9F 46 A6
3B 5B B8 DB CF BB 31 06
Data to be absorbed
84 70 54 DC 02 DB 89 A0 47 91 5B B6 BB 1B 13 E1
86 BD E8 15 E8 2C 00 DE CD 7A 89 36 D2 5C D5 29
75 AF 75 25 77 D4 4B 24 C5 40 64 13 CB A0 C7 E2
BF 62 AB 62 AA AD 9B 66 43 3E D1 9C 73 D3 2C 45
D9 9B 4C F9 DA 67 C1 EE 07 7B 7A 0B F5 26 C8 89
3B EA D3 4C D4 90 DD 6E 22 48 1D 7A 28 85 B4 D3
86 8D 9C D2 B3 50 E2 92 66 D0 71 B5 3E FE E4 7C
08 EC 06 01 00 01 04 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)
B3 67 22 72 7E 84 B8 9B D4 BB 23 DC C6 1A C8 4F
00 51 3A 42 8B C2 15 3D 9B AC EC AB 16 54 31 DF
05 94 34 56 72 EF 1D A0 67 CD 46 0B E1 5F 1F A3
FA A0 88 AD 93 24 5D 66 66 AB 3F 89 58 32 37 02
79 6D 38 CB 53 0B 8F 1C B1 DE 31 73 40 E4 C8 6D
EC F8 EA 4B 33 70 20 4D 7D 85 60 25 57 BD F7 88
84 B9 1E 4B 7F 8B 93 F2 2A AD 35 B8 DB D8 3F 91
28 EB C5 94 12 06 20 DD 5B 22 33 C8 2D BD 7C F0
1A BE 11 C4 59 BB 6F 6F 68 A9 A6 F8 4E 99 6B B5
B2 DF D8 F9 DB 14 24 11 7D BD 41 C6 1C 07 A8 04
FF 87 92 1D B5 BD C2 AE D3 6C D3 0C 53 78 7F F7
54 D8 6F 00 2B EC C4 6F 0D 0D 5A 38 20 9F 46 A6
3B 5B B8 DB CF BB 31 06

After Permutation
6B 3E 79 0B 33 0C 88 9A 20 4C 2F BC 72 8D 80 9F
19 36 73 28 D8 52 F4 00 2D C8 29 F7 3A FD 6B CE
FB 7F E5 B6 07 B1 3A 80 1C 0B E5 C1 17 0B DB 79

4E 33 94 58 FD B0 E6 2A 6A F3 D4 25 58 97 02 49
49 ED C3 B2 02 05 9D AC 31 CA F7 D0 4D 19 F9 A1
A8 DA 9E D6 C2 47 66 77 03 FF E1 E6 F1 12 97 AE
D4 CC D3 79 FB 74 F7 6B E8 76 4E 3E 94 D2 13 32
85 30 5D 7C C3 4F B4 6D DD B4 2B 60 2F 1F D2 B2
58 2C C9 C5 FD 84 1B D6 D9 70 20 03 8B D5 A4 64
45 C8 BA F6 72 CB B5 77 17 28 A3 87 50 9D A8 BC
DF F0 9D 04 4F E8 E7 A3 C0 55 A3 80 2F 34 E9 AA
A5 DE 28 83 2A 5E C4 62 76 FB 02 B5 F7 A0 92 75
B2 85 12 4E 36 82 10 04

Outval is

6B 3E 79 0B 33 0C 88 9A 20 4C 2F BC 72 8D 80 9F
19 36 73 28 D8 52 F4 00 2D C8 29 F7 3A FD 6B CE
FB 7F E5 B6 07 B1 3A 80 1C 0B E5 C1 17 0B DB 79
4E 33 94 58 FD B0 E6 2A 6A F3 D4 25 58 97 02 49

==========