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

  Block Cipher Modes of Operation

     FF1 Method for Format-Preserving Encryption

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

Sample #1

FF1-AES128

Key is 2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C
Radix = 10
--------------------------------------------------------------


PT is <0123456789>

FF1.Encrypt()

X is    0 1 2 3 4 5 6 7 8 9
Tweak is <empty>

Step 1
        u is 5, v is 5
Step 2
        A is    0 1 2 3 4
        B is    5 6 7 8 9
Step 3
        b is 3
Step 4
        d is 8
Step 5
        P is  [ 1, 2, 1, 0, 0, 10, 10, 5, 0, 0, 0, 10, 0, 0, 0, 0 ]

Round #0
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 221,
213 ]
        Step 6.ii
                R is  [ 195, 184, 41, 161, 232, 100, 43, 120, 204, 41,
148, 123, 59, 147, 219, 99 ]
        Step 6.iii
                S is c3b829a1e8642b78
        Step 6.iv
                y is  14103068008476060536
        Step 6.v
                m is 5
        Step 6.vi
```

```
                c is  61770
        Step 6.vii
                C is    6 1 7 7 0
        Step 6.viii
                A is    5 6 7 8 9
        Step 6.ix
                B is    6 1 7 7 0

Round #1
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 241,
74 ]
        Step 6.ii
                R is  [ 121, 100, 61, 158, 221, 250, 131, 16, 72, 2,
224, 89, 189, 220, 199, 44 ]
        Step 6.iii
                S is 79643d9eddfa8310
        Step 6.iv
                y is  8747184128798655248
        Step 6.v
                m is 5
        Step 6.vi
                c is  12037
        Step 6.vii
                C is    1 2 0 3 7
        Step 6.viii
                A is    6 1 7 7 0
        Step 6.ix
                B is    1 2 0 3 7

Round #2
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 47,
5 ]
        Step 6.ii
                R is  [ 9, 132, 75, 58, 46, 151, 10, 51, 165, 69, 95,
100, 199, 67, 56, 77 ]
        Step 6.iii
                S is 09844b3a2e970a33
        Step 6.iv
                y is  685755756528994867
        Step 6.v
                m is 5
        Step 6.vi
                c is  56637
        Step 6.vii
                C is    5 6 6 3 7
        Step 6.viii
                A is    1 2 0 3 7
        Step 6.ix
```

```
                B is    5 6 6 3 7

Round #3
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 221,
61 ]
        Step 6.ii
                R is  [ 125, 29, 160, 178, 41, 158, 148, 66, 104, 179,
136, 46, 59, 198, 72, 57 ]
        Step 6.iii
                S is 7d1da0b2299e9442
        Step 6.iv
                y is  9015538716128482370
        Step 6.v
                m is 5
        Step 6.vi
                c is  94407
        Step 6.vii
                C is    9 4 4 0 7
        Step 6.viii
                A is    5 6 6 3 7
        Step 6.ix
                B is    9 4 4 0 7

Round #4
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 1, 112,
199 ]
        Step 6.ii
                R is  [ 67, 122, 82, 147, 218, 251, 246, 239, 143, 18,
111, 55, 229, 180, 6, 114 ]
        Step 6.iii
                S is 437a5293dafbf6ef
        Step 6.iv
                y is  4862289542687487727
        Step 6.v
                m is 5
        Step 6.vi
                c is  44364
        Step 6.vii
                C is    4 4 3 6 4
        Step 6.viii
                A is    9 4 4 0 7
        Step 6.ix
                B is    4 4 3 6 4

Round #5
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 0, 173,
76 ]
```

```
        Step 6.ii
                R is  [ 216, 186, 138, 193, 244, 52, 17, 22, 8, 188,
121, 95, 62, 150, 28, 18 ]
        Step 6.iii
                S is d8ba8ac1f4341116
        Step 6.iv
                y is  15616947223490990358
        Step 6.v
                m is 5
        Step 6.vi
                c is  84765
        Step 6.vii
                C is    8 4 7 6 5
        Step 6.viii
                A is    4 4 3 6 4
        Step 6.ix
                B is    8 4 7 6 5

Round #6
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 6, 1, 75,
29 ]
        Step 6.ii
                R is  [ 190, 15, 19, 163, 157, 41, 253, 232, 18, 10,
55, 166, 7, 219, 21, 192 ]
        Step 6.iii
                S is be0f13a39d29fde8
        Step 6.iv
                y is  13695186585294339560
        Step 6.v
                m is 5
        Step 6.vi
                c is  83924
        Step 6.vii
                C is    8 3 9 2 4
        Step 6.viii
                A is    8 4 7 6 5
        Step 6.ix
                B is    8 3 9 2 4

Round #7
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 7, 1, 71,
212 ]
        Step 6.ii
                R is  [ 79, 25, 29, 191, 153, 112, 242, 154, 155, 129,
202, 99, 245, 71, 41, 192 ]
        Step 6.iii
                S is 4f191dbf9970f29a
        Step 6.iv
```

```
                y is  5699619512164348570
        Step 6.v
                m is 5
        Step 6.vi
                c is  33335
        Step 6.vii
                C is    3 3 3 3 5
        Step 6.viii
                A is    8 3 9 2 4
        Step 6.ix
                B is    3 3 3 3 5

Round #8
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8, 0, 130,
55 ]
        Step 6.ii
                R is  [ 194, 52, 118, 117, 58, 50, 235, 26, 244, 207,
225, 21, 85, 189, 189, 27 ]
        Step 6.iii
                S is c23476753a32eb1a
        Step 6.iv
                y is  13993940188006640410
        Step 6.v
                m is 5
        Step 6.vi
                c is  24334
        Step 6.vii
                C is    2 4 3 3 4
        Step 6.viii
                A is    3 3 3 3 5
        Step 6.ix
                B is    2 4 3 3 4

Round #9
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 9, 0, 95,
14 ]
        Step 6.ii
                R is  [ 143, 196, 218, 77, 67, 14, 128, 21, 112, 172,
197, 74, 236, 154, 4, 243 ]
        Step 6.iii
                S is 8fc4da4d430e8015
        Step 6.iv
                y is  10359645068231344149
        Step 6.v
                m is 5
        Step 6.vi
                c is  77484
        Step 6.vii
```

```
                C is    7 7 4 8 4
        Step 6.viii
                A is    2 4 3 3 4
        Step 6.ix
                B is    7 7 4 8 4

Step 7
        A || B is    2 4 3 3 4 7 7 4 8 4

CT is <2433477484>

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

FF1.Decrypt()

X is    2 4 3 3 4 7 7 4 8 4
Tweak is <empty>

Step 1
        u is 5, v is 5
Step 2
        A is    2 4 3 3 4
        B is    7 7 4 8 4
Step 3
        b is 3
Step 4
        d is 8
Step 5
        P is  [ 1, 2, 1, 0, 0, 10, 10, 5, 0, 0, 0, 10, 0, 0, 0, 0 ]

Round #9
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 9, 0, 95, 
14 ]
        Step 6.ii
                R is  [ 143, 196, 218, 77, 67, 14, 128, 21, 112, 172, 
197, 74, 236, 154, 4, 243 ]
        Step 6.iii
                S is 8fc4da4d430e8015
        Step 6.iv
                y is  10359645068231344149
        Step 6.v
                m is 5
        Step 6.vi
                c is  33335
        Step 6.vii
                C is    3 3 3 3 5
        Step 6.viii
                B is    2 4 3 3 4
        Step 6.ix
```

```
                A is    3 3 3 3 5

Round #8
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8, 0, 130,
55 ]
        Step 6.ii
                R is  [ 194, 52, 118, 117, 58, 50, 235, 26, 244, 207,
225, 21, 85, 189, 189, 27 ]
        Step 6.iii
                S is c23476753a32eb1a
        Step 6.iv
                y is  13993940188006640410
        Step 6.v
                m is 5
        Step 6.vi
                c is  83924
        Step 6.vii
                C is    8 3 9 2 4
        Step 6.viii
                B is    3 3 3 3 5
        Step 6.ix
                A is    8 3 9 2 4

Round #7
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 7, 1, 71,
212 ]
        Step 6.ii
                R is  [ 79, 25, 29, 191, 153, 112, 242, 154, 155, 129,
202, 99, 245, 71, 41, 192 ]
        Step 6.iii
                S is 4f191dbf9970f29a
        Step 6.iv
                y is  5699619512164348570
        Step 6.v
                m is 5
        Step 6.vi
                c is  84765
        Step 6.vii
                C is    8 4 7 6 5
        Step 6.viii
                B is    8 3 9 2 4
        Step 6.ix
                A is    8 4 7 6 5

Round #6
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 6, 1, 75,
29 ]
```

```
        Step 6.ii
                R is  [ 190, 15, 19, 163, 157, 41, 253, 232, 18, 10,
55, 166, 7, 219, 21, 192 ]
        Step 6.iii
                S is be0f13a39d29fde8
        Step 6.iv
                y is  13695186585294339560
        Step 6.v
                m is 5
        Step 6.vi
                c is  44364
        Step 6.vii
                C is    4 4 3 6 4
        Step 6.viii
                B is    8 4 7 6 5
        Step 6.ix
                A is    4 4 3 6 4

Round #5
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 0, 173,
76 ]
        Step 6.ii
                R is  [ 216, 186, 138, 193, 244, 52, 17, 22, 8, 188,
121, 95, 62, 150, 28, 18 ]
        Step 6.iii
                S is d8ba8ac1f4341116
        Step 6.iv
                y is  15616947223490990358
        Step 6.v
                m is 5
        Step 6.vi
                c is  94407
        Step 6.vii
                C is    9 4 4 0 7
        Step 6.viii
                B is    4 4 3 6 4
        Step 6.ix
                A is    9 4 4 0 7

Round #4
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 1, 112,
199 ]
        Step 6.ii
                R is  [ 67, 122, 82, 147, 218, 251, 246, 239, 143, 18,
111, 55, 229, 180, 6, 114 ]
        Step 6.iii
                S is 437a5293dafbf6ef
        Step 6.iv
```

```
                y is  4862289542687487727
        Step 6.v
                m is 5
        Step 6.vi
                c is  56637
        Step 6.vii
                C is    5 6 6 3 7
        Step 6.viii
                B is    9 4 4 0 7
        Step 6.ix
                A is    5 6 6 3 7

Round #3
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 221,
61 ]
        Step 6.ii
                R is  [ 125, 29, 160, 178, 41, 158, 148, 66, 104, 179,
136, 46, 59, 198, 72, 57 ]
        Step 6.iii
                S is 7d1da0b2299e9442
        Step 6.iv
                y is  9015538716128482370
        Step 6.v
                m is 5
        Step 6.vi
                c is  12037
        Step 6.vii
                C is    1 2 0 3 7
        Step 6.viii
                B is    5 6 6 3 7
        Step 6.ix
                A is    1 2 0 3 7

Round #2
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 47,
5 ]
        Step 6.ii
                R is  [ 9, 132, 75, 58, 46, 151, 10, 51, 165, 69, 95,
100, 199, 67, 56, 77 ]
        Step 6.iii
                S is 09844b3a2e970a33
        Step 6.iv
                y is  685755756528994867
        Step 6.v
                m is 5
        Step 6.vi
                c is  61770
        Step 6.vii
```

```
                C is    6 1 7 7 0
        Step 6.viii
                B is    1 2 0 3 7
        Step 6.ix
                A is    6 1 7 7 0

Round #1
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 241,
74 ]
        Step 6.ii
                R is  [ 121, 100, 61, 158, 221, 250, 131, 16, 72, 2,
224, 89, 189, 220, 199, 44 ]
        Step 6.iii
                S is 79643d9eddfa8310
        Step 6.iv
                y is  8747184128798655248
        Step 6.v
                m is 5
        Step 6.vi
                c is  56789
        Step 6.vii
                C is    5 6 7 8 9
        Step 6.viii
                B is    6 1 7 7 0
        Step 6.ix
                A is    5 6 7 8 9

Round #0
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 221,
213 ]
        Step 6.ii
                R is  [ 195, 184, 41, 161, 232, 100, 43, 120, 204, 41,
148, 123, 59, 147, 219, 99 ]
        Step 6.iii
                S is c3b829a1e8642b78
        Step 6.iv
                y is  14103068008476060536
        Step 6.v
                m is 5
        Step 6.vi
                c is  1234
        Step 6.vii
                C is    0 1 2 3 4
        Step 6.viii
                B is    5 6 7 8 9
        Step 6.ix
                A is    0 1 2 3 4
Step 7
```

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

PT is <0123456789>

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

Sample #2

FF1-AES128

Key is 2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C
Radix = 10
--------------------------------------------------------------


PT is <0123456789>

FF1.Encrypt()

X is    0 1 2 3 4 5 6 7 8 9
Tweak is 39 38 37 36 35 34 33 32 31 30

Step 1
        u is 5, v is 5
Step 2
        A is    0 1 2 3 4
        B is    5 6 7 8 9
Step 3
        b is 3
Step 4
        d is 8
Step 5
        P is  [ 1, 2, 1, 0, 0, 10, 10, 5, 0, 0, 0, 10, 0, 0, 0, 10 ]

Round #0
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
0, 0, 221, 213 ]
        Step 6.ii
                R is  [ 178, 23, 94, 227, 235, 107, 241, 88, 255, 225,
124, 35, 113, 229, 204, 19 ]
        Step 6.iii
                S is b2175ee3eb6bf158
        Step 6.iv
                y is  12832829996215824728
        Step 6.v
                m is 5
        Step 6.vi
                c is  25962
        Step 6.vii
```

```
                C is    2 5 9 6 2
        Step 6.viii
                A is    5 6 7 8 9
        Step 6.ix
                B is    2 5 9 6 2

Round #1
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
1, 0, 101, 106 ]
        Step 6.ii
                R is  [ 51, 190, 249, 61, 4, 109, 120, 103, 51, 255,
70, 97, 20, 140, 87, 153 ]
        Step 6.iii
                S is 33bef93d046d7867
        Step 6.iv
                y is  3728691581971953767
        Step 6.v
                m is 5
        Step 6.vi
                c is  10556
        Step 6.vii
                C is    1 0 5 5 6
        Step 6.viii
                A is    2 5 9 6 2
        Step 6.ix
                B is    1 0 5 5 6

Round #2
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
2, 0, 41, 60 ]
        Step 6.ii
                R is  [ 46, 119, 157, 146, 150, 130, 241, 192, 111,
134, 229, 160, 201, 157, 218, 98 ]
        Step 6.iii
                S is 2e779d929682f1c0
        Step 6.iv
                y is  3348318100889203136
        Step 6.v
                m is 5
        Step 6.vi
                c is  29098
        Step 6.vii
                C is    2 9 0 9 8
        Step 6.viii
                A is    1 0 5 5 6
        Step 6.ix
                B is    2 9 0 9 8
```

```
Round #3
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
3, 0, 113, 170 ]
        Step 6.ii
                R is  [ 174, 123, 224, 87, 184, 248, 56, 84, 44, 10,
27, 227, 157, 233, 178, 91 ]
        Step 6.iii
                S is ae7be057b8f83854
        Step 6.iv
                y is  12572889452104923220
        Step 6.v
                m is 5
        Step 6.vi
                c is  33776
        Step 6.vii
                C is    3 3 7 7 6
        Step 6.viii
                A is    2 9 0 9 8
        Step 6.ix
                B is    3 3 7 7 6

Round #4
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
4, 0, 131, 240 ]
        Step 6.ii
                R is  [ 143, 241, 191, 84, 85, 109, 85, 62, 98, 142,
122, 217, 177, 208, 239, 4 ]
        Step 6.iii
                S is 8ff1bf54556d553e
        Step 6.iv
                y is  10372281785742349630
        Step 6.v
                m is 5
        Step 6.vi
                c is  78728
        Step 6.vii
                C is    7 8 7 2 8
        Step 6.viii
                A is    3 3 7 7 6
        Step 6.ix
                B is    7 8 7 2 8

Round #5
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
5, 1, 51, 136 ]
        Step 6.ii
                R is  [ 38, 71, 126, 189, 186, 53, 31, 145, 238, 76,
86, 253, 112, 160, 174, 231 ]
        Step 6.iii
                S is 26477ebdba351f91
        Step 6.iv
                y is  2758312650125680529
        Step 6.v
                m is 5
        Step 6.vi
                c is  14305
        Step 6.vii
                C is    1 4 3 0 5
        Step 6.viii
                A is    7 8 7 2 8
        Step 6.ix
                B is    1 4 3 0 5

Round #6
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
6, 0, 55, 225 ]
        Step 6.ii
                R is  [ 125, 75, 237, 158, 131, 55, 209, 9, 101, 197,
0, 121, 194, 2, 116, 132 ]
        Step 6.iii
                S is 7d4bed9e8337d109
        Step 6.iv
                y is  9028571143056380169
        Step 6.v
                m is 5
        Step 6.vi
                c is  58897
        Step 6.vii
                C is    5 8 8 9 7
        Step 6.viii
                A is    1 4 3 0 5
        Step 6.ix
                B is    5 8 8 9 7

Round #7
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
7, 0, 230, 17 ]
        Step 6.ii
                R is  [ 242, 246, 229, 238, 234, 164, 97, 149, 226,
83, 116, 152, 51, 255, 35, 135 ]
        Step 6.iii
                S is f2f6e5eeeaa46195
        Step 6.iv
                y is  17507433415751000469
        Step 6.v
```

```
                m is 5
        Step 6.vi
                c is  14774
        Step 6.vii
                C is    1 4 7 7 4
        Step 6.viii
                A is    5 8 8 9 7
        Step 6.ix
                B is    1 4 7 7 4

Round #8
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
8, 0, 57, 182 ]
        Step 6.ii
                R is  [ 207, 0, 24, 102, 176, 164, 198, 169, 67, 219,
228, 100, 60, 109, 178, 131 ]
        Step 6.iii
                S is cf001866b0a4c6a9
        Step 6.iv
                y is  14915948795180402345
        Step 6.v
                m is 5
        Step 6.vi
                c is  61242
        Step 6.vii
                C is    6 1 2 4 2
        Step 6.viii
                A is    1 4 7 7 4
        Step 6.ix
                B is    6 1 2 4 2

Round #9
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
9, 0, 239, 58 ]
        Step 6.ii
                R is  [ 242, 84, 227, 1, 12, 169, 217, 207, 48, 18,
229, 133, 12, 69, 210, 146 ]
        Step 6.iii
                S is f254e3010ca9d9cf
        Step 6.iv
                y is  17461831248869185999
        Step 6.v
                m is 5
        Step 6.vi
                c is  773
        Step 6.vii
                C is    0 0 7 7 3
        Step 6.viii
```

```
                A is    6 1 2 4 2
        Step 6.ix
                B is    0 0 7 7 3

Step 7
        A || B is    6 1 2 4 2 0 0 7 7 3

CT is <6124200773>

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

FF1.Decrypt()

X is    6 1 2 4 2 0 0 7 7 3
Tweak is 39 38 37 36 35 34 33 32 31 30

Step 1
        u is 5, v is 5
Step 2
        A is    6 1 2 4 2
        B is    0 0 7 7 3
Step 3
        b is 3
Step 4
        d is 8
Step 5
        P is  [ 1, 2, 1, 0, 0, 10, 10, 5, 0, 0, 0, 10, 0, 0, 0, 10 ]

Round #9
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
9, 0, 239, 58 ]
        Step 6.ii
                R is  [ 242, 84, 227, 1, 12, 169, 217, 207, 48, 18,
229, 133, 12, 69, 210, 146 ]
        Step 6.iii
                S is f254e3010ca9d9cf
        Step 6.iv
                y is  17461831248869185999
        Step 6.v
                m is 5
        Step 6.vi
                c is  14774
        Step 6.vii
                C is    1 4 7 7 4
        Step 6.viii
                B is    6 1 2 4 2
        Step 6.ix
                A is    1 4 7 7 4
```

```
Round #8
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
8, 0, 57, 182 ]
        Step 6.ii
                R is  [ 207, 0, 24, 102, 176, 164, 198, 169, 67, 219,
228, 100, 60, 109, 178, 131 ]
        Step 6.iii
                S is cf001866b0a4c6a9
        Step 6.iv
                y is  14915948795180402345
        Step 6.v
                m is 5
        Step 6.vi
                c is  58897
        Step 6.vii
                C is    5 8 8 9 7
        Step 6.viii
                B is    1 4 7 7 4
        Step 6.ix
                A is    5 8 8 9 7

Round #7
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
7, 0, 230, 17 ]
        Step 6.ii
                R is  [ 242, 246, 229, 238, 234, 164, 97, 149, 226,
83, 116, 152, 51, 255, 35, 135 ]
        Step 6.iii
                S is f2f6e5eeeaa46195
        Step 6.iv
                y is  17507433415751000469
        Step 6.v
                m is 5
        Step 6.vi
                c is  14305
        Step 6.vii
                C is    1 4 3 0 5
        Step 6.viii
                B is    5 8 8 9 7
        Step 6.ix
                A is    1 4 3 0 5

Round #6
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
6, 0, 55, 225 ]
        Step 6.ii
                R is  [ 125, 75, 237, 158, 131, 55, 209, 9, 101, 197,
0, 121, 194, 2, 116, 132 ]
        Step 6.iii
                S is 7d4bed9e8337d109
        Step 6.iv
                y is  9028571143056380169
        Step 6.v
                m is 5
        Step 6.vi
                c is  78728
        Step 6.vii
                C is    7 8 7 2 8
        Step 6.viii
                B is    1 4 3 0 5
        Step 6.ix
                A is    7 8 7 2 8

Round #5
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
5, 1, 51, 136 ]
        Step 6.ii
                R is  [ 38, 71, 126, 189, 186, 53, 31, 145, 238, 76,
86, 253, 112, 160, 174, 231 ]
        Step 6.iii
                S is 26477ebdba351f91
        Step 6.iv
                y is  2758312650125680529
        Step 6.v
                m is 5
        Step 6.vi
                c is  33776
        Step 6.vii
                C is    3 3 7 7 6
        Step 6.viii
                B is    7 8 7 2 8
        Step 6.ix
                A is    3 3 7 7 6

Round #4
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
4, 0, 131, 240 ]
        Step 6.ii
                R is  [ 143, 241, 191, 84, 85, 109, 85, 62, 98, 142,
122, 217, 177, 208, 239, 4 ]
        Step 6.iii
                S is 8ff1bf54556d553e
        Step 6.iv
                y is  10372281785742349630
        Step 6.v
```

```
                m is 5
        Step 6.vi
                c is  29098
        Step 6.vii
                C is    2 9 0 9 8
        Step 6.viii
                B is    3 3 7 7 6
        Step 6.ix
                A is    2 9 0 9 8

Round #3
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
3, 0, 113, 170 ]
        Step 6.ii
                R is  [ 174, 123, 224, 87, 184, 248, 56, 84, 44, 10,
27, 227, 157, 233, 178, 91 ]
        Step 6.iii
                S is ae7be057b8f83854
        Step 6.iv
                y is  12572889452104923220
        Step 6.v
                m is 5
        Step 6.vi
                c is  10556
        Step 6.vii
                C is    1 0 5 5 6
        Step 6.viii
                B is    2 9 0 9 8
        Step 6.ix
                A is    1 0 5 5 6

Round #2
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
2, 0, 41, 60 ]
        Step 6.ii
                R is  [ 46, 119, 157, 146, 150, 130, 241, 192, 111,
134, 229, 160, 201, 157, 218, 98 ]
        Step 6.iii
                S is 2e779d929682f1c0
        Step 6.iv
                y is  3348318100889203136
        Step 6.v
                m is 5
        Step 6.vi
                c is  25962
        Step 6.vii
                C is    2 5 9 6 2
        Step 6.viii
```

```
                B is    1 0 5 5 6
        Step 6.ix
                A is    2 5 9 6 2

Round #1
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
1, 0, 101, 106 ]
        Step 6.ii
                R is  [ 51, 190, 249, 61, 4, 109, 120, 103, 51, 255,
70, 97, 20, 140, 87, 153 ]
        Step 6.iii
                S is 33bef93d046d7867
        Step 6.iv
                y is  3728691581971953767
        Step 6.v
                m is 5
        Step 6.vi
                c is  56789
        Step 6.vii
                C is    5 6 7 8 9
        Step 6.viii
                B is    2 5 9 6 2
        Step 6.ix
                A is    5 6 7 8 9

Round #0
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
0, 0, 221, 213 ]
        Step 6.ii
                R is  [ 178, 23, 94, 227, 235, 107, 241, 88, 255, 225,
124, 35, 113, 229, 204, 19 ]
        Step 6.iii
                S is b2175ee3eb6bf158
        Step 6.iv
                y is  12832829996215824728
        Step 6.v
                m is 5
        Step 6.vi
                c is  1234
        Step 6.vii
                C is    0 1 2 3 4
        Step 6.viii
                B is    5 6 7 8 9
        Step 6.ix
                A is    0 1 2 3 4
Step 7
        A || B is    0 1 2 3 4 5 6 7 8 9
```

```
PT is <0123456789>

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

Sample #3

FF1-AES128

Key is 2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C
Radix = 36
--------------------------------------------------------------


PT is <0123456789abcdefghi>

FF1.Encrypt()

X is    0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
Tweak is 37 37 37 37 70 71 72 73 37 37 37

Step 1
        u is 9, v is 10
Step 2
        A is    0 1 2 3 4 5 6 7 8
        B is    9 10 11 12 13 14 15 16 17 18
Step 3
        b is 7
Step 4
        d is 12
Step 5
        P is  [ 1, 2, 1, 0, 0, 36, 10, 9, 0, 0, 0, 19, 0, 0, 0, 11 ]

Round #0
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 89, 199, 207, 155,
163, 54 ]
        Step 6.ii
                R is  [ 6, 251, 135, 106, 117, 248, 75, 85, 167, 247,
46, 141, 81, 123, 105, 129 ]
        Step 6.iii
                S is 06fb876a75f84b55a7f72e8d
        Step 6.iv
                y is  2160989922982028678440365709
        Step 6.v
                m is 9
        Step 6.vi
                c is  86328211778865
        Step 6.vii
                C is    30 21 22 22 28 13 4 26 9
        Step 6.viii
                A is    9 10 11 12 13 14 15 16 17 18
        Step 6.ix
                B is    30 21 22 22 28 13 4 26 9

Round #1
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 78, 131, 218, 101,
173, 49 ]
        Step 6.ii
                R is  [ 234, 197, 139, 125, 49, 154, 29, 140, 64, 194,
47, 243, 194, 238, 169, 76 ]
        Step 6.iii
                S is eac58b7d319a1d8c40c22ff3
        Step 6.iv
                y is  72658309403017157865885544435
        Step 6.v
                m is 10
        Step 6.vi
                c is  2050840795665193
        Step 6.vii
                C is    20 6 34 23 9 6 21 20 4 25
        Step 6.viii
                A is    30 21 22 22 28 13 4 26 9
        Step 6.ix
                B is    20 6 34 23 9 6 21 20 4 25

Round #2
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 7, 73, 58, 149, 29, 211,
41 ]
        Step 6.ii
                R is  [ 37, 33, 19, 155, 176, 144, 199, 195, 108, 53,
208, 135, 86, 238, 38, 253 ]
        Step 6.iii
                S is 2521139bb090c7c36c35d087
        Step 6.iv
                y is  11490932512368444843291431047
        Step 6.v
                m is 9
        Step 6.vi
                c is  62046104419768
        Step 6.vii
                C is    21 35 27 21 4 21 6 29 4
        Step 6.viii
                A is    20 6 34 23 9 6 21 20 4 25
        Step 6.ix
                B is    21 35 27 21 4 21 6 29 4
```

```
Round #3
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 56, 110, 60, 3, 125,
184 ]
        Step 6.ii
                R is  [ 190, 118, 245, 148, 40, 145, 113, 254, 140,
123, 254, 229, 175, 179, 68, 242 ]
        Step 6.iii
                S is be76f594289171fe8c7bfee5
        Step 6.iv
                y is  58945964825599758243647454949
        Step 6.v
                m is 10
        Step 6.vi
                c is  657917498479118
        Step 6.vii
                C is    6 17 7 23 4 19 24 1 28 14
        Step 6.viii
                A is    21 35 27 21 4 21 6 29 4
        Step 6.ix
                B is    6 17 7 23 4 19 24 1 28 14

Round #4
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 2, 86, 95, 90, 201, 210,
14 ]
        Step 6.ii
                R is  [ 190, 6, 122, 0, 221, 107, 29, 148, 239, 20,
204, 3, 65, 191, 89, 232 ]
        Step 6.iii
                S is be067a00dd6b1d94ef14cc03
        Step 6.iv
                y is  58809981565639039559866305539
        Step 6.v
                m is 9
        Step 6.vi
                c is  11087478016443
        Step 6.vii
                C is    3 33 17 18 22 5 2 16 27
        Step 6.viii
                A is    6 17 7 23 4 19 24 1 28 14
        Step 6.ix
                B is    3 33 17 18 22 5 2 16 27

Round #5
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 0, 10, 21, 129, 48, 73,
187 ]
        Step 6.ii
                R is  [ 24, 60, 229, 110, 43, 172, 59, 131, 171, 195,
209, 140, 10, 15, 60, 28 ]
        Step 6.iii
                S is 183ce56e2bac3b83abc3d18c
        Step 6.iv
                y is  7501259239102540333015355788
        Step 6.v
                m is 10
        Step 6.vi
                c is  1474067707044762
        Step 6.vii
                C is    14 18 18 17 12 29 17 2 15 30
        Step 6.viii
                A is    3 33 17 18 22 5 2 16 27
        Step 6.ix
                B is    14 18 18 17 12 29 17 2 15 30

Round #6
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 6, 5, 60, 168, 34, 13, 163,
154 ]
        Step 6.ii
                R is  [ 102, 69, 248, 239, 138, 120, 149, 151, 91,
100, 200, 48, 50, 18, 66, 154 ]
        Step 6.iii
                S is 6645f8ef8a7895975b64c830
        Step 6.iv
                y is  31652062448968081163323492400
        Step 6.v
                m is 9
        Step 6.vi
                c is  16581561225707
        Step 6.vii
                C is    5 31 21 16 25 15 18 0 11
        Step 6.viii
                A is    14 18 18 17 12 29 17 2 15 30
        Step 6.ix
                B is    5 31 21 16 25 15 18 0 11

Round #7
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 7, 0, 15, 20, 178, 17, 17,
235 ]
        Step 6.ii
                R is  [ 216, 147, 240, 22, 142, 188, 102, 147, 1, 98,
89, 224, 215, 167, 201, 78 ]
        Step 6.iii
                S is d893f0168ebc6693016259e0
        Step 6.iv
                y is  67027608000963352100272757216
        Step 6.v
                m is 10
        Step 6.vi
                c is  3562872354372986
        Step 6.vii
                C is    35 2 33 20 34 25 5 21 20 26
        Step 6.viii
                A is    5 31 21 16 25 15 18 0 11
        Step 6.ix
                B is    35 2 33 20 34 25 5 21 20 26

Round #8
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8, 12, 168, 105, 221, 15,
253, 122 ]
        Step 6.ii
                R is  [ 224, 21, 156, 34, 235, 118, 75, 203, 253, 130,
208, 126, 246, 84, 24, 95 ]
        Step 6.iii
                S is e0159c22eb764bcbfd82d07e
        Step 6.iv
                y is  69350766975520660763466453118
        Step 6.v
                m is 9
        Step 6.vi
                c is  28981384438377
        Step 6.vii
                C is    10 9 29 31 4 0 22 21 21
        Step 6.viii
                A is    35 2 33 20 34 25 5 21 20 26
        Step 6.ix
                B is    10 9 29 31 4 0 22 21 21

Round #9
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 9, 0, 26, 91, 193, 31, 226,
105 ]
        Step 6.ii
                R is  [ 163, 250, 122, 135, 113, 186, 179, 153, 25,
193, 9, 244, 214, 165, 149, 93 ]
        Step 6.iii
                S is a3fa7a8771bab39919c109f4
        Step 6.iv
```

```
                y is  50748866682999323485418883572
        Step 6.v
                m is 10
        Step 6.vi
                c is  971546148538222
        Step 6.vii
                C is    9 20 13 30 5 0 9 14 30 22
        Step 6.viii
                A is    10 9 29 31 4 0 22 21 21
        Step 6.ix
                B is    9 20 13 30 5 0 9 14 30 22

Step 7
        A || B is    10 9 29 31 4 0 22 21 21 9 20 13 30 5 0 9 14 30 22

CT is <a9tv40mll9kdu509eum>

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

FF1.Decrypt()

X is    10 9 29 31 4 0 22 21 21 9 20 13 30 5 0 9 14 30 22
Tweak is 37 37 37 37 70 71 72 73 37 37 37

Step 1
        u is 9, v is 10
Step 2
        A is    10 9 29 31 4 0 22 21 21
        B is    9 20 13 30 5 0 9 14 30 22
Step 3
        b is 7
Step 4
        d is 12
Step 5
        P is  [ 1, 2, 1, 0, 0, 36, 10, 9, 0, 0, 0, 19, 0, 0, 0, 11 ]

Round #9
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 9, 0, 26, 91, 193, 31, 226,
105 ]
        Step 6.ii
                R is  [ 163, 250, 122, 135, 113, 186, 179, 153, 25,
193, 9, 244, 214, 165, 149, 93 ]
        Step 6.iii
                S is a3fa7a8771bab39919c109f4
        Step 6.iv
                y is  50748866682999323485418883572
        Step 6.v
                m is 10
        Step 6.vi
                c is  3562872354372986
        Step 6.vii
                C is    35 2 33 20 34 25 5 21 20 26
        Step 6.viii
                B is    10 9 29 31 4 0 22 21 21
        Step 6.ix
                A is    35 2 33 20 34 25 5 21 20 26

Round #8
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8, 12, 168, 105, 221, 15,
253, 122 ]
        Step 6.ii
                R is  [ 224, 21, 156, 34, 235, 118, 75, 203, 253, 130,
208, 126, 246, 84, 24, 95 ]
        Step 6.iii
                S is e0159c22eb764bcbfd82d07e
        Step 6.iv
                y is  69350766975520660763466453118
        Step 6.v
                m is 9
        Step 6.vi
                c is  16581561225707
        Step 6.vii
                C is    5 31 21 16 25 15 18 0 11
        Step 6.viii
                B is    35 2 33 20 34 25 5 21 20 26
        Step 6.ix
                A is    5 31 21 16 25 15 18 0 11

Round #7
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 7, 0, 15, 20, 178, 17, 17,
235 ]
        Step 6.ii
                R is  [ 216, 147, 240, 22, 142, 188, 102, 147, 1, 98,
89, 224, 215, 167, 201, 78 ]
        Step 6.iii
                S is d893f0168ebc6693016259e0
        Step 6.iv
                y is  67027608000963352100272757216
        Step 6.v
                m is 10
        Step 6.vi
                c is  1474067707044762
        Step 6.vii
                C is    14 18 18 17 12 29 17 2 15 30
        Step 6.viii
                B is    5 31 21 16 25 15 18 0 11
        Step 6.ix
                A is    14 18 18 17 12 29 17 2 15 30

Round #6
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 6, 5, 60, 168, 34, 13, 163,
154 ]
        Step 6.ii
                R is  [ 102, 69, 248, 239, 138, 120, 149, 151, 91,
100, 200, 48, 50, 18, 66, 154 ]
        Step 6.iii
                S is 6645f8ef8a7895975b64c830
        Step 6.iv
                y is  31652062448968081163323492400
        Step 6.v
                m is 9
        Step 6.vi
                c is  11087478016443
        Step 6.vii
                C is    3 33 17 18 22 5 2 16 27
        Step 6.viii
                B is    14 18 18 17 12 29 17 2 15 30
        Step 6.ix
                A is    3 33 17 18 22 5 2 16 27

Round #5
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 0, 10, 21, 129, 48, 73,
187 ]
        Step 6.ii
                R is  [ 24, 60, 229, 110, 43, 172, 59, 131, 171, 195,
209, 140, 10, 15, 60, 28 ]
        Step 6.iii
                S is 183ce56e2bac3b83abc3d18c
        Step 6.iv
                y is  7501259239102540333015355788
        Step 6.v
                m is 10
        Step 6.vi
                c is  657917498479118
        Step 6.vii
                C is    6 17 7 23 4 19 24 1 28 14
        Step 6.viii
                B is    3 33 17 18 22 5 2 16 27
        Step 6.ix
                A is    6 17 7 23 4 19 24 1 28 14
```

```
Round #4
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 2, 86, 95, 90, 201, 210,
14 ]
        Step 6.ii
                R is  [ 190, 6, 122, 0, 221, 107, 29, 148, 239, 20,
204, 3, 65, 191, 89, 232 ]
        Step 6.iii
                S is be067a00dd6b1d94ef14cc03
        Step 6.iv
                y is  58809981565639039559866305539
        Step 6.v
                m is 9
        Step 6.vi
                c is  62046104419768
        Step 6.vii
                C is    21 35 27 21 4 21 6 29 4
        Step 6.viii
                B is    6 17 7 23 4 19 24 1 28 14
        Step 6.ix
                A is    21 35 27 21 4 21 6 29 4

Round #3
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 56, 110, 60, 3, 125,
184 ]
        Step 6.ii
                R is  [ 190, 118, 245, 148, 40, 145, 113, 254, 140,
123, 254, 229, 175, 179, 68, 242 ]
        Step 6.iii
                S is be76f594289171fe8c7bfee5
        Step 6.iv
                y is  58945964825599758243647454949
        Step 6.v
                m is 10
        Step 6.vi
                c is  205084079566519 3
        Step 6.vii
                C is    20 6 34 23 9 6 21 20 4 25
        Step 6.viii
                B is    21 35 27 21 4 21 6 29 4
        Step 6.ix
                A is    20 6 34 23 9 6 21 20 4 25

Round #2
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 7, 73, 58, 149, 29, 211,
41 ]
        Step 6.ii
                R is  [ 37, 33, 19, 155, 176, 144, 199, 195, 108, 53,
208, 135, 86, 238, 38, 253 ]
        Step 6.iii
                S is 2521139bb090c7c36c35d087
        Step 6.iv
                y is  1149093251236844843291431047
        Step 6.v
                m is 9
        Step 6.vi
                c is  86328211778865
        Step 6.vii
                C is    30 21 22 22 28 13 4 26 9
        Step 6.viii
                B is    20 6 34 23 9 6 21 20 4 25
        Step 6.ix
                A is    30 21 22 22 28 13 4 26 9

Round #1
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 78, 131, 218, 101,
173, 49 ]
        Step 6.ii
                R is  [ 234, 197, 139, 125, 49, 154, 29, 140, 64, 194,
47, 243, 194, 238, 169, 76 ]
        Step 6.iii
                S is eac58b7d319a1d8c40c22ff3
        Step 6.iv
                y is  7265830940301715786588554435
        Step 6.v
                m is 10
        Step 6.vi
                c is  943139646579510
        Step 6.vii
                C is    9 10 11 12 13 14 15 16 17 18
        Step 6.viii
                B is    30 21 22 22 28 13 4 26 9
        Step 6.ix
                A is    9 10 11 12 13 14 15 16 17 18

Round #0
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 89, 199, 207, 155,
163, 54 ]
        Step 6.ii
                R is  [ 6, 251, 135, 106, 117, 248, 75, 85, 167, 247,
46, 141, 81, 123, 105, 129 ]
        Step 6.iii
                S is 06fb876a75f84b55a7f72e8d
        Step 6.iv
                y is  2160989922982028678440365709
        Step 6.v
                m is 9
        Step 6.vi
                c is  82906087076
        Step 6.vii
                C is    0 1 2 3 4 5 6 7 8
        Step 6.viii
                B is    9 10 11 12 13 14 15 16 17 18
        Step 6.ix
                A is    0 1 2 3 4 5 6 7 8
Step 7
        A || B is    0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18

PT is <0123456789abcdefghi>

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

Sample #4

FF1-AES192

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


PT is <0123456789>

FF1.Encrypt()

X is    0 1 2 3 4 5 6 7 8 9
Tweak is <empty>

Step 1
        u is 5, v is 5
Step 2
        A is    0 1 2 3 4
        B is    5 6 7 8 9
Step 3
        b is 3
Step 4
        d is 8
Step 5
        P is  [ 1, 2, 1, 0, 0, 10, 10, 5, 0, 0, 0, 10, 0, 0, 0, 0 ]
```

```
Round #0
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 221,
213 ]
        Step 6.ii
                R is  [ 218, 224, 209, 93, 155, 127, 33, 31, 56, 9,
56, 226, 148, 92, 125, 83 ]
        Step 6.iii
                S is dae0d15d9b7f211f
        Step 6.iv
                y is  15771836095022440735
        Step 6.v
                m is 5
        Step 6.vi
                c is  41969
        Step 6.vii
                C is    4 1 9 6 9
        Step 6.viii
                A is    5 6 7 8 9
        Step 6.ix
                B is    4 1 9 6 9

Round #1
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 163,
241 ]
        Step 6.ii
                R is  [ 248, 93, 91, 186, 160, 60, 208, 226, 105, 124,
242, 50, 99, 186, 30, 131 ]
        Step 6.iii
                S is f85d5bbaa03cd0e2
        Step 6.iv
                y is  17896561351350604002
        Step 6.v
                m is 5
        Step 6.vi
                c is  60791
        Step 6.vii
                C is    6 0 7 9 1
        Step 6.viii
                A is    4 1 9 6 9
        Step 6.ix
                B is    6 0 7 9 1

Round #2
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 237,
119 ]
        Step 6.ii
```

```
                R is  [ 245, 226, 145, 48, 198, 231, 145, 104, 47,
175, 248, 143, 17, 27, 248, 14 ]
        Step 6.iii
                S is f5e29130c6e79168
        Step 6.iv
                y is  17717883522710475112
        Step 6.v
                m is 5
        Step 6.vi
                c is  17081
        Step 6.vii
                C is    1 7 0 8 1
        Step 6.viii
                A is    6 0 7 9 1
        Step 6.ix
                B is    1 7 0 8 1

Round #3
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 66,
185 ]
        Step 6.ii
                R is  [ 183, 184, 63, 73, 147, 0, 59, 248, 121, 146,
109, 188, 87, 255, 122, 41 ]
        Step 6.iii
                S is b7b83f4993003bf8
        Step 6.iv
                y is  13238400689887001592
        Step 6.v
                m is 5
        Step 6.vi
                c is  62383
        Step 6.vii
                C is    6 2 3 8 3
        Step 6.viii
                A is    1 7 0 8 1
        Step 6.ix
                B is    6 2 3 8 3

Round #4
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 0, 243,
175 ]
        Step 6.ii
                R is  [ 186, 50, 129, 208, 56, 210, 79, 221, 252, 195,
36, 1, 252, 128, 36, 228 ]
        Step 6.iii
                S is ba3281d038d24fdd
        Step 6.iv
                y is  13416928971196616669
        Step 6.v
                m is 5
        Step 6.vi
                c is  33750
        Step 6.vii
                C is    3 3 7 5 0
        Step 6.viii
                A is    6 2 3 8 3
        Step 6.ix
                B is    3 3 7 5 0

Round #5
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 0, 131,
214 ]
        Step 6.ii
                R is  [ 64, 98, 46, 91, 23, 106, 173, 17, 139, 88, 99,
107, 33, 245, 227, 144 ]
        Step 6.iii
                S is 40622e5b176aad11
        Step 6.iv
                y is  4639321534914800913
        Step 6.v
                m is 5
        Step 6.vi
                c is  63296
        Step 6.vii
                C is    6 3 2 9 6
        Step 6.viii
                A is    3 3 7 5 0
        Step 6.ix
                B is    6 3 2 9 6

Round #6
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 6, 0, 247,
64 ]
        Step 6.ii
                R is  [ 83, 25, 142, 32, 135, 231, 170, 153, 228, 117,
228, 10, 15, 160, 193, 187 ]
        Step 6.iii
                S is 53198e2087e7aa99
        Step 6.iv
                y is  5987973449935989401
        Step 6.v
                m is 5
        Step 6.vi
                c is  23151
        Step 6.vii
                C is    2 3 1 5 1
        Step 6.viii
                A is    6 3 2 9 6
        Step 6.ix
                B is    2 3 1 5 1

Round #7
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 7, 0, 90,
111 ]
        Step 6.ii
                R is  [ 6, 60, 69, 210, 248, 212, 27, 65, 129, 80,
127, 172, 156, 189, 243, 222 ]
        Step 6.iii
                S is 063c45d2f8d41b41
        Step 6.iv
                y is  449310835250305857
        Step 6.v
                m is 5
        Step 6.vi
                c is  69153
        Step 6.vii
                C is    6 9 1 5 3
        Step 6.viii
                A is    2 3 1 5 1
        Step 6.ix
                B is    6 9 1 5 3

Round #8
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8, 1, 14,
33 ]
        Step 6.ii
                R is  [ 44, 180, 177, 187, 210, 235, 159, 163, 172,
17, 83, 47, 25, 2, 246, 150 ]
        Step 6.iii
                S is 2cb4b1bbd2eb9fa3
        Step 6.iv
                y is  3221395053732405155
        Step 6.v
                m is 5
        Step 6.vi
                c is  28306
        Step 6.vii
                C is    2 8 3 0 6
        Step 6.viii
                A is    6 9 1 5 3
        Step 6.ix
                B is    2 8 3 0 6

Round #9
```

```
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 9, 0, 110,
146 ]
        Step 6.ii
                R is  [ 166, 31, 223, 78, 22, 140, 56, 3, 50, 112,
162, 234, 33, 174, 46, 146 ]
        Step 6.iii
                S is a61fdf4e168c3803
        Step 6.iv
                y is  11970531861052798979
        Step 6.v
                m is 5
        Step 6.vi
                c is  68132
        Step 6.vii
                C is    6 8 1 3 2
        Step 6.viii
                A is    2 8 3 0 6
        Step 6.ix
                B is    6 8 1 3 2

Step 7
        A || B is    2 8 3 0 6 6 8 1 3 2

CT is <2830668132>

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

FF1.Decrypt()

X is    2 8 3 0 6 6 8 1 3 2
Tweak is <empty>

Step 1
        u is 5, v is 5
Step 2
        A is    2 8 3 0 6
        B is    6 8 1 3 2
Step 3
        b is 3
Step 4
        d is 8
Step 5
        P is  [ 1, 2, 1, 0, 0, 10, 10, 5, 0, 0, 0, 10, 0, 0, 0, 0 ]

Round #9
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 9, 0, 110,
146 ]
        Step 6.ii
```

```
                R is  [ 166, 31, 223, 78, 22, 140, 56, 3, 50, 112, 
162, 234, 33, 174, 46, 146 ]
        Step 6.iii
                S is a61fdf4e168c3803
        Step 6.iv
                y is  11970531861052798979
        Step 6.v
                m is 5
        Step 6.vi
                c is  69153
        Step 6.vii
                C is    6 9 1 5 3
        Step 6.viii
                B is    2 8 3 0 6
        Step 6.ix
                A is    6 9 1 5 3

Round #8
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8, 1, 14, 
33 ]
        Step 6.ii
                R is  [ 44, 180, 177, 187, 210, 235, 159, 163, 172, 
17, 83, 47, 25, 2, 246, 150 ]
        Step 6.iii
                S is 2cb4b1bbd2eb9fa3
        Step 6.iv
                y is  3221395053732405155
        Step 6.v
                m is 5
        Step 6.vi
                c is  23151
        Step 6.vii
                C is    2 3 1 5 1
        Step 6.viii
                B is    6 9 1 5 3
        Step 6.ix
                A is    2 3 1 5 1

Round #7
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 7, 0, 90, 
111 ]
        Step 6.ii
                R is  [ 6, 60, 69, 210, 248, 212, 27, 65, 129, 80, 
127, 172, 156, 189, 243, 222 ]
        Step 6.iii
                S is 063c45d2f8d41b41
        Step 6.iv
                y is  449310835250305857
        Step 6.v
                m is 5
        Step 6.vi
                c is  63296
        Step 6.vii
                C is    6 3 2 9 6
        Step 6.viii
                B is    2 3 1 5 1
        Step 6.ix
                A is    6 3 2 9 6

Round #6
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 6, 0, 247,
64 ]
        Step 6.ii
                R is  [ 83, 25, 142, 32, 135, 231, 170, 153, 228, 117,
228, 10, 15, 160, 193, 187 ]
        Step 6.iii
                S is 53198e2087e7aa99
        Step 6.iv
                y is  5987973449935989401
        Step 6.v
                m is 5
        Step 6.vi
                c is  33750
        Step 6.vii
                C is    3 3 7 5 0
        Step 6.viii
                B is    6 3 2 9 6
        Step 6.ix
                A is    3 3 7 5 0

Round #5
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 0, 131,
214 ]
        Step 6.ii
                R is  [ 64, 98, 46, 91, 23, 106, 173, 17, 139, 88, 99,
107, 33, 245, 227, 144 ]
        Step 6.iii
                S is 40622e5b176aad11
        Step 6.iv
                y is  4639321534914800913
        Step 6.v
                m is 5
        Step 6.vi
                c is  62383
        Step 6.vii
                C is    6 2 3 8 3
        Step 6.viii
                B is    3 3 7 5 0
        Step 6.ix
                A is    6 2 3 8 3

Round #4
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 0, 243,
175 ]
        Step 6.ii
                R is  [ 186, 50, 129, 208, 56, 210, 79, 221, 252, 195,
36, 1, 252, 128, 36, 228 ]
        Step 6.iii
                S is ba3281d038d24fdd
        Step 6.iv
                y is  13416928971196616669
        Step 6.v
                m is 5
        Step 6.vi
                c is  17081
        Step 6.vii
                C is    1 7 0 8 1
        Step 6.viii
                B is    6 2 3 8 3
        Step 6.ix
                A is    1 7 0 8 1

Round #3
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 66,
185 ]
        Step 6.ii
                R is  [ 183, 184, 63, 73, 147, 0, 59, 248, 121, 146,
109, 188, 87, 255, 122, 41 ]
        Step 6.iii
                S is b7b83f4993003bf8
        Step 6.iv
                y is  13238400689887001592
        Step 6.v
                m is 5
        Step 6.vi
                c is  60791
        Step 6.vii
                C is    6 0 7 9 1
        Step 6.viii
                B is    1 7 0 8 1
        Step 6.ix
                A is    6 0 7 9 1

Round #2
```

```
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 237,
119 ]
        Step 6.ii
                R is  [ 245, 226, 145, 48, 198, 231, 145, 104, 47,
175, 248, 143, 17, 27, 248, 14 ]
        Step 6.iii
                S is f5e29130c6e79168
        Step 6.iv
                y is  17717883522710475112
        Step 6.v
                m is 5
        Step 6.vi
                c is  41969
        Step 6.vii
                C is    4 1 9 6 9
        Step 6.viii
                B is    6 0 7 9 1
        Step 6.ix
                A is    4 1 9 6 9

Round #1
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 163,
241 ]
        Step 6.ii
                R is  [ 248, 93, 91, 186, 160, 60, 208, 226, 105, 124,
242, 50, 99, 186, 30, 131 ]
        Step 6.iii
                S is f85d5bbaa03cd0e2
        Step 6.iv
                y is  17896561351350604002
        Step 6.v
                m is 5
        Step 6.vi
                c is  56789
        Step 6.vii
                C is    5 6 7 8 9
        Step 6.viii
                B is    4 1 9 6 9
        Step 6.ix
                A is    5 6 7 8 9

Round #0
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 221,
213 ]
        Step 6.ii
                R is  [ 218, 224, 209, 93, 155, 127, 33, 31, 56, 9,
56, 226, 148, 92, 125, 83 ]
```

```
        Step 6.iii
                S is dae0d15d9b7f211f
        Step 6.iv
                y is  15771836095022440735
        Step 6.v
                m is 5
        Step 6.vi
                c is  1234
        Step 6.vii
                C is    0 1 2 3 4
        Step 6.viii
                B is    5 6 7 8 9
        Step 6.ix
                A is    0 1 2 3 4
Step 7
        A || B is    0 1 2 3 4 5 6 7 8 9

PT is <0123456789>

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

Sample #5

FF1-AES192

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


PT is <0123456789>

FF1.Encrypt()

X is    0 1 2 3 4 5 6 7 8 9
Tweak is 39 38 37 36 35 34 33 32 31 30

Step 1
        u is 5, v is 5
Step 2
        A is    0 1 2 3 4
        B is    5 6 7 8 9
Step 3
        b is 3
Step 4
        d is 8
Step 5
        P is  [ 1, 2, 1, 0, 0, 10, 10, 5, 0, 0, 0, 10, 0, 0, 0, 10 ]
```

```
Round #0
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
0, 0, 221, 213 ]
        Step 6.ii
                R is  [ 112, 16, 205, 170, 62, 50, 190, 188, 155, 253,
85, 202, 210, 92, 216, 16 ]
        Step 6.iii
                S is 7010cdaa3e32bebc
        Step 6.iv
                y is  8075180262946946748
        Step 6.v
                m is 5
        Step 6.vi
                c is  47982
        Step 6.vii
                C is    4 7 9 8 2
        Step 6.viii
                A is    5 6 7 8 9
        Step 6.ix
                B is    4 7 9 8 2

Round #1
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
1, 0, 187, 110 ]
        Step 6.ii
                R is  [ 110, 183, 202, 34, 97, 2, 82, 23, 236, 94, 6,
159, 169, 202, 154, 67 ]
        Step 6.iii
                S is 6eb7ca2261025217
        Step 6.iv
                y is  7978067513915363863
        Step 6.v
                m is 5
        Step 6.vi
                c is  20652
        Step 6.vii
                C is    2 0 6 5 2
        Step 6.viii
                A is    4 7 9 8 2
        Step 6.ix
                B is    2 0 6 5 2

Round #2
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
2, 0, 80, 172 ]
        Step 6.ii
                R is  [ 77, 185, 202, 213, 23, 247, 236, 146, 216, 16,
80, 114, 81, 64, 194, 156 ]
        Step 6.iii
                S is 4db9cad517f7ec92
        Step 6.iv
                y is  5600730628190891154
        Step 6.v
                m is 5
        Step 6.vi
                c is  39136
        Step 6.vii
                C is    3 9 1 3 6
        Step 6.viii
                A is    2 0 6 5 2
        Step 6.ix
                B is    3 9 1 3 6

Round #3
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
3, 0, 152, 224 ]
        Step 6.ii
                R is  [ 248, 131, 99, 76, 163, 213, 249, 170, 207,
246, 88, 18, 149, 117, 206, 201 ]
        Step 6.iii
                S is f883634ca3d5f9aa
        Step 6.iv
                y is  17907265724172597674
        Step 6.v
                m is 5
        Step 6.vi
                c is  18326
        Step 6.vii
                C is    1 8 3 2 6
        Step 6.viii
                A is    3 9 1 3 6
        Step 6.ix
                B is    1 8 3 2 6

Round #4
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
4, 0, 71, 150 ]
        Step 6.ii
                R is  [ 232, 173, 241, 62, 215, 103, 225, 236, 213,
219, 131, 232, 209, 121, 131, 85 ]
        Step 6.iii
                S is e8adf13ed767e1ec
        Step 6.iv
                y is  16766322239974400492
        Step 6.v
```

```
                m is 5
        Step 6.vi
                c is  39628
        Step 6.vii
                C is    3 9 6 2 8
        Step 6.viii
                A is    1 8 3 2 6
        Step 6.ix
                B is    3 9 6 2 8

Round #5
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
5, 0, 154, 204 ]
        Step 6.ii
                R is  [ 243, 200, 197, 156, 194, 73, 229, 96, 210,
102, 198, 51, 88, 117, 150, 183 ]
        Step 6.iii
                S is f3c8c59cc249e560
        Step 6.iv
                y is  17566507623623812448
        Step 6.v
                m is 5
        Step 6.vi
                c is  30774
        Step 6.vii
                C is    3 0 7 7 4
        Step 6.viii
                A is    3 9 6 2 8
        Step 6.ix
                B is    3 0 7 7 4

Round #6
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
6, 0, 120, 54 ]
        Step 6.ii
                R is  [ 22, 49, 140, 229, 78, 126, 128, 124, 96, 168,
14, 191, 118, 196, 3, 159 ]
        Step 6.iii
                S is 16318ce54e7e807c
        Step 6.iv
                y is  1599214259185549436
        Step 6.v
                m is 5
        Step 6.vi
                c is  89064
        Step 6.vii
                C is    8 9 0 6 4
        Step 6.viii
```

```
                A is    3 0 7 7 4
        Step 6.ix
                B is    8 9 0 6 4

Round #7
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
7, 1, 91, 232 ]
        Step 6.ii
                R is  [ 201, 231, 34, 87, 24, 209, 194, 187, 141, 236,
62, 170, 118, 31, 102, 254 ]
        Step 6.iii
                S is c9e7225718d1c2bb
        Step 6.iv
                y is  14548634878717575867
        Step 6.v
                m is 5
        Step 6.vi
                c is  6641
        Step 6.vii
                C is    0 6 6 4 1
        Step 6.viii
                A is    8 9 0 6 4
        Step 6.ix
                B is    0 6 6 4 1

Round #8
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
8, 0, 25, 241 ]
        Step 6.ii
                R is  [ 232, 57, 243, 35, 205, 180, 65, 30, 157, 118,
122, 9, 50, 76, 141, 147 ]
        Step 6.iii
                S is e839f323cdb4411e
        Step 6.iv
                y is  16733673225572335902
        Step 6.v
                m is 5
        Step 6.vi
                c is  24966
        Step 6.vii
                C is    2 4 9 6 6
        Step 6.viii
                A is    0 6 6 4 1
        Step 6.ix
                B is    2 4 9 6 6

Round #9
        Step 6.i
```

```
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
9, 0, 97, 134 ]
        Step 6.ii
                R is  [ 171, 238, 207, 235, 71, 34, 238, 44, 25, 22,
131, 21, 159, 75, 228, 55 ]
        Step 6.iii
                S is abeecfeb4722ee2c
        Step 6.iv
                y is  12389068234360548908
        Step 6.v
                m is 5
        Step 6.vi
                c is  55549
        Step 6.vii
                C is    5 5 5 4 9
        Step 6.viii
                A is    2 4 9 6 6
        Step 6.ix
                B is    5 5 5 4 9

Step 7
        A || B is    2 4 9 6 6 5 5 5 4 9

CT is <2496655549>

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

FF1.Decrypt()

X is    2 4 9 6 6 5 5 5 4 9
Tweak is 39 38 37 36 35 34 33 32 31 30

Step 1
        u is 5, v is 5
Step 2
        A is    2 4 9 6 6
        B is    5 5 5 4 9
Step 3
        b is 3
Step 4
        d is 8
Step 5
        P is  [ 1, 2, 1, 0, 0, 10, 10, 5, 0, 0, 0, 10, 0, 0, 0, 10 ]

Round #9
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
9, 0, 97, 134 ]
        Step 6.ii
                R is  [ 171, 238, 207, 235, 71, 34, 238, 44, 25, 22,
131, 21, 159, 75, 228, 55 ]
        Step 6.iii
                S is abeecfeb4722ee2c
        Step 6.iv
                y is  12389068234360548908
        Step 6.v
                m is 5
        Step 6.vi
                c is  6641
        Step 6.vii
                C is    0 6 6 4 1
        Step 6.viii
                B is    2 4 9 6 6
        Step 6.ix
                A is    0 6 6 4 1

Round #8
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
8, 0, 25, 241 ]
        Step 6.ii
                R is  [ 232, 57, 243, 35, 205, 180, 65, 30, 157, 118,
122, 9, 50, 76, 141, 147 ]
        Step 6.iii
                S is e839f323cdb4411e
        Step 6.iv
                y is  16733673225572335902
        Step 6.v
                m is 5
        Step 6.vi
                c is  89064
        Step 6.vii
                C is    8 9 0 6 4
        Step 6.viii
                B is    0 6 6 4 1
        Step 6.ix
                A is    8 9 0 6 4

Round #7
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
7, 1, 91, 232 ]
        Step 6.ii
                R is  [ 201, 231, 34, 87, 24, 209, 194, 187, 141, 236,
62, 170, 118, 31, 102, 254 ]
        Step 6.iii
                S is c9e7225718d1c2bb
        Step 6.iv
                y is  14548634878717575867
        Step 6.v
```

```
                m is 5
        Step 6.vi
                c is  30774
        Step 6.vii
                C is    3 0 7 7 4
        Step 6.viii
                B is    8 9 0 6 4
        Step 6.ix
                A is    3 0 7 7 4

Round #6
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
6, 0, 120, 54 ]
        Step 6.ii
                R is  [ 22, 49, 140, 229, 78, 126, 128, 124, 96, 168,
14, 191, 118, 196, 3, 159 ]
        Step 6.iii
                S is 16318ce54e7e807c
        Step 6.iv
                y is  1599214259185549436
        Step 6.v
                m is 5
        Step 6.vi
                c is  39628
        Step 6.vii
                C is    3 9 6 2 8
        Step 6.viii
                B is    3 0 7 7 4
        Step 6.ix
                A is    3 9 6 2 8

Round #5
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
5, 0, 154, 204 ]
        Step 6.ii
                R is  [ 243, 200, 197, 156, 194, 73, 229, 96, 210,
102, 198, 51, 88, 117, 150, 183 ]
        Step 6.iii
                S is f3c8c59cc249e560
        Step 6.iv
                y is  17566507623623812448
        Step 6.v
                m is 5
        Step 6.vi
                c is  18326
        Step 6.vii
                C is    1 8 3 2 6
        Step 6.viii
```

```
                B is    3 9 6 2 8
        Step 6.ix
                A is    1 8 3 2 6

Round #4
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
4, 0, 71, 150 ]
        Step 6.ii
                R is  [ 232, 173, 241, 62, 215, 103, 225, 236, 213,
219, 131, 232, 209, 121, 131, 85 ]
        Step 6.iii
                S is e8adf13ed767e1ec
        Step 6.iv
                y is  16766322239974400492
        Step 6.v
                m is 5
        Step 6.vi
                c is  39136
        Step 6.vii
                C is    3 9 1 3 6
        Step 6.viii
                B is    1 8 3 2 6
        Step 6.ix
                A is    3 9 1 3 6

Round #3
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
3, 0, 152, 224 ]
        Step 6.ii
                R is  [ 248, 131, 99, 76, 163, 213, 249, 170, 207,
246, 88, 18, 149, 117, 206, 201 ]
        Step 6.iii
                S is f883634ca3d5f9aa
        Step 6.iv
                y is  17907265724172597674
        Step 6.v
                m is 5
        Step 6.vi
                c is  20652
        Step 6.vii
                C is    2 0 6 5 2
        Step 6.viii
                B is    3 9 1 3 6
        Step 6.ix
                A is    2 0 6 5 2

Round #2
        Step 6.i
```

```
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
2, 0, 80, 172 ]
        Step 6.ii
                R is  [ 77, 185, 202, 213, 23, 247, 236, 146, 216, 16,
80, 114, 81, 64, 194, 156 ]
        Step 6.iii
                S is 4db9cad517f7ec92
        Step 6.iv
                y is  5600730628190891154
        Step 6.v
                m is 5
        Step 6.vi
                c is  47982
        Step 6.vii
                C is    4 7 9 8 2
        Step 6.viii
                B is    2 0 6 5 2
        Step 6.ix
                A is    4 7 9 8 2

Round #1
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
1, 0, 187, 110 ]
        Step 6.ii
                R is  [ 110, 183, 202, 34, 97, 2, 82, 23, 236, 94, 6,
159, 169, 202, 154, 67 ]
        Step 6.iii
                S is 6eb7ca2261025217
        Step 6.iv
                y is  7978067513915363863
        Step 6.v
                m is 5
        Step 6.vi
                c is  56789
        Step 6.vii
                C is    5 6 7 8 9
        Step 6.viii
                B is    4 7 9 8 2
        Step 6.ix
                A is    5 6 7 8 9

Round #0
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
0, 0, 221, 213 ]
        Step 6.ii
                R is  [ 112, 16, 205, 170, 62, 50, 190, 188, 155, 253,
85, 202, 210, 92, 216, 16 ]
        Step 6.iii
```

```
                S is 7010cdaa3e32bebc
        Step 6.iv
                y is  8075180262946946748
        Step 6.v
                m is 5
        Step 6.vi
                c is  1234
        Step 6.vii
                C is    0 1 2 3 4
        Step 6.viii
                B is    5 6 7 8 9
        Step 6.ix
                A is    0 1 2 3 4
Step 7
        A || B is    0 1 2 3 4 5 6 7 8 9

PT is <0123456789>

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

Sample #6

FF1-AES192

Key is 2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C EF 43 59 D8 D5
80 AA 4F
Radix = 36
--------------------------------------------------------------


PT is <0123456789abcdefghi>

FF1.Encrypt()

X is    0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
Tweak is 37 37 37 37 70 71 72 73 37 37 37

Step 1
        u is 9, v is 10
Step 2
        A is    0 1 2 3 4 5 6 7 8
        B is    9 10 11 12 13 14 15 16 17 18
Step 3
        b is 7
Step 4
        d is 12
Step 5
        P is  [ 1, 2, 1, 0, 0, 36, 10, 9, 0, 0, 0, 19, 0, 0, 0, 11 ]

Round #0
```

```
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 89, 199, 207, 155,
163, 54 ]
        Step 6.ii
                R is  [ 225, 238, 247, 123, 137, 230, 22, 54, 5, 163,
154, 25, 218, 40, 23, 48 ]
        Step 6.iii
                S is e1eef77b89e6163605a39a19
        Step 6.iv
                y is  69923020258278366124416670233
        Step 6.v
                m is 9
        Step 6.vi
                c is  74443406317757
        Step 6.vii
                C is    26 13 34 29 30 1 28 19 17
        Step 6.viii
                A is    9 10 11 12 13 14 15 16 17 18
        Step 6.ix
                B is    26 13 34 29 30 1 28 19 17

Round #1
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 67, 180, 180, 202,
24, 189 ]
        Step 6.ii
                R is  [ 11, 66, 76, 139, 82, 150, 184, 220, 184, 125,
202, 48, 68, 104, 44, 131 ]
        Step 6.iii
                S is 0b424c8b5296b8dcb87dca30
        Step 6.iv
                y is  3484485682030632835911371312
        Step 6.v
                m is 10
        Step 6.vi
                c is  887248406539622
        Step 6.vii
                C is    8 26 18 4 10 17 6 15 21 2
        Step 6.viii
                A is    26 13 34 29 30 1 28 19 17
        Step 6.ix
                B is    8 26 18 4 10 17 6 15 21 2

Round #2
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 3, 38, 242, 158, 25,
109, 102 ]
```

```
        Step 6.ii
                R is  [ 160, 235, 56, 15, 222, 178, 107, 202, 91, 205,
232, 58, 168, 245, 133, 82 ]
        Step 6.iii
                S is a0eb380fdeb26bca5bcde83a
        Step 6.iv
                y is  49801963884295857596938446906
        Step 6.v
                m is 9
        Step 6.vi
                c is  30411825086711
        Step 6.vii
                C is    10 28 2 35 35 16 2 27 11
        Step 6.viii
                A is    8 26 18 4 10 17 6 15 21 2
        Step 6.ix
                B is    10 28 2 35 35 16 2 27 11

Round #3
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 27, 168, 206, 8, 0,
247 ]
        Step 6.ii
                R is  [ 210, 168, 189, 131, 204, 156, 173, 50, 164,
116, 195, 152, 23, 34, 66, 112 ]
        Step 6.iii
                S is d2a8bd83cc9cad32a474c398
        Step 6.iv
                y is  65195846558710307865574556568
        Step 6.v
                m is 10
        Step 6.vi
                c is  2463858254819582
        Step 6.vii
                C is    24 9 13 4 30 29 35 16 1 26
        Step 6.viii
                A is    10 28 2 35 35 16 2 27 11
        Step 6.ix
                B is    24 9 13 4 30 29 35 16 1 26

Round #4
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 8, 192, 221, 180, 14,
48, 254 ]
        Step 6.ii
                R is  [ 50, 228, 242, 3, 81, 153, 230, 28, 225, 33,
253, 16, 5, 235, 47, 133 ]
        Step 6.iii
```

```
                S is 32e4f2035199e61ce121fd10
        Step 6.iv
                y is  15751028451848459363561897232
        Step 6.v
                m is 9
        Step 6.vi
                c is  3710307925511
        Step 6.vii
                C is    1 11 12 17 25 19 17 29 35
        Step 6.viii
                A is    24 9 13 4 30 29 35 16 1 26
        Step 6.ix
                B is    1 11 12 17 25 19 17 29 35

Round #5
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 0, 3, 95, 223, 149, 254,
7 ]
        Step 6.ii
                R is  [ 20, 139, 225, 142, 115, 92, 228, 59, 37, 141,
157, 233, 13, 24, 120, 20 ]
        Step 6.iii
                S is 148be18e735ce43b258d9de9
        Step 6.iv
                y is  6358806045562408921612525033
        Step 6.v
                m is 10
        Step 6.vi
                c is  505986281098983
        Step 6.vii
                C is    4 35 12 30 31 35 21 5 23 27
        Step 6.viii
                A is    1 11 12 17 25 19 17 29 35
        Step 6.ix
                B is    4 35 12 30 31 35 21 5 23 27

Round #6
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 6, 1, 204, 49, 28, 139,
206, 231 ]
        Step 6.ii
                R is  [ 111, 210, 244, 114, 175, 68, 226, 88, 28, 15,
237, 141, 213, 149, 8, 140 ]
        Step 6.iii
                S is 6fd2f472af44e2581c0fed8d
        Step 6.iv
                y is  34607864885268487474569538957
        Step 6.v
```

```
                m is 9
        Step 6.vi
                c is  83995813604244
        Step 6.vii
                C is    29 27 31 5 6 25 23 6 12
        Step 6.viii
                A is    4 35 12 30 31 35 21 5 23 27
        Step 6.ix
                B is    29 27 31 5 6 25 23 6 12

Round #7
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 7, 0, 76, 100, 204, 161,
235, 148 ]
        Step 6.ii
                R is  [ 249, 112, 52, 211, 119, 17, 237, 12, 232, 70,
240, 146, 159, 96, 189, 19 ]
        Step 6.iii
                S is f97034d37711ed0ce846f092
        Step 6.iv
                y is  77197416601211768759113937042
        Step 6.v
                m is 10
        Step 6.vi
                c is  1678890359766905
        Step 6.vii
                C is    16 19 4 7 21 0 19 16 26 17
        Step 6.viii
                A is    29 27 31 5 6 25 23 6 12
        Step 6.ix
                B is    16 19 4 7 21 0 19 16 26 17

Round #8
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8, 5, 246, 241, 31, 130,
191, 121 ]
        Step 6.ii
                R is  [ 243, 10, 51, 1, 73, 227, 154, 9, 74, 56, 166,
35, 13, 232, 47, 130 ]
        Step 6.iii
                S is f30a330149e39a094a38a623
        Step 6.iv
                y is  75217187509244636966656976419
        Step 6.v
                m is 9
        Step 6.vi
                c is  94000208056759
        Step 6.vii
```

```
                C is    33 11 19 3 20 31 3 5 19
        Step 6.viii
                A is    16 19 4 7 21 0 19 16 26 17
        Step 6.ix
                B is    33 11 19 3 20 31 3 5 19

Round #9
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 9, 0, 85, 126, 33, 2, 145,
183 ]
        Step 6.ii
                R is  [ 46, 192, 125, 183, 222, 27, 102, 190, 19, 229,
44, 50, 183, 135, 221, 189 ]
        Step 6.iii
                S is 2ec07db7de1b66be13e52c32
        Step 6.iv
                y is  144690178967169048247379671 54
        Step 6.v
                m is 10
        Step 6.vi
                c is  2772911295818667
        Step 6.vii
                C is    27 10 32 33 31 3 2 34 28 27
        Step 6.viii
                A is    33 11 19 3 20 31 3 5 19
        Step 6.ix
                B is    27 10 32 33 31 3 2 34 28 27

Step 7
        A || B is    33 11 19 3 20 31 3 5 19 27 10 32 33 31 3 2 34 28
27

CT is <xbj3kv35jrawxv32ysr>

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

FF1.Decrypt()

X is    33 11 19 3 20 31 3 5 19 27 10 32 33 31 3 2 34 28 27
Tweak is 37 37 37 37 70 71 72 73 37 37 37

Step 1
        u is 9, v is 10
Step 2
        A is    33 11 19 3 20 31 3 5 19
        B is    27 10 32 33 31 3 2 34 28 27
Step 3
        b is 7
Step 4
```

```
        d is 12
Step 5
        P is  [ 1, 2, 1, 0, 0, 36, 10, 9, 0, 0, 0, 19, 0, 0, 0, 11 ]

Round #9
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 9, 0, 85, 126, 33, 2, 145,
183 ]
        Step 6.ii
                R is  [ 46, 192, 125, 183, 222, 27, 102, 190, 19, 229,
44, 50, 183, 135, 221, 189 ]
        Step 6.iii
                S is 2ec07db7de1b66be13e52c32
        Step 6.iv
                y is  14469017896716904824737967154
        Step 6.v
                m is 10
        Step 6.vi
                c is  1678890359766905
        Step 6.vii
                C is    16 19 4 7 21 0 19 16 26 17
        Step 6.viii
                B is    33 11 19 3 20 31 3 5 19
        Step 6.ix
                A is    16 19 4 7 21 0 19 16 26 17

Round #8
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8, 5, 246, 241, 31, 130,
191, 121 ]
        Step 6.ii
                R is  [ 243, 10, 51, 1, 73, 227, 154, 9, 74, 56, 166,
35, 13, 232, 47, 130 ]
        Step 6.iii
                S is f30a330149e39a094a38a623
        Step 6.iv
                y is  75217187509244636966656976419
        Step 6.v
                m is 9
        Step 6.vi
                c is  83995813604244
        Step 6.vii
                C is    29 27 31 5 6 25 23 6 12
        Step 6.viii
                B is    16 19 4 7 21 0 19 16 26 17
        Step 6.ix
                A is    29 27 31 5 6 25 23 6 12
```

```
Round #7
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 7, 0, 76, 100, 204, 161,
235, 148 ]
        Step 6.ii
                R is  [ 249, 112, 52, 211, 119, 17, 237, 12, 232, 70,
240, 146, 159, 96, 189, 19 ]
        Step 6.iii
                S is f97034d37711ed0ce846f092
        Step 6.iv
                y is  77197416601211768759113937042
        Step 6.v
                m is 10
        Step 6.vi
                c is  505986281098983
        Step 6.vii
                C is    4 35 12 30 31 35 21 5 23 27
        Step 6.viii
                B is    29 27 31 5 6 25 23 6 12
        Step 6.ix
                A is    4 35 12 30 31 35 21 5 23 27

Round #6
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 6, 1, 204, 49, 28, 139,
206, 231 ]
        Step 6.ii
                R is  [ 111, 210, 244, 114, 175, 68, 226, 88, 28, 15,
237, 141, 213, 149, 8, 140 ]
        Step 6.iii
                S is 6fd2f472af44e2581c0fed8d
        Step 6.iv
                y is  34607864885268487474569538957
        Step 6.v
                m is 9
        Step 6.vi
                c is  3710307925511
        Step 6.vii
                C is    1 11 12 17 25 19 17 29 35
        Step 6.viii
                B is    4 35 12 30 31 35 21 5 23 27
        Step 6.ix
                A is    1 11 12 17 25 19 17 29 35

Round #5
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 0, 3, 95, 223, 149, 254,
7 ]
        Step 6.ii
                R is  [ 20, 139, 225, 142, 115, 92, 228, 59, 37, 141,
157, 233, 13, 24, 120, 20 ]
        Step 6.iii
                S is 148be18e735ce43b258d9de9
        Step 6.iv
                y is  6358806045562408921612525033
        Step 6.v
                m is 10
        Step 6.vi
                c is  2463858254819582
        Step 6.vii
                C is    24 9 13 4 30 29 35 16 1 26
        Step 6.viii
                B is    1 11 12 17 25 19 17 29 35
        Step 6.ix
                A is    24 9 13 4 30 29 35 16 1 26

Round #4
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 8, 192, 221, 180, 14,
48, 254 ]
        Step 6.ii
                R is  [ 50, 228, 242, 3, 81, 153, 230, 28, 225, 33,
253, 16, 5, 235, 47, 133 ]
        Step 6.iii
                S is 32e4f2035199e61ce121fd10
        Step 6.iv
                y is  15751028451848459363561897232
        Step 6.v
                m is 9
        Step 6.vi
                c is  30411825086711
        Step 6.vii
                C is    10 28 2 35 35 16 2 27 11
        Step 6.viii
                B is    24 9 13 4 30 29 35 16 1 26
        Step 6.ix
                A is    10 28 2 35 35 16 2 27 11

Round #3
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 27, 168, 206, 8, 0,
247 ]
        Step 6.ii
                R is  [ 210, 168, 189, 131, 204, 156, 173, 50, 164,
116, 195, 152, 23, 34, 66, 112 ]
```

```
        Step 6.iii
                S is d2a8bd83cc9cad32a474c398
        Step 6.iv
                y is  65195846558710307865574556568
        Step 6.v
                m is 10
        Step 6.vi
                c is  887248406539622
        Step 6.vii
                C is    8 26 18 4 10 17 6 15 21 2
        Step 6.viii
                B is    10 28 2 35 35 16 2 27 11
        Step 6.ix
                A is    8 26 18 4 10 17 6 15 21 2

Round #2
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 3, 38, 242, 158, 25,
109, 102 ]
        Step 6.ii
                R is  [ 160, 235, 56, 15, 222, 178, 107, 202, 91, 205,
232, 58, 168, 245, 133, 82 ]
        Step 6.iii
                S is a0eb380fdeb26bca5bcde83a
        Step 6.iv
                y is  49801963884295857596938446906
        Step 6.v
                m is 9
        Step 6.vi
                c is  74443406317757
        Step 6.vii
                C is    26 13 34 29 30 1 28 19 17
        Step 6.viii
                B is    8 26 18 4 10 17 6 15 21 2
        Step 6.ix
                A is    26 13 34 29 30 1 28 19 17

Round #1
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 67, 180, 180, 202,
24, 189 ]
        Step 6.ii
                R is  [ 11, 66, 76, 139, 82, 150, 184, 220, 184, 125,
202, 48, 68, 104, 44, 131 ]
        Step 6.iii
                S is 0b424c8b5296b8dcb87dca30
        Step 6.iv
                y is  3484485682030632835911371312
        Step 6.v
                m is 10
        Step 6.vi
                c is  943139646579510
        Step 6.vii
                C is    9 10 11 12 13 14 15 16 17 18
        Step 6.viii
                B is    26 13 34 29 30 1 28 19 17
        Step 6.ix
                A is    9 10 11 12 13 14 15 16 17 18

Round #0
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 89, 199, 207, 155,
163, 54 ]
        Step 6.ii
                R is  [ 225, 238, 247, 123, 137, 230, 22, 54, 5, 163,
154, 25, 218, 40, 23, 48 ]
        Step 6.iii
                S is e1eef77b89e6163605a39a19
        Step 6.iv
                y is  69923020258278366124416670233
        Step 6.v
                m is 9
        Step 6.vi
                c is  82906087076
        Step 6.vii
                C is    0 1 2 3 4 5 6 7 8
        Step 6.viii
                B is    9 10 11 12 13 14 15 16 17 18
        Step 6.ix
                A is    0 1 2 3 4 5 6 7 8
Step 7
        A || B is    0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18

PT is <0123456789abcdefghi>

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

Sample #7

FF1-AES256

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

```
PT is <0123456789>

FF1.Encrypt()

X is    0 1 2 3 4 5 6 7 8 9
Tweak is <empty>

Step 1
        u is 5, v is 5
Step 2
        A is    0 1 2 3 4
        B is    5 6 7 8 9
Step 3
        b is 3
Step 4
        d is 8
Step 5
        P is  [ 1, 2, 1, 0, 0, 10, 10, 5, 0, 0, 0, 10, 0, 0, 0, 0 ]

Round #0
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 221,
213 ]
        Step 6.ii
                R is  [ 210, 74, 41, 163, 76, 134, 233, 117, 238, 73,
133, 25, 212, 244, 76, 173 ]
        Step 6.iii
                S is d24a29a34c86e975
        Step 6.iv
                y is  15152969677581773173
        Step 6.v
                m is 5
        Step 6.vi
                c is  74407
        Step 6.vii
                C is    7 4 4 0 7
        Step 6.viii
                A is    5 6 7 8 9
        Step 6.ix
                B is    7 4 4 0 7

Round #1
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 34,
167 ]
        Step 6.ii
                R is  [ 83, 27, 87, 30, 53, 175, 207, 62, 162, 72,
103, 14, 28, 135, 227, 179 ]
        Step 6.iii
                S is 531b571e35afcf3e
        Step 6.iv
                y is  5988475916780556094
        Step 6.v
                m is 5
        Step 6.vi
                c is  12883
        Step 6.vii
                C is    1 2 8 8 3
        Step 6.viii
                A is    7 4 4 0 7
        Step 6.ix
                B is    1 2 8 8 3

Round #2
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 50,
83 ]
        Step 6.ii
                R is  [ 94, 85, 158, 65, 193, 9, 34, 42, 197, 94, 194,
4, 0, 16, 196, 55 ]
        Step 6.iii
                S is 5e559e41c109222a
        Step 6.iv
                y is  6797513217834295850
        Step 6.v
                m is 5
        Step 6.vi
                c is  70257
        Step 6.vii
                C is    7 0 2 5 7
        Step 6.viii
                A is    1 2 8 8 3
        Step 6.ix
                B is    7 0 2 5 7

Round #3
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 1, 18,
113 ]
        Step 6.ii
                R is  [ 202, 144, 213, 104, 61, 32, 230, 39, 195, 155,
31, 102, 159, 32, 37, 132 ]
        Step 6.iii
                S is ca90d5683d20e627
        Step 6.iv
                y is  14596401035986658855
        Step 6.v
                m is 5
        Step 6.vi
                c is  71738
        Step 6.vii
                C is    7 1 7 3 8
        Step 6.viii
                A is    7 0 2 5 7
        Step 6.ix
                B is    7 1 7 3 8

Round #4
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 1, 24,
58 ]
        Step 6.ii
                R is  [ 58, 44, 107, 123, 115, 117, 7, 192, 52, 250,
62, 7, 161, 97, 215, 251 ]
        Step 6.iii
                S is 3a2c6b7b737507c0
        Step 6.iv
                y is  4191843531137288128
        Step 6.v
                m is 5
        Step 6.vi
                c is  58385
        Step 6.vii
                C is    5 8 3 8 5
        Step 6.viii
                A is    7 1 7 3 8
        Step 6.ix
                B is    5 8 3 8 5

Round #5
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 0, 228,
17 ]
        Step 6.ii
                R is  [ 228, 72, 223, 130, 164, 159, 254, 9, 73, 87,
102, 223, 158, 45, 239, 163 ]
        Step 6.iii
                S is e448df82a49ffe09
        Step 6.iv
                y is  16449643391171427849
        Step 6.v
                m is 5
        Step 6.vi
                c is  99587
        Step 6.vii
                C is    9 9 5 8 7
        Step 6.viii
                A is    5 8 3 8 5
        Step 6.ix
                B is    9 9 5 8 7
```

```
Round #6
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 6, 1, 133,
3 ]
        Step 6.ii
                R is  [ 20, 211, 216, 181, 50, 177, 180, 97, 81, 210,
8, 6, 114, 219, 134, 203 ]
        Step 6.iii
                S is 14d3d8b532b1b461
        Step 6.iv
                y is  1500781373595694177
        Step 6.v
                m is 5
        Step 6.vi
                c is  52562
        Step 6.vii
                C is    5 2 5 6 2
        Step 6.viii
                A is    9 9 5 8 7
        Step 6.ix
                B is    5 2 5 6 2

Round #7
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 7, 0, 205,
82 ]
        Step 6.ii
                R is  [ 41, 15, 253, 95, 123, 44, 77, 52, 201, 168,
91, 246, 141, 144, 221, 82 ]
        Step 6.iii
                S is 290ffd5f7b2c4d34
        Step 6.iv
                y is  2958862066735926580
        Step 6.v
                m is 5
        Step 6.vi
                c is  26167
        Step 6.vii
                C is    2 6 1 6 7
        Step 6.viii
                A is    5 2 5 6 2
        Step 6.ix
                B is    2 6 1 6 7

Round #8
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8, 0, 102,
55 ]
        Step 6.ii
```

```
                R is  [ 167, 151, 192, 233, 24, 181, 44, 222, 211, 13,
120, 98, 178, 250, 41, 247 ]
        Step 6.iii
                S is a797c0e918b52cde
        Step 6.iv
                y is  12076333033191714014
        Step 6.v
                m is 5
        Step 6.vi
                c is  66576
        Step 6.vii
                C is    6 6 5 7 6
        Step 6.viii
                A is    2 6 1 6 7
        Step 6.ix
                B is    6 6 5 7 6

Round #9
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 9, 1, 4,
16 ]
        Step 6.ii
                R is  [ 235, 113, 164, 87, 117, 110, 72, 74, 226, 69,
197, 156, 99, 83, 123, 144 ]
        Step 6.iii
                S is eb71a457756e484a
        Step 6.iv
                y is  16965521966820640842
        Step 6.v
                m is 5
        Step 6.vi
                c is  67009
        Step 6.vii
                C is    6 7 0 0 9
        Step 6.viii
                A is    6 6 5 7 6
        Step 6.ix
                B is    6 7 0 0 9

Step 7
        A || B is    6 6 5 7 6 6 7 0 0 9

CT is <6657667009>

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

FF1.Decrypt()

X is    6 6 5 7 6 6 7 0 0 9
Tweak is <empty>
```

```
Step 1
        u is 5, v is 5
Step 2
        A is    6 6 5 7 6
        B is    6 7 0 0 9
Step 3
        b is 3
Step 4
        d is 8
Step 5
        P is  [ 1, 2, 1, 0, 0, 10, 10, 5, 0, 0, 0, 10, 0, 0, 0, 0 ]

Round #9
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 9, 1, 4, 
16 ]
        Step 6.ii
                R is  [ 235, 113, 164, 87, 117, 110, 72, 74, 226, 69, 
197, 156, 99, 83, 123, 144 ]
        Step 6.iii
                S is eb71a457756e484a
        Step 6.iv
                y is  16965521966820640842
        Step 6.v
                m is 5
        Step 6.vi
                c is  26167
        Step 6.vii
                C is    2 6 1 6 7
        Step 6.viii
                B is    6 6 5 7 6
        Step 6.ix
                A is    2 6 1 6 7

Round #8
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8, 0, 102, 
55 ]
        Step 6.ii
                R is  [ 167, 151, 192, 233, 24, 181, 44, 222, 211, 13, 
120, 98, 178, 250, 41, 247 ]
        Step 6.iii
                S is a797c0e918b52cde
        Step 6.iv
                y is  12076333033191714014
        Step 6.v
                m is 5
        Step 6.vi
                c is  52562
        Step 6.vii
                C is    5 2 5 6 2
        Step 6.viii
                B is    2 6 1 6 7
        Step 6.ix
                A is    5 2 5 6 2

Round #7
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 7, 0, 205,
82 ]
        Step 6.ii
                R is  [ 41, 15, 253, 95, 123, 44, 77, 52, 201, 168,
91, 246, 141, 144, 221, 82 ]
        Step 6.iii
                S is 290ffd5f7b2c4d34
        Step 6.iv
                y is  2958862066735926580
        Step 6.v
                m is 5
        Step 6.vi
                c is  99587
        Step 6.vii
                C is    9 9 5 8 7
        Step 6.viii
                B is    5 2 5 6 2
        Step 6.ix
                A is    9 9 5 8 7

Round #6
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 6, 1, 133,
3 ]
        Step 6.ii
                R is  [ 20, 211, 216, 181, 50, 177, 180, 97, 81, 210,
8, 6, 114, 219, 134, 203 ]
        Step 6.iii
                S is 14d3d8b532b1b461
        Step 6.iv
                y is  1500781373595694177
        Step 6.v
                m is 5
        Step 6.vi
                c is  58385
        Step 6.vii
                C is    5 8 3 8 5
        Step 6.viii
                B is    9 9 5 8 7
        Step 6.ix
                A is    5 8 3 8 5
```

```
Round #5
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 0, 228,
17 ]
        Step 6.ii
                R is  [ 228, 72, 223, 130, 164, 159, 254, 9, 73, 87,
102, 223, 158, 45, 239, 163 ]
        Step 6.iii
                S is e448df82a49ffe09
        Step 6.iv
                y is  16449643391171427849
        Step 6.v
                m is 5
        Step 6.vi
                c is  71738
        Step 6.vii
                C is    7 1 7 3 8
        Step 6.viii
                B is    5 8 3 8 5
        Step 6.ix
                A is    7 1 7 3 8

Round #4
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 1, 24,
58 ]
        Step 6.ii
                R is  [ 58, 44, 107, 123, 115, 117, 7, 192, 52, 250,
62, 7, 161, 97, 215, 251 ]
        Step 6.iii
                S is 3a2c6b7b737507c0
        Step 6.iv
                y is  4191843531137288128
        Step 6.v
                m is 5
        Step 6.vi
                c is  70257
        Step 6.vii
                C is    7 0 2 5 7
        Step 6.viii
                B is    7 1 7 3 8
        Step 6.ix
                A is    7 0 2 5 7

Round #3
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 1, 18,
113 ]
        Step 6.ii
```

```
                R is  [ 202, 144, 213, 104, 61, 32, 230, 39, 195, 155,
31, 102, 159, 32, 37, 132 ]
        Step 6.iii
                S is ca90d5683d20e627
        Step 6.iv
                y is  14596401035986658855
        Step 6.v
                m is 5
        Step 6.vi
                c is  12883
        Step 6.vii
                C is    1 2 8 8 3
        Step 6.viii
                B is    7 0 2 5 7
        Step 6.ix
                A is    1 2 8 8 3

Round #2
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 50,
83 ]
        Step 6.ii
                R is  [ 94, 85, 158, 65, 193, 9, 34, 42, 197, 94, 194,
4, 0, 16, 196, 55 ]
        Step 6.iii
                S is 5e559e41c109222a
        Step 6.iv
                y is  6797513217834295850
        Step 6.v
                m is 5
        Step 6.vi
                c is  74407
        Step 6.vii
                C is    7 4 4 0 7
        Step 6.viii
                B is    1 2 8 8 3
        Step 6.ix
                A is    7 4 4 0 7

Round #1
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 34,
167 ]
        Step 6.ii
                R is  [ 83, 27, 87, 30, 53, 175, 207, 62, 162, 72,
103, 14, 28, 135, 227, 179 ]
        Step 6.iii
                S is 531b571e35afcf3e
        Step 6.iv
                y is  5988475916780556094
        Step 6.v
                m is 5
        Step 6.vi
                c is  56789
        Step 6.vii
                C is    5 6 7 8 9
        Step 6.viii
                B is    7 4 4 0 7
        Step 6.ix
                A is    5 6 7 8 9

Round #0
        Step 6.i
                Q is  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 221,
213 ]
        Step 6.ii
                R is  [ 210, 74, 41, 163, 76, 134, 233, 117, 238, 73,
133, 25, 212, 244, 76, 173 ]
        Step 6.iii
                S is d24a29a34c86e975
        Step 6.iv
                y is  15152969677581773173
        Step 6.v
                m is 5
        Step 6.vi
                c is  1234
        Step 6.vii
                C is    0 1 2 3 4
        Step 6.viii
                B is    5 6 7 8 9
        Step 6.ix
                A is    0 1 2 3 4
Step 7
        A || B is    0 1 2 3 4 5 6 7 8 9

PT is <0123456789>

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

Sample #8

FF1-AES256

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


PT is <0123456789>
```

```
FF1.Encrypt()

X is    0 1 2 3 4 5 6 7 8 9
Tweak is 39 38 37 36 35 34 33 32 31 30

Step 1
        u is 5, v is 5
Step 2
        A is    0 1 2 3 4
        B is    5 6 7 8 9
Step 3
        b is 3
Step 4
        d is 8
Step 5
        P is  [ 1, 2, 1, 0, 0, 10, 10, 5, 0, 0, 0, 10, 0, 0, 0, 10 ]

Round #0
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
0, 0, 221, 213 ]
        Step 6.ii
                R is  [ 126, 234, 51, 33, 47, 42, 219, 26, 19, 214,
205, 182, 160, 27, 106, 86 ]
        Step 6.iii
                S is 7eea33212f2adb1a
        Step 6.iv
                y is  9145178210947488538
        Step 6.v
                m is 5
        Step 6.vi
                c is  89772
        Step 6.vii
                C is    8 9 7 7 2
        Step 6.viii
                A is    5 6 7 8 9
        Step 6.ix
                B is    8 9 7 7 2

Round #1
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
1, 1, 94, 172 ]
        Step 6.ii
                R is  [ 164, 155, 179, 154, 229, 79, 208, 126, 26,
177, 78, 139, 201, 179, 158, 93 ]
        Step 6.iii
                S is a49bb39ae54fd07e
        Step 6.iv
```

```
                y is  11861271521463881854
        Step 6.v
                m is 5
        Step 6.vi
                c is  38643
        Step 6.vii
                C is    3 8 6 4 3
        Step 6.viii
                A is    8 9 7 7 2
        Step 6.ix
                B is    3 8 6 4 3

Round #2
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
2, 0, 150, 243 ]
        Step 6.ii
                R is  [ 235, 228, 166, 105, 67, 137, 24, 136, 165, 13,
199, 217, 80, 211, 216, 144 ]
        Step 6.iii
                S is ebe4a66943891888
        Step 6.iv
                y is  16997893864637929608
        Step 6.v
                m is 5
        Step 6.vi
                c is  19380
        Step 6.vii
                C is    1 9 3 8 0
        Step 6.viii
                A is    3 8 6 4 3
        Step 6.ix
                B is    1 9 3 8 0

Round #3
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
3, 0, 75, 180 ]
        Step 6.ii
                R is  [ 11, 61, 98, 240, 134, 36, 235, 73, 69, 116,
15, 177, 138, 142, 4, 242 ]
        Step 6.iii
                S is 0b3d62f08624eb49
        Step 6.iv
                y is  809912293178796873
        Step 6.v
                m is 5
        Step 6.vi
                c is  35516
        Step 6.vii
```

```
                C is    3 5 5 1 6
        Step 6.viii
                A is    1 9 3 8 0
        Step 6.ix
                B is    3 5 5 1 6

Round #4
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
4, 0, 138, 188 ]
        Step 6.ii
                R is  [ 167, 216, 127, 81, 156, 24, 17, 40, 11, 1,
174, 223, 77, 106, 215, 247 ]
        Step 6.iii
                S is a7d87f519c181128
        Step 6.iv
                y is  12094556787791368488
        Step 6.v
                m is 5
        Step 6.vi
                c is  87868
        Step 6.vii
                C is    8 7 8 6 8
        Step 6.viii
                A is    3 5 5 1 6
        Step 6.ix
                B is    8 7 8 6 8

Round #5
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
5, 1, 87, 60 ]
        Step 6.ii
                R is  [ 14, 107, 87, 214, 161, 55, 104, 140, 102, 245,
251, 238, 54, 150, 217, 179 ]
        Step 6.iii
                S is 0e6b57d6a137688c
        Step 6.iv
                y is  1039020718378412172
        Step 6.v
                m is 5
        Step 6.vi
                c is  47688
        Step 6.vii
                C is    4 7 6 8 8
        Step 6.viii
                A is    8 7 8 6 8
        Step 6.ix
                B is    4 7 6 8 8
```

```
Round #6
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
6, 0, 186, 72 ]
        Step 6.ii
                R is  [ 243, 12, 189, 213, 35, 125, 119, 132, 173, 68,
57, 199, 132, 44, 155, 97 ]
        Step 6.iii
                S is f30cbdd5237d7784
        Step 6.iv
                y is  17513581774058125188
        Step 6.v
                m is 5
        Step 6.vi
                c is  13056
        Step 6.vii
                C is    1 3 0 5 6
        Step 6.viii
                A is    4 7 6 8 8
        Step 6.ix
                B is    1 3 0 5 6

Round #7
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
7, 0, 51, 0 ]
        Step 6.ii
                R is  [ 152, 182, 125, 28, 14, 219, 138, 101, 2, 74,
253, 211, 157, 110, 202, 125 ]
        Step 6.iii
                S is 98b67d1c0edb8a65
        Step 6.iv
                y is  11004120298988210789
        Step 6.v
                m is 5
        Step 6.vi
                c is  58477
        Step 6.vii
                C is    5 8 4 7 7
        Step 6.viii
                A is    1 3 0 5 6
        Step 6.ix
                B is    5 8 4 7 7

Round #8
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
8, 0, 228, 109 ]
        Step 6.ii
                R is  [ 62, 4, 136, 216, 137, 238, 127, 160, 202, 40,
187, 115, 78, 79, 232, 206 ]
        Step 6.iii
                S is 3e0488d889ee7fa0
        Step 6.iv
                y is  4468847193866796960
        Step 6.v
                m is 5
        Step 6.vi
                c is  10016
        Step 6.vii
                C is    1 0 0 1 6
        Step 6.viii
                A is    5 8 4 7 7
        Step 6.ix
                B is    1 0 0 1 6

Round #9
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
9, 0, 39, 32 ]
        Step 6.ii
                R is  [ 74, 156, 68, 166, 81, 159, 2, 250, 106, 246,
248, 24, 235, 215, 117, 189 ]
        Step 6.iii
                S is 4a9c44a6519f02fa
        Step 6.iv
                y is  5376247536298164986
        Step 6.v
                m is 5
        Step 6.vi
                c is  23463
        Step 6.vii
                C is    2 3 4 6 3
        Step 6.viii
                A is    1 0 0 1 6
        Step 6.ix
                B is    2 3 4 6 3

Step 7
        A || B is    1 0 0 1 6 2 3 4 6 3

CT is <1001623463>

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

FF1.Decrypt()

X is    1 0 0 1 6 2 3 4 6 3
Tweak is 39 38 37 36 35 34 33 32 31 30
```

```
Step 1
        u is 5, v is 5
Step 2
        A is    1 0 0 1 6
        B is    2 3 4 6 3
Step 3
        b is 3
Step 4
        d is 8
Step 5
        P is  [ 1, 2, 1, 0, 0, 10, 10, 5, 0, 0, 0, 10, 0, 0, 0, 10 ]

Round #9
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
9, 0, 39, 32 ]
        Step 6.ii
                R is  [ 74, 156, 68, 166, 81, 159, 2, 250, 106, 246,
248, 24, 235, 215, 117, 189 ]
        Step 6.iii
                S is 4a9c44a6519f02fa
        Step 6.iv
                y is  5376247536298164986
        Step 6.v
                m is 5
        Step 6.vi
                c is  58477
        Step 6.vii
                C is    5 8 4 7 7
        Step 6.viii
                B is    1 0 0 1 6
        Step 6.ix
                A is    5 8 4 7 7

Round #8
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
8, 0, 228, 109 ]
        Step 6.ii
                R is  [ 62, 4, 136, 216, 137, 238, 127, 160, 202, 40,
187, 115, 78, 79, 232, 206 ]
        Step 6.iii
                S is 3e0488d889ee7fa0
        Step 6.iv
                y is  4468847193866796960
        Step 6.v
                m is 5
        Step 6.vi
                c is  13056
        Step 6.vii
```

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

Round #7
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
7, 0, 51, 0 ]
        Step 6.ii
                R is  [ 152, 182, 125, 28, 14, 219, 138, 101, 2, 74,
253, 211, 157, 110, 202, 125 ]
        Step 6.iii
                S is 98b67d1c0edb8a65
        Step 6.iv
                y is  11004120298988210789
        Step 6.v
                m is 5
        Step 6.vi
                c is  47688
        Step 6.vii
                C is    4 7 6 8 8
        Step 6.viii
                B is    1 3 0 5 6
        Step 6.ix
                A is    4 7 6 8 8

Round #6
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
6, 0, 186, 72 ]
        Step 6.ii
                R is  [ 243, 12, 189, 213, 35, 125, 119, 132, 173, 68,
57, 199, 132, 44, 155, 97 ]
        Step 6.iii
                S is f30cbdd5237d7784
        Step 6.iv
                y is  17513581774058125188
        Step 6.v
                m is 5
        Step 6.vi
                c is  87868
        Step 6.vii
                C is    8 7 8 6 8
        Step 6.viii
                B is    4 7 6 8 8
        Step 6.ix
                A is    8 7 8 6 8
```

```
Round #5
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
5, 1, 87, 60 ]
        Step 6.ii
                R is  [ 14, 107, 87, 214, 161, 55, 104, 140, 102, 245,
251, 238, 54, 150, 217, 179 ]
        Step 6.iii
                S is 0e6b57d6a137688c
        Step 6.iv
                y is  1039020718378412172
        Step 6.v
                m is 5
        Step 6.vi
                c is  35516
        Step 6.vii
                C is    3 5 5 1 6
        Step 6.viii
                B is    8 7 8 6 8
        Step 6.ix
                A is    3 5 5 1 6

Round #4
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
4, 0, 138, 188 ]
        Step 6.ii
                R is  [ 167, 216, 127, 81, 156, 24, 17, 40, 11, 1,
174, 223, 77, 106, 215, 247 ]
        Step 6.iii
                S is a7d87f519c181128
        Step 6.iv
                y is  12094556787791368488
        Step 6.v
                m is 5
        Step 6.vi
                c is  19380
        Step 6.vii
                C is    1 9 3 8 0
        Step 6.viii
                B is    3 5 5 1 6
        Step 6.ix
                A is    1 9 3 8 0

Round #3
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
3, 0, 75, 180 ]
        Step 6.ii
                R is  [ 11, 61, 98, 240, 134, 36, 235, 73, 69, 116,
15, 177, 138, 142, 4, 242 ]
        Step 6.iii
                S is 0b3d62f08624eb49
        Step 6.iv
                y is  809912293178796873
        Step 6.v
                m is 5
        Step 6.vi
                c is  38643
        Step 6.vii
                C is    3 8 6 4 3
        Step 6.viii
                B is    1 9 3 8 0
        Step 6.ix
                A is    3 8 6 4 3

Round #2
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
2, 0, 150, 243 ]
        Step 6.ii
                R is  [ 235, 228, 166, 105, 67, 137, 24, 136, 165, 13,
199, 217, 80, 211, 216, 144 ]
        Step 6.iii
                S is ebe4a66943891888
        Step 6.iv
                y is  16997893864637929608
        Step 6.v
                m is 5
        Step 6.vi
                c is  89772
        Step 6.vii
                C is    8 9 7 7 2
        Step 6.viii
                B is    3 8 6 4 3
        Step 6.ix
                A is    8 9 7 7 2

Round #1
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
1, 1, 94, 172 ]
        Step 6.ii
                R is  [ 164, 155, 179, 154, 229, 79, 208, 126, 26,
177, 78, 139, 201, 179, 158, 93 ]
        Step 6.iii
                S is a49bb39ae54fd07e
        Step 6.iv
                y is  11861271521463881854
        Step 6.v
```

```
                m is 5
        Step 6.vi
                c is  56789
        Step 6.vii
                C is    5 6 7 8 9
        Step 6.viii
                B is    8 9 7 7 2
        Step 6.ix
                A is    5 6 7 8 9

Round #0
        Step 6.i
                Q is  [ 57, 56, 55, 54, 53, 52, 51, 50, 49, 48, 0, 0,
0, 0, 221, 213 ]
        Step 6.ii
                R is  [ 126, 234, 51, 33, 47, 42, 219, 26, 19, 214,
205, 182, 160, 27, 106, 86 ]
        Step 6.iii
                S is 7eea33212f2adb1a
        Step 6.iv
                y is  9145178210947488538
        Step 6.v
                m is 5
        Step 6.vi
                c is  1234
        Step 6.vii
                C is    0 1 2 3 4
        Step 6.viii
                B is    5 6 7 8 9
        Step 6.ix
                A is    0 1 2 3 4
Step 7
        A || B is    0 1 2 3 4 5 6 7 8 9

PT is <0123456789>

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

Sample #9

FF1-AES256

Key is 2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C EF 43 59 D8 D5
80 AA 4F 7F 03 6D 6F 04 FC 6A 94
Radix = 36
--------------------------------------------------------------


PT is <0123456789abcdefghi>
```

```
FF1.Encrypt()

X is    0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
Tweak is 37 37 37 37 70 71 72 73 37 37 37

Step 1
        u is 9, v is 10
Step 2
        A is    0 1 2 3 4 5 6 7 8
        B is    9 10 11 12 13 14 15 16 17 18
Step 3
        b is 7
Step 4
        d is 12
Step 5
        P is  [ 1, 2, 1, 0, 0, 36, 10, 9, 0, 0, 0, 19, 0, 0, 0, 11 ]

Round #0
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 89, 199, 207, 155,
163, 54 ]
        Step 6.ii
                R is  [ 169, 244, 14, 81, 94, 34, 73, 25, 163, 180,
21, 69, 163, 95, 31, 120 ]
        Step 6.iii
                S is a9f40e515e224919a3b41545
        Step 6.iv
                y is  52598012173893380641865864517
        Step 6.v
                m is 9
        Step 6.vi
                c is  55071529931753
        Step 6.vii
                C is    19 18 27 18 15 0 21 18 17
        Step 6.viii
                A is    9 10 11 12 13 14 15 16 17 18
        Step 6.ix
                B is    19 18 27 18 15 0 21 18 17

Round #1
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 50, 22, 86, 250, 147,
233 ]
        Step 6.ii
                R is  [ 195, 167, 66, 120, 89, 50, 41, 161, 103, 88,
190, 184, 105, 93, 57, 22 ]
        Step 6.iii
                S is c3a74278593229a16758beb8
        Step 6.iv
                y is  60551781423262335106649996984
        Step 6.v
                m is 10
        Step 6.vi
                c is  3375932902760942
        Step 6.vii
                C is    33 8 24 2 5 34 10 27 33 26
        Step 6.viii
                A is    19 18 27 18 15 0 21 18 17
        Step 6.ix
                B is    33 8 24 2 5 34 10 27 33 26

Round #2
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 11, 254, 100, 161, 116,
97, 238 ]
        Step 6.ii
                R is  [ 48, 13, 232, 79, 41, 98, 175, 116, 205, 255,
62, 178, 248, 112, 69, 178 ]
        Step 6.iii
                S is 300de84f2962af74cdff3eb2
        Step 6.iv
                y is  14872093556378499878284639922
        Step 6.v
                m is 9
        Step 6.vi
                c is  58407579144859
        Step 6.vii
                C is    20 25 12 2 20 21 0 23 31
        Step 6.viii
                A is    33 8 24 2 5 34 10 27 33 26
        Step 6.ix
                B is    20 25 12 2 20 21 0 23 31

Round #3
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 53, 31, 19, 1, 210,
155 ]
        Step 6.ii
                R is  [ 158, 135, 120, 203, 201, 76, 7, 15, 27, 148,
156, 158, 184, 96, 43, 71 ]
        Step 6.iii
                S is 9e8778cbc94c070f1b949c9e
        Step 6.iv
                y is  49062406980592463378887515294
        Step 6.v
                m is 10
        Step 6.vi
                c is  602181337677452
        Step 6.vii
                C is    5 33 16 14 10 12 21 10 33 8
        Step 6.viii
                A is    20 25 12 2 20 21 0 23 31
        Step 6.ix
                B is    5 33 16 14 10 12 21 10 33 8

Round #4
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 2, 35, 174, 68, 184,
254, 140 ]
        Step 6.ii
                R is  [ 119, 110, 245, 135, 78, 173, 10, 92, 170, 119,
156, 117, 165, 116, 58, 168 ]
        Step 6.iii
                S is 776ef5874ead0a5caa779c75
        Step 6.iv
                y is  36962857484665624300376005749
        Step 6.v
                m is 9
        Step 6.vi
                c is  47863841517328
        Step 6.vii
                C is    16 34 28 12 15 15 19 15 4
        Step 6.viii
                A is    5 33 16 14 10 12 21 10 33 8
        Step 6.ix
                B is    16 34 28 12 15 15 19 15 4

Round #5
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 0, 43, 136, 43, 69, 111,
16 ]
        Step 6.ii
                R is  [ 232, 42, 137, 218, 210, 229, 119, 96, 201, 74,
253, 239, 210, 8, 93, 229 ]
        Step 6.iii
                S is e82a89dad2e57760c94afdef
        Step 6.iv
                y is  71851948163770915354772700655
        Step 6.v
                m is 10
        Step 6.vi
                c is  2416627861945467
        Step 6.vii
                C is    23 28 22 15 18 17 18 25 31 15
        Step 6.viii
                A is    16 34 28 12 15 15 19 15 4
        Step 6.ix
                B is    23 28 22 15 18 17 18 25 31 15

Round #6
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 6, 8, 149, 233, 5, 67, 252,
123 ]
        Step 6.ii
                R is  [ 115, 112, 72, 205, 83, 97, 8, 64, 246, 109,
170, 55, 131, 138, 139, 107 ]
        Step 6.iii
                S is 737048cd53610840f66daa37
        Step 6.iv
                y is  35726519619228915548824644151
        Step 6.v
                m is 9
        Step 6.vi
                c is  48491323136327
        Step 6.vii
                C is    17 6 28 21 29 28 11 11 11
        Step 6.viii
                A is    23 28 22 15 18 17 18 25 31 15
        Step 6.ix
                B is    17 6 28 21 29 28 11 11 11

Round #7
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 7, 0, 44, 26, 68, 23, 25,
71 ]
        Step 6.ii
                R is  [ 153, 197, 59, 250, 40, 212, 157, 122, 243, 99,
153, 189, 22, 101, 104, 46 ]
        Step 6.iii
                S is 99c53bfa28d49d7af36399bd
        Step 6.iv
                y is  47589648123380534806738868669
        Step 6.v
                m is 10
        Step 6.vi
                c is  3532592868988472
        Step 6.vii
                C is    34 28 7 6 27 13 12 22 20 8
        Step 6.viii
                A is    17 6 28 21 29 28 11 11 11
        Step 6.ix
                B is    34 28 7 6 27 13 12 22 20 8
```

```
Round #8
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8, 12, 140, 223, 223, 23,
150, 56 ]
        Step 6.ii
                R is  [ 219, 115, 118, 188, 190, 243, 246, 208, 39,
191, 160, 207, 71, 15, 7, 214 ]
        Step 6.iii
                S is db7376bcbef3f6d027bfa0cf
        Step 6.iv
                y is  67916804341122729541776679119
        Step 6.v
                m is 9
        Step 6.vi
                c is  95308842973718
        Step 6.vii
                C is    33 28 8 10 0 10 35 17 2
        Step 6.viii
                A is    34 28 7 6 27 13 12 22 20 8
        Step 6.ix
                B is    33 28 8 10 0 10 35 17 2

Round #9
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 9, 0, 86, 174, 209, 186,
186, 22 ]
        Step 6.ii
                R is  [ 128, 76, 111, 36, 235, 254, 134, 14, 103, 122,
230, 245, 220, 239, 132, 25 ]
        Step 6.iii
                S is 804c6f24ebfe860e677ae6f5
        Step 6.iv
                y is  39706484483190442437633566453
        Step 6.v
                m is 10
        Step 6.vi
                c is  1105741451787565
        Step 6.vii
                C is    10 31 34 10 21 34 35 30 32 13
        Step 6.viii
                A is    33 28 8 10 0 10 35 17 2
        Step 6.ix
                B is    10 31 34 10 21 34 35 30 32 13

Step 7
        A || B is    33 28 8 10 0 10 35 17 2 10 31 34 10 21 34 35 30
32 13
```

```
CT is <xs8a0azh2avyalyzuwd>

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

FF1.Decrypt()

X is    33 28 8 10 0 10 35 17 2 10 31 34 10 21 34 35 30 32 13
Tweak is 37 37 37 37 70 71 72 73 37 37 37

Step 1
        u is 9, v is 10
Step 2
        A is    33 28 8 10 0 10 35 17 2
        B is    10 31 34 10 21 34 35 30 32 13
Step 3
        b is 7
Step 4
        d is 12
Step 5
        P is  [ 1, 2, 1, 0, 0, 36, 10, 9, 0, 0, 0, 19, 0, 0, 0, 11 ]

Round #9
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 9, 0, 86, 174, 209, 186,
186, 22 ]
        Step 6.ii
                R is  [ 128, 76, 111, 36, 235, 254, 134, 14, 103, 122,
230, 245, 220, 239, 132, 25 ]
        Step 6.iii
                S is 804c6f24ebfe860e677ae6f5
        Step 6.iv
                y is  39706484483190442437633566453
        Step 6.v
                m is 10
        Step 6.vi
                c is  3532592868988472
        Step 6.vii
                C is    34 28 7 6 27 13 12 22 20 8
        Step 6.viii
                B is    33 28 8 10 0 10 35 17 2
        Step 6.ix
                A is    34 28 7 6 27 13 12 22 20 8

Round #8
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8, 12, 140, 223, 223, 23,
150, 56 ]
```

```
        Step 6.ii
                R is  [ 219, 115, 118, 188, 190, 243, 246, 208, 39,
191, 160, 207, 71, 15, 7, 214 ]
        Step 6.iii
                S is db7376bcbef3f6d027bfa0cf
        Step 6.iv
                y is  67916804341122729541776679119
        Step 6.v
                m is 9
        Step 6.vi
                c is  48491323136327
        Step 6.vii
                C is    17 6 28 21 29 28 11 11 11
        Step 6.viii
                B is    34 28 7 6 27 13 12 22 20 8
        Step 6.ix
                A is    17 6 28 21 29 28 11 11 11

Round #7
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 7, 0, 44, 26, 68, 23, 25,
71 ]
        Step 6.ii
                R is  [ 153, 197, 59, 250, 40, 212, 157, 122, 243, 99,
153, 189, 22, 101, 104, 46 ]
        Step 6.iii
                S is 99c53bfa28d49d7af36399bd
        Step 6.iv
                y is  47589648123380534806738868669
        Step 6.v
                m is 10
        Step 6.vi
                c is  2416627861945467
        Step 6.vii
                C is    23 28 22 15 18 17 18 25 31 15
        Step 6.viii
                B is    17 6 28 21 29 28 11 11 11
        Step 6.ix
                A is    23 28 22 15 18 17 18 25 31 15

Round #6
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 6, 8, 149, 233, 5, 67, 252,
123 ]
        Step 6.ii
                R is  [ 115, 112, 72, 205, 83, 97, 8, 64, 246, 109,
170, 55, 131, 138, 139, 107 ]
        Step 6.iii
```

```
                S is 737048cd53610840f66daa37
        Step 6.iv
                y is  35726519619228915548824644151
        Step 6.v
                m is 9
        Step 6.vi
                c is  47863841517328
        Step 6.vii
                C is    16 34 28 12 15 15 19 15 4
        Step 6.viii
                B is    23 28 22 15 18 17 18 25 31 15
        Step 6.ix
                A is    16 34 28 12 15 15 19 15 4

Round #5
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 0, 43, 136, 43, 69, 111,
16 ]
        Step 6.ii
                R is  [ 232, 42, 137, 218, 210, 229, 119, 96, 201, 74,
253, 239, 210, 8, 93, 229 ]
        Step 6.iii
                S is e82a89dad2e57760c94afdef
        Step 6.iv
                y is  71851948163770915354772700655
        Step 6.v
                m is 10
        Step 6.vi
                c is  602181337677452
        Step 6.vii
                C is    5 33 16 14 10 12 21 10 33 8
        Step 6.viii
                B is    16 34 28 12 15 15 19 15 4
        Step 6.ix
                A is    5 33 16 14 10 12 21 10 33 8

Round #4
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 2, 35, 174, 68, 184,
254, 140 ]
        Step 6.ii
                R is  [ 119, 110, 245, 135, 78, 173, 10, 92, 170, 119,
156, 117, 165, 116, 58, 168 ]
        Step 6.iii
                S is 776ef5874ead0a5caa779c75
        Step 6.iv
                y is  36962857484665624300376005749
        Step 6.v
```

```
                m is 9
        Step 6.vi
                c is  58407579144859
        Step 6.vii
                C is    20 25 12 2 20 21 0 23 31
        Step 6.viii
                B is    5 33 16 14 10 12 21 10 33 8
        Step 6.ix
                A is    20 25 12 2 20 21 0 23 31

Round #3
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 53, 31, 19, 1, 210,
155 ]
        Step 6.ii
                R is  [ 158, 135, 120, 203, 201, 76, 7, 15, 27, 148,
156, 158, 184, 96, 43, 71 ]
        Step 6.iii
                S is 9e8778cbc94c070f1b949c9e
        Step 6.iv
                y is  49062406980592463378887515294
        Step 6.v
                m is 10
        Step 6.vi
                c is  3375932902760942
        Step 6.vii
                C is    33 8 24 2 5 34 10 27 33 26
        Step 6.viii
                B is    20 25 12 2 20 21 0 23 31
        Step 6.ix
                A is    33 8 24 2 5 34 10 27 33 26

Round #2
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 11, 254, 100, 161, 116,
97, 238 ]
        Step 6.ii
                R is  [ 48, 13, 232, 79, 41, 98, 175, 116, 205, 255,
62, 178, 248, 112, 69, 178 ]
        Step 6.iii
                S is 300de84f2962af74cdff3eb2
        Step 6.iv
                y is  14872093556378499878284639922
        Step 6.v
                m is 9
        Step 6.vi
                c is  55071529931753
        Step 6.vii
```

```
                C is    19 18 27 18 15 0 21 18 17
        Step 6.viii
                B is    33 8 24 2 5 34 10 27 33 26
        Step 6.ix
                A is    19 18 27 18 15 0 21 18 17

Round #1
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 50, 22, 86, 250, 147,
233 ]
        Step 6.ii
                R is  [ 195, 167, 66, 120, 89, 50, 41, 161, 103, 88,
190, 184, 105, 93, 57, 22 ]
        Step 6.iii
                S is c3a74278593229a16758beb8
        Step 6.iv
                y is  60551781423262335106649996984
        Step 6.v
                m is 10
        Step 6.vi
                c is  943139646579510
        Step 6.vii
                C is    9 10 11 12 13 14 15 16 17 18
        Step 6.viii
                B is    19 18 27 18 15 0 21 18 17
        Step 6.ix
                A is    9 10 11 12 13 14 15 16 17 18

Round #0
        Step 6.i
                Q is  [ 55, 55, 55, 55, 112, 113, 114, 115, 55, 55,
55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 89, 199, 207, 155,
163, 54 ]
        Step 6.ii
                R is  [ 169, 244, 14, 81, 94, 34, 73, 25, 163, 180,
21, 69, 163, 95, 31, 120 ]
        Step 6.iii
                S is a9f40e515e224919a3b41545
        Step 6.iv
                y is  52598012173893380641865864517
        Step 6.v
                m is 9
        Step 6.vi
                c is  82906087076
        Step 6.vii
                C is    0 1 2 3 4 5 6 7 8
        Step 6.viii
                B is    9 10 11 12 13 14 15 16 17 18
        Step 6.ix
```

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

PT is <0123456789abcdefghi>

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