ARIA 테스트 벡터

Version 1.0.

2004년 5월 5일

ARIA 테스트 벡터

본 문서에서는 ARIA를 위한 테스트 벡터들을 제시한다. 테스트 벡터는 암호키의 길이인 128, 192, 256 비트 세 경우에 대해 각각 별도로 주어지고, 하나의 암호키 길이마다 먼저 키와 평문을 고정했을 때의 각 라운드 키와 라운드 출력값을 제시하며, 또한 128 비트 암호문 10 블록에 대한 ECB, CBC, CFB-128, CFB-64, CFB-16, CFB-8, OFB-128, OFB-64, OFB-16, OFB-8, Counter 운영 모드에 의한 암호화 결과를 제시하도록 한다. 모든 데이터는 16진법으로 표기된다.

제 1 절 128 비트 암호키에 대한 테스트 벡터

먼저, 128 비트 암호키에 대하여 다음의 키와 평문을 사용했을 때의 각 라운드 키와 라운드 출력값을 제시하도록 한다.

- 128 비트 암호키

```
key        : 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff
```

- 128 비트 평문

```
plaintext  : 11 11 11 11 aa aa aa aa 11 11 11 11 bb bb bb bb
```

- 암/복호화 라운드 키

```
Encryption keys:
 1 round key : 63 cd f6 c4 8e a6 ab 28 84 19 46 87 62 f0 ae e4
 2 round key : 7b a3 70 31 e7 7d c8 c1 f3 da 3a 4e c4 20 5b aa
 3 round key : f3 70 da 55 0c 86 8f 1f 88 a5 6e fc 52 7f 19 fe
 4 round key : 0e 1c b5 92 d3 68 e4 90 e5 fd 31 dc fd e9 09 fe
 5 round key : 01 a7 1f fe 0b 29 c9 4b 5d 69 62 b5 0f 17 0c 2b
 6 round key : f3 73 96 4c 10 00 bc 5d ad 8c 52 9e b2 97 51 52
 7 round key : ac 00 8c e6 01 b2 3a db b7 7b 3f ee b8 01 61 76
 8 round key : 2a 78 88 6e f7 0c c8 7c c1 99 0c 20 d9 8d 25 12
 9 round key : ec 2d 8c 1e 04 4e 05 ab 5c 6e 60 48 01 82 e2 7f
10 round key : ec 9a 93 65 2f b4 b8 1a 46 4a fc ef ac 1d 8c d9
11 round key : 74 5a 14 34 9f 23 5f f6 ef 5e 4d 68 34 83 31 6a
12 round key : 42 d0 60 c7 8e b5 31 c5 a9 31 e4 89 a0 34 dc ab
             : 35 6d 10 30 f4 a7 de c2 88 f4 25 c8 9f 02 c5 30

Decryption keys:
 1 round key : 35 6d 10 30 f4 a7 de c2 88 f4 25 c8 9f 02 c5 30
 2 round key : 08 83 09 b7 c0 3b a6 92 a2 e3 15 a1 5c 08 da 6d
 3 round key : f7 2e e1 36 9f b9 32 01 e3 3f 5a 12 e5 c8 fb 3a
```

```
 4 round key : 6f 44 6b c0 37 33 62 5f 7b b5 78 a9 a2 8c 3b f1
 5 round key : 4d 25 7a 41 a7 a4 46 a1 f3 21 78 b0 28 e2 7c a8
 6 round key : a1 6b a0 de 78 43 1f 6b 4a 4a 7c 08 24 b0 23 d4
 7 round key : 71 e7 24 74 dc b4 06 3c 3e 13 22 12 40 22 0d c1
 8 round key : 07 0a f3 a4 55 f2 c3 95 5a 41 0e f8 a4 36 ec 58
 9 round key : 13 6d 96 af f8 7e 46 60 b8 f0 60 cb e9 55 0d 8e
10 round key : 5d 56 c5 fb 1d 66 f3 47 77 b6 59 6d 01 d5 0f 38
11 round key : 9d c2 cd 9e 3c 05 d0 f3 7f 3d 8f 72 31 af 6c 38
12 round key : 4c 8b 96 c8 3a 64 ce 03 4e bc 8d 22 8a aa 1f 2a
             : 63 cd f6 c4 8e a6 ab 28 84 19 46 87 62 f0 ae e4
```

- 라운드 별 출력값

```
Encryption:
 1 round : 71 f2 58 e5 33 a1 25 79 48 29 48 8f 65 5d 8f f6
 2 round : d5 b0 6a 76 fb 8b 55 96 3f c4 4b 2f 03 f0 70 4d
 3 round : 8d 40 db a4 e1 86 bb 7b bf d9 c1 57 04 4b 24 74
 4 round : 6c 07 61 05 c3 1e 92 ac ab 19 8d 71 59 a3 04 6c
 5 round : ae 5c 56 34 83 ff 97 9e be e0 78 c6 94 3d 7f e8
 6 round : 83 4c bc 0e 00 c0 5e 66 d4 04 36 19 f6 6c 61 71
 7 round : 4f 6b f4 a8 2a 33 7b 1d e1 fb 5d 56 7b f7 01 42
 8 round : b8 34 ab 22 69 87 b9 99 f4 dc ba 5d 24 a5 c3 37
 9 round : 48 c9 b1 56 b1 f1 8d 37 73 19 57 f5 11 e9 c9 7b
10 round : 18 c0 6a 98 d0 d5 e3 4a 9f 63 a2 94 39 56 1c 6f
11 round : 4f f0 7f d1 78 83 28 84 29 3a 5f 91 5f f6 34 bb
12 round : c6 ec d0 8e 22 c3 0a bd b2 15 cf 74 e2 07 5e 6e

Decryption:
 1 round : 58 0c 83 f3 44 88 de 8a f3 0d 74 a2 8b ba 20 d4
 2 round : ea 71 72 cd 40 83 a4 de 3a 60 38 3c 28 8a 95 c7
 3 round : 4f 33 56 cc 0b e1 1a 33 b9 65 02 09 9d e5 40 96
 4 round : f1 ab 6a 66 6e 49 2b 26 a7 29 a9 f2 32 b3 4a a0
 5 round : b4 92 a8 42 04 4f 93 e8 b1 0a 3c e2 0b 7a 71 ac
 6 round : fc aa 9e 73 fe d4 f7 77 bc cc c7 55 63 19 3c 62
 7 round : 3b 1f 79 97 bd 16 94 bb 18 f6 6f 8c 15 5e 53 00
 8 round : 52 39 09 2a 59 43 89 d0 fe 3b ec 84 80 87 d5 7f
 9 round : aa 66 39 72 75 2b 89 bf de 31 9b 71 d0 09 eb ce
10 round : 3e 00 f9 b2 25 8a 85 83 81 da cf b4 c0 4b 24 ab
11 round : 0c f9 26 74 0c 58 c7 ce 64 de 57 16 bf 3f 30 e4
12 round : 11 11 11 11 aa aa aa aa 11 11 11 11 bb bb bb bb
```

다음으로 각 운영 모드에 대한 출력값을 제시하도록 한다. 먼저 사용할 암호키, 초기치, 그리고 평문 10 블록은 다음과 같다.

- 128 비트 암호키

```
key         : 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff
```

- 128 비트 초기 벡터(IV)

```
IV          : 0f 1e 2d 3c 4b 5a 69 78 87 96 a5 b4 c3 d2 e1 f0
```

- 평문 10 블록

```
plaintext  : 11 11 11 11 aa aa aa aa 11 11 11 11 bb bb bb bb
           : 11 11 11 11 cc cc cc cc 11 11 11 11 dd dd dd dd
           : 22 22 22 22 aa aa aa aa 22 22 22 22 bb bb bb bb
           : 22 22 22 22 cc cc cc cc 22 22 22 22 dd dd dd dd
           : 33 33 33 33 aa aa aa aa 33 33 33 33 bb bb bb bb
           : 33 33 33 33 cc cc cc cc 33 33 33 33 dd dd dd dd
           : 44 44 44 44 aa aa aa aa 44 44 44 44 bb bb bb bb
           : 44 44 44 44 cc cc cc cc 44 44 44 44 dd dd dd dd
           : 55 55 55 55 aa aa aa aa 55 55 55 55 bb bb bb bb
           : 55 55 55 55 cc cc cc cc 55 55 55 55 dd dd dd dd
```

이제 각 운영 모드에 의한 위의 평문의 암호화 결과는 다음과 같다. (Counter 모드의 경우 카운터는 0으로 출발하여 1씩 증가시켰다.)

```
ECB mode   : c6 ec d0 8e 22 c3 0a bd b2 15 cf 74 e2 07 5e 6e
           : 29 cc aa c6 34 48 70 8d 33 1b 2f 81 6c 51 b1 7d
           : 9e 13 3d 15 28 db f0 af 57 87 c7 f3 a3 f5 c2 bf
           : 6b 6f 34 59 07 a3 05 56 12 ce 07 2f f5 4d e7 d7
           : 88 42 4d a6 e8 cc fe 81 72 b3 91 be 49 93 54 16
           : 56 65 ba 78 64 91 70 00 a6 ee b2 ec b4 a6 98 ed
           : fc 78 87 e7 f5 56 37 76 14 ab 0a 28 22 93 e6 d8
           : 84 db b8 42 06 cd b1 6e d1 75 4e 77 a1 f2 43 fd
           : 08 69 53 f7 52 cc 1e 46 c7 c7 94 ae 85 53 7d ca
           : ec 8d d7 21 f5 5c 93 b6 ed fe 2a de a4 38 73 e8

CBC mode   : 49 d6 18 60 b1 49 09 10 9c ef 0d 22 a9 26 81 34
           : fa df 9f b2 31 51 e9 64 5f ba 75 01 8b db 15 38
           : b5 33 34 63 4b bf 7d 4c d4 b5 37 70 33 06 0c 15
           : 5f e3 94 8c a7 5d e1 03 1e 1d 85 61 9e 0a d6 1e
           : b4 19 a8 66 b3 c2 db fd 10 a4 ed 18 b2 21 49 f7
           : 58 97 f0 b8 66 8b 0c 1c 54 2c 68 77 78 83 5f b7
           : cd 46 e4 5f 85 ea a7 07 24 37 dd 9f a6 79 3d 6f
           : 8d 4c ce fc 4e b1 ac 64 1a c1 bd 30 b1 8c 6d 64
           : c4 9b ca 13 7e b2 1c 2e 04 da 62 71 2c a2 b4 f5
           : 40 c5 71 12 c3 87 91 85 2c fa c7 a5 d1 9e d8 3a

CFB-128 mode : 37 20 e5 3b a7 d6 15 38 34 06 b0 9f 0a 05 a2 00 c0 7c
21 e6 37 0f 41 3a 5d 13 25 00 a6 82 85 01 7c 61 b4 34 c7 b7 ca 96 85
a5 10 71 86 1e 4d 4b b8 73 b5 99 b4 79 e2 d5 73 dd de af ba 89 f8 12
ac 6a 9e 44 d5 54 07 8e b3 be 94 83 9d b4 b3 3d a3 f5 9c 06 31 23 a7
```

```
ef 6f 20 e1 05 79 fa 4f d2 39 10 0c a7 3b 52 d4 fc af ea de e7 3f 13
9f 78 f9 b7 61 4c 2b 3b 9d be 01 0f 87 db 06 a8 9a 94 35 f7 9c e8 12
14 31 37 1f 4e 87 b9 84 e0 23 0c 22 a6 da cb 32 fc 42 dc c6 ac ce f3
32 85 bf 11

CFB-64 mode  : 37 20 e5 3b a7 d6 15 38 59 57 43 81 4e 94 3a cc 82 1a
05 6e 3c 5f db 10 ee ae d5 e2 de 03 e5 bb 60 f5 28 f9 ba d9 a2 67 e9
8d a2 23 70 54 ef 90 60 56 4e c4 89 a1 95 33 ab 0f ad 70 fe 04 4b 43
a3 c0 57 9d a9 de f9 a2 6e 42 8d bd ac 64 5e bf aa 94 bc e0 88 52 cd
1f 35 38 d5 7e a3 fa 9f 1a 37 23 84 6f 22 87 62 7c 94 b1 5a 06 13 6b
66 83 50 4c 98 60 e2 ad 9d e7 d9 6f 31 00 83 a4 aa 25 10 f2 f6 7b 04
fe a7 74 80 1c ae 4f 0d 0a 6b ad 46 7b 6c 3a 90 e0 19 a7 c6 7a d2 44
93 bb df 46

CFB-16 mode  : 37 20 3a 2a c0 bf f7 52 e4 ba b5 89 f4 ad 3e a8 22 77
a6 ff 4b 58 41 ad 92 f4 b8 e5 d1 aa 6e 8a 95 bf de 0a d6 ec 9f 7c c7
11 e4 f6 72 12 d0 af e9 24 97 46 30 54 be cd 39 8e 26 ee 39 38 8b e7
25 fa 38 c3 3a d0 7c fa da 2b e8 3a 77 0a 03 4e 96 9b 29 b9 c6 d3 52
3e 14 8d 06 95 f2 33 8f 95 ff 2e c0 1a b6 9f cf 8f 9c 77 fc b7 16 91
ce b8 30 fd 16 6d 05 de dd b2 db a6 a3 8e ff 5b f1 42 b1 ab fb 0f e8
b5 20 f3 a6 91 a8 a4 f8 7e 24 a6 e8 57 be ca 43 7e 66 ab cc 4a 5b f4
3d 6d 6b fe

CFB-8 mode   : 37 3c 8f 6a 96 55 99 ec 78 5c c8 f8 14 9f 6c 81 b6 32
cc b8 e0 c6 eb 6a 97 07 ae 52 c5 92 57 a4 1f 94 70 1c 10 96 93 31 27
a9 01 95 ed 0c 8e 98 69 05 47 57 24 23 bb 45 c3 d7 0e 4a 18 ee 56 b9
67 c1 0e 00 0b a4 df 5f ba 7c 40 41 34 a3 43 d8 37 5d 04 b1 51 d1 61
ef 83 41 7f e1 74 84 47 d3 0a 67 23 c4 06 73 3d f7 d1 8a a3 9a 20 75
2d 23 81 94 2e 24 48 11 bb 97 f7 2e ae 44 6b 18 15 aa 69 0c d1 b1 ad
cb d0 07 c0 08 8e cd c9 1c b2 e2 ca f0 e1 1e 72 45 98 78 13 7e ea 64
ac 62 a9 a1

OFB-128 mode : 37 20 e5 3b a7 d6 15 38 34 06 b0 9f 0a 05 a2 00 00 63
06 3f 05 60 08 34 83 fa eb 04 1c 8a de ce f3 0c f8 0c ef b0 02 a0 d2
80 75 91 68 ec 01 db 3d 49 f6 1a ce d2 60 bd 43 ee c0 a2 73 17 30 ee
c6 fa 4f 23 04 31 9c f8 cc ac 2d 7b e7 83 3e 4f 8a e6 ce 96 70 12 c1
c6 ba dc 5d 28 e7 e4 14 4f 6b f5 ce be 01 25 3e e2 02 af ce 4b c6 1f
28 de c0 69 a6 f1 6f 6c 8a 7d d2 af ae 44 14 8f 6f f4 d0 02 9d 5c 60
7b 5f a6 b8 c8 a6 30 1c de 5c 70 33 56 5c d0 b8 f0 97 4a b4 90 b2 36
19 7b a0 4a

OFB-64 mode  : 37 20 e5 3b a7 d6 15 38 00 63 06 3f 72 17 7f 43 c0 3f
cb 3f 89 d6 64 c6 0e 7a c5 29 df c3 71 ac d7 eb 5e 32 04 31 9c f8 9b
f7 df 87 07 65 b6 b1 0d 93 a8 d8 67 43 58 84 a6 0f c0 97 7e 7d 9b 6c
b6 64 fb 3a 60 7b 5f a6 55 30 3a b6 cf 87 e0 3d de d0 ae 70 8b 55 b2
08 e9 54 d4 11 80 20 36 fa 6f c0 c9 f6 96 02 9f 3a 2a 0a ca 3f cf ee
```

```
ce 10 ce af ff be 82 c1 fe 67 a5 0e a3 a0 3a ce 49 0f 7d a6 f4 20 9c
01 e2 10 b6 56 cf 1a dc 9f 68 29 bc 0c 72 40 33 bf 23 dc c8 96 c1 8c
90 39 55 d9

OFB-16 mode  : 37 20 00 63 7b 84 b5 c1 e4 d8 a8 c4 94 0a 3f 96 94 46
77 12 21 2f 16 ab 3a 95 7f 5f 57 36 3c 97 0a d1 c1 21 43 f3 37 69 30
3b 60 2b 06 4f 2c 2e 4e 78 c6 2e 39 52 72 f7 c0 b4 e0 b9 34 e6 aa 11
b3 6e 0b 5b ae 74 c0 83 91 20 8f d2 eb ef e9 5a d2 f3 c2 73 4e 6e 7c
6b 35 22 fe cd 23 05 72 c3 00 62 64 58 89 1a 21 8e e8 31 91 5b ac 49
93 7f 69 ac 1c a6 66 5d 09 d7 ef d3 37 85 93 42 2f e4 26 50 6b 1b 5a
e0 9b 3a 7f ac 2f 56 22 a0 7b 49 a5 e1 09 ec 94 08 42 77 b6 e8 e5 d4
15 e9 a4 e1

OFB-8 mode   : 37 00 c0 0e 5f 13 85 2e 94 77 fc cb 90 d5 31 5a 39 f2
f8 8c de 8e 71 5b 7d f5 e4 af 3f 1f 34 aa a2 1a 26 48 08 16 fa f8 c3
d3 a0 92 bd 76 45 14 66 02 01 a9 60 19 db e4 0f 7a 88 e7 76 ae 93 2f
40 0d c3 02 80 d0 33 6a c3 6f 6b bd 58 0b 73 c2 3e ff 27 5c de a7 32
4f 9f e5 86 06 b6 41 af cc 47 19 0e 2e 4b db fb 43 32 8a 94 86 8f 96
ba a7 6f e6 c6 2e b6 b3 34 b4 35 b2 bd 66 77 6d 67 d3 16 fe ff ed f3
89 1d 70 0c c4 57 11 bf 1f 25 60 80 c3 32 98 31 8b cd 53 7f 32 2d 11
fd cc 66 cf

CTR mode   : ac 5d 7d e8 05 a0 bf 1c 57 c8 54 50 1a f6 0f a1
           : 14 97 e2 a3 45 19 de a1 56 9e 91 e5 b5 cc ae 2f
           : f3 bf a1 bf 97 5f 45 71 f4 8b e1 91 61 35 46 c3
           : 91 11 63 c0 85 f8 71 f0 e7 ae 5f 2a 08 5b 81 85
           : 1c 2a 3d df 20 ec b8 fa 51 90 1a ec 8e e4 ba 32
           : a3 5d ab 67 bb 72 cd 91 40 ad 18 8a 96 7a c0 fb
           : bd fa 94 ea 6c ce 47 dc f8 52 5a b5 a8 14 cf eb
           : 2b b6 0e e2 b1 26 e2 d9 d8 47 c1 a9 e9 6f 90 19
           : e3 e6 a7 fe 40 d3 82 9a fb 73 db 1c c2 45 64 6a
           : dd b6 2d 9b 90 7b aa af be 46 a7 3d bc 13 1d 3d
```

제 2 절 192 비트 암호키에 대한 테스트 벡터

192 비트 암호키에 대하여 다음의 키와 평문을 사용했을 때의 각 라운드 키와 라운드 출력값을 제시하도록 한다.

- 192 비트 암호키

```
key         : 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff
              00 11 22 33 44 55 66 77
```

- 128 비트 평문

```
plaintext  : 11 11 11 11 aa aa aa aa 11 11 11 11 bb bb bb bb
```

- 암/복호화 라운드 키

```
Encryption keys:
 1 round key : 8c b8 5c 32 5b e2 09 ac 82 b0 93 7c 03 3f 56 ba
 2 round key : e1 92 e9 ed 1e fb c7 9a 56 4a ee 3e 5c 0b 12 6a
 3 round key : 5c 2c 50 ea d0 1d 3c b4 d8 cf 59 33 bc d2 4f 05
 4 round key : 32 6c d4 0d dc c4 e4 17 ec 8e df c5 2b f8 8d 61
 5 round key : 84 49 e8 a4 a4 44 9d 01 75 29 08 28 50 a1 10 d4
 6 round key : 82 19 e4 1a 3b be 53 70 a3 07 f8 5c d0 95 87 3c
 7 round key : 9f ec e8 e9 a9 fa ab bb 78 59 e8 01 39 88 d1 7c
 8 round key : 16 08 e9 f1 f8 a0 c8 fb c8 ea e2 39 0f 9c a1 8d
 9 round key : 39 d6 ed d1 fc 10 ea de f6 98 b5 0c a3 06 e4 d6
10 round key : 61 23 63 9c 09 f9 40 d3 da 68 1f 36 54 ff fd 3f
11 round key : 0a bb 04 c6 75 49 3d 3b d8 aa 97 ba 46 18 dd 43
12 round key : 7e a0 01 58 81 19 31 42 a0 42 0a 90 76 25 58 34
13 round key : bf 7d 0a 97 a3 4a 59 fd 69 8f 98 1e 34 d9 90 22
14 round key : ab 46 9c 69 3a 76 29 d4 12 ba 39 7d 93 75 e5 c5
             : 5e f2 47 52 16 bc d4 cf 86 0b 0b 46 fe d1 16 d7

Decryption keys:
 1 round key : 5e f2 47 52 16 bc d4 cf 86 0b 0b 46 fe d1 16 d7
 2 round key : 42 c0 47 dd 0e b6 86 8f 8a b9 08 d7 73 61 ac 78
 3 round key : c2 4d 17 c7 3a ec b2 29 ff 6b 1c e8 76 a4 c0 4d
 4 round key : 77 fa c8 c2 3a 5d 26 aa 06 48 c0 f6 76 da 34 a7
 5 round key : 39 01 db 90 bb ab 56 7c 33 e4 35 bd ef 9d 3d 8f
 6 round key : 65 90 28 60 d5 03 0d b8 47 64 5c e4 d9 54 ae 4a
 7 round key : 4b 38 0c ac 0c e4 82 b2 a8 5e e0 c1 38 99 74 42
 8 round key : de 12 61 ab 82 25 9f 53 ee e1 a9 5f 0e 62 cd 1e
 9 round key : 93 cd 42 6e 59 b0 cc 66 7d cb dc a2 75 7e ac bb
10 round key : c4 62 39 fa 9c 7c ac ea 81 7d 19 e5 55 75 c1 1f
11 round key : 70 75 d4 50 b1 ac bd dc 15 7c 95 80 6c 60 d1 e8
12 round key : 22 2f 04 8e e7 00 73 7f d3 1d 8c 3a 2b 07 e1 f2
13 round key : 8c 57 13 02 b0 ca 40 7f 9a 91 94 e2 b4 6d c8 35
14 round key : 31 a2 ad 49 e3 bd 61 87 78 3f 0f 84 0e e2 8f 4c
             : 8c b8 5c 32 5b e2 09 ac 82 b0 93 7c 03 3f 56 ba
```

- 라운드 별 출력값

```
Encryption:
 1 round : ab cc ef ff be 1a 1a c2 c2 b7 04 8e ae ea 9a 29
 2 round : d2 f1 9b ff 2f fb e4 40 53 5b 04 69 f8 6f 0f c0
 3 round : 4e 25 a5 6a 11 47 0e 73 54 ae 6b 27 6f 1f 89 40
 4 round : 88 5b d9 68 c2 b8 30 2e 9a 74 8b a8 c6 c1 b4 ef
 5 round : b5 bf dc 65 ff 30 17 11 c2 7a 26 7e f1 cd 06 d0
 6 round : 85 78 a7 6a 9f 2e d6 1a d5 33 5d db 80 cd ba 30
 7 round : 2b 96 8b b0 76 66 a5 66 85 e2 97 4f 25 85 23 2a
```

```
 8 round : 9e 74 98 be 4e 4f 41 7e c0 20 ca c0 a6 08 d2 7d
 9 round : 3a 87 b2 48 67 5d 1c c8 83 b4 44 6a 54 ea b2 b9
10 round : 9d 2c 2e 87 b2 82 2e 4f 51 58 34 0d 64 be fb d3
11 round : d6 ee 53 31 2d d3 a0 55 05 8b 82 4a 1a 41 fb 24
12 round : 11 0c 88 75 ff 30 af 0d 67 b0 07 38 16 b4 29 75
13 round : cd 14 2e a9 01 2c 0c f8 17 c6 55 dd 46 18 89 c6
14 round : 8d 14 70 62 5f 59 eb ac b0 e5 5b 53 4b 3e 46 2b

Decryption:
 1 round : a6 6b 56 dd 44 d6 50 aa 21 52 66 a0 e0 ab 77 eb
 2 round : ad 4c 17 49 90 81 33 02 d6 ee d8 68 ce b6 ca 13
 3 round : ff 9f 5d e0 fc 79 a4 c1 a1 a8 b1 86 e5 0e 17 47
 4 round : 6e 5c e5 bc fe f6 1c 7f 26 6b 0c 2e bd 3d b9 0b
 5 round : 39 6d 17 b9 e2 50 03 3c 42 14 37 e3 b2 df 8a 3b
 6 round : c0 aa a6 d3 ea 25 be 97 cd 0e 7d 83 ad 84 67 d8
 7 round : 7c f1 f3 fe 87 09 8c ba 7b d6 7b 90 58 ad c8 2b
 8 round : 21 08 45 2e d1 d9 d7 e1 a5 2f c1 e3 0e 18 a0 6d
 9 round : 3a 06 17 fd af d3 b4 a7 5e d9 58 3f c5 8a dc 87
10 round : 71 fd 77 18 31 f9 3a ea 8f fd 18 db ea 4e 23 ee
11 round : 3b 6b 5d 2e f1 52 5e 3d ee fe 01 df 30 7e 93 5b
12 round : d0 47 7c 66 f7 7b 81 38 7d 33 13 45 b0 dc 0c 1c
13 round : 6f 67 c8 c0 42 30 10 a6 a4 e2 1e 6b 62 42 dc 24
14 round : 11 11 11 11 aa aa aa aa 11 11 11 11 bb bb bb bb
```

다음으로 각 운영 모드에 대한 출력값을 제시하도록 한다. 먼저 사용할 암호키, 초기치, 그리고 평문 10 블록은 다음과 같다.

- 192 비트 암호키

```
key         : 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff
              00 11 22 33 44 55 66 77
```

- 128 비트 초기 벡터(IV)

```
IV          : 0f 1e 2d 3c 4b 5a 69 78 87 96 a5 b4 c3 d2 e1 f0
```

- 평문 10 블록

```
plaintext   : 11 11 11 11 aa aa aa aa 11 11 11 11 bb bb bb bb
            : 11 11 11 11 cc cc cc cc 11 11 11 11 dd dd dd dd
            : 22 22 22 22 aa aa aa aa 22 22 22 22 bb bb bb bb
            : 22 22 22 22 cc cc cc cc 22 22 22 22 dd dd dd dd
            : 33 33 33 33 aa aa aa aa 33 33 33 33 bb bb bb bb
            : 33 33 33 33 cc cc cc cc 33 33 33 33 dd dd dd dd
            : 44 44 44 44 aa aa aa aa 44 44 44 44 bb bb bb bb
            : 44 44 44 44 cc cc cc cc 44 44 44 44 dd dd dd dd
            : 55 55 55 55 aa aa aa aa 55 55 55 55 bb bb bb bb
            : 55 55 55 55 cc cc cc cc 55 55 55 55 dd dd dd dd
```

이제 각 운영 모드에 의한 위의 평문의 암호화 결과는 다음과 같다. (Counter 모드의 경우 카운터는 0으로 출발하여 1씩 증가시켰다.)

```
ECB mode   : 8d 14 70 62 5f 59 eb ac b0 e5 5b 53 4b 3e 46 2b
           : 5f 23 d3 3b ff 78 f4 6c 3c 15 91 1f 4a 21 80 9a
           : ac ca d8 0b 4b da 91 5a a9 da e6 bc eb e0 6a 6c
           : 83 f7 7f d5 39 1a cf e6 1d e2 f6 46 b5 d4 47 ed
           : bf d5 bb 49 b1 2f bb 91 45 b2 27 89 5a 75 7b 2a
           : f1 f7 18 87 34 86 3d 7b 8b 6e de 5a 5b 2f 06 a0
           : a2 33 c8 52 3d 2d b7 78 fb 31 b0 e3 11 f3 27 00
           : 15 2f 33 86 1e 9d 04 0c 83 b5 eb 40 cd 88 ea 49
           : 97 57 09 dc 62 93 65 a1 89 f7 8a 3e c4 03 45 fc
           : 6a 5a 30 7a 8f 9a 44 13 09 1e 00 7e ca 56 45 a0

CBC mode   : af e6 cf 23 97 4b 53 3c 67 2a 82 62 64 ea 78 5f
           : 4e 4f 7f 78 0d c7 f3 f1 e0 96 2b 80 90 23 86 d5
           : 14 e9 c3 e7 72 59 de 92 dd 11 02 ff ab 08 6c 1e
           : a5 2a 71 26 0d b5 92 0a 83 29 5c 25 32 0e 42 11
           : 47 ca 45 d5 32 f3 27 b8 56 ea 94 7c d2 19 6a e2
           : e0 40 82 65 48 b4 c8 91 b0 ed 0c a6 e7 14 db c4
           : 63 19 98 d5 48 11 0d 66 6b 3d 54 c2 a0 91 95 5c
           : 6f 05 be b4 f6 23 09 36 86 96 c9 79 1f c4 c5 51
           : 56 4a 26 37 f1 94 34 6e c4 5f bc a6 c7 2a 5b 46
           : 12 e2 08 d5 31 d6 c3 4c c5 c6 4e ac 6b d0 cf 8c

CFB-128 mode : 41 71 f7 19 2b f4 49 54 94 d2 73 61 29 64 0f 5c 4d 87
a9 a2 13 66 4c 94 48 47 7c 6e cc 20 13 59 8d 97 66 95 2d d8 c3 86 8f
17 e3 6e f6 6f d8 4b fa 45 d1 59 3d 2d 6e e3 ea 21 15 04 7d 71 0d 4f
b6 61 87 ca a3 a3 15 b3 c8 ea 2d 31 39 62 ed cf e5 a3 e2 02 8d 5b a9
a0 9f d5 c6 5c 19 d3 44 0e 47 7f 0c ab 06 28 ec 69 02 c7 3e e0 2f 1a
fe e9 f8 01 15 be 7b 9d f8 2d 1e 28 22 8e 28 58 1a 20 56 0e 19 5c bb
9e 2b 32 7b f5 6f d2 d0 ae 55 02 e4 2c 13 e9 b4 01 5d 4d a4 2d c8 59
25 2e 7d a4

CFB-64 mode  : 41 71 f7 19 2b f4 49 54 3d 2e 82 1b e5 10 70 cf 40 6c
d5 31 40 10 6a 8e 88 e7 6c a3 6c 18 2b d1 2d 70 3f 53 ee 98 19 3b 8b
d2 2a 40 86 46 ec 98 d6 ee 2e 93 af b1 fd 8e d0 1c 51 1c b7 87 c9 17
c3 86 e7 d3 1d 3e 42 92 1d 86 4e aa be 55 b8 cf 14 76 dc 0a ab cb f6
3d 2d 31 91 43 c1 26 95 c2 67 98 ec c5 fc 3f 3f 2a 16 6f 95 88 35 8a
65 55 25 c2 bb f9 8c eb 39 05 52 cd 31 13 34 37 89 b3 ad 12 53 1c cc
ca 79 79 c7 81 c0 11 4d 70 be b0 73 d1 75 c9 42 07 c5 d5 29 90 fc 30
74 bd 8b 0b

CFB-16 mode  : 41 71 bb f5 01 18 55 7e f0 c8 f1 b6 dd 18 97 77 dc cf
7f b1 f1 2e 2d 2f 3d cd be 86 c2 0c 78 02 c5 61 d8 72 95 64 5f bc 20
54 2f e5 85 73 24 a1 7a 67 1b 75 4b 52 3e e8 90 da 74 19 71 fe 2f ab
```

```
8b 4b 31 4c fd 69 1f 06 ab 30 8b 48 61 90 e0 fe a3 e4 22 f3 d6 df 17
3f d4 3c b8 22 90 cc a2 cf 43 8e b1 07 cf 83 98 70 2b 09 1a b5 e0 7d
0d f5 fd 50 55 ce 27 90 e7 7b 41 9b 32 ae 67 9a 92 de 4d 1a de a1 d0
77 18 50 e7 da d0 ae 2e ac 8c 4e 17 fa 39 95 ae 3d 2c 20 72 52 1d 0f
0b f6 4d 51

CFB-8 mode   : 41 1d 3b 4f 57 f7 05 aa 4d 13 c4 6e 2c f4 26 af 7c 8c
91 6e d7 92 3d 88 9f 00 47 bb f1 14 71 b6 d5 4f 87 57 ef 51 93 39 10
5b e3 cb 69 ba bb 97 6a 57 d5 63 1f c2 3c c3 05 1f e9 d3 6e 8b 8e 27
a2 b2 c0 c4 d3 19 28 cc bf 30 ea 82 39 b4 6b a1 b7 7f 61 98 e7 ec d2
ce 27 b3 59 58 14 8e 82 6f 06 aa f3 85 bd 30 36 2f f1 41 58 3e 7c 1d
89 24 d4 4d 36 a1 13 30 94 07 46 31 e1 8a da fa 9d 2e 55 de 98 f6 89
5c 89 d4 26 6e bd 33 f3 d4 be 51 53 a9 6f a1 21 32 ec e2 e8 1e 66 e5
5b aa 7a de

OFB-128 mode : 41 71 f7 19 2b f4 49 54 94 d2 73 61 29 64 0f 5c c2 24
d2 6d 36 4b 5a 06 dd de 13 d0 f1 e7 4f aa 84 6d e3 54 c6 3c da 77 46
9d 1a 2d 42 5c 47 ff 41 73 4c 71 b3 fa 1f cd c1 1e 0b 2d e2 2b fe ed
54 89 8e 23 3d f6 52 c7 5a e1 36 e6 1d e6 52 4e 62 b3 f8 06 fb 2e 8e
61 6e b4 10 a1 b9 50 05 37 e3 27 ff b0 4f 19 f7 f8 2f de 2b 12 21 00
26 1f 81 b8 27 23 bf 93 6b e7 be aa f3 06 7d 1c 03 60 01 f1 ad e7 14
22 26 8d 27 4d 7d c6 c6 ae 19 70 b2 7a 5f 2c 2f 39 c1 d2 41 fe 8c ac
5c cd 74 e9

OFB-64 mode  : 41 71 f7 19 2b f4 49 54 c2 24 d2 6d 41 3c 2d 71 b7 5e
d0 67 a0 5a bc 11 72 40 7f 42 a2 eb 0e dc 45 98 9f 32 3d f6 52 c7 73
a2 e9 17 8c 59 f9 16 85 41 99 d6 29 7f 91 9e e7 de 41 45 ae 82 7a f6
67 97 cb 81 14 22 26 8d d4 1c 39 4a 58 4e b6 a5 4b b9 5b aa 23 0a d0
d1 d7 e4 7c 63 6f 79 3a 4e 66 11 36 6c e1 d5 7c 6a d0 db 8f 54 74 9d
35 27 1c d4 a9 c7 e4 9a 5f f7 14 5c fc c3 4d 0c 59 82 73 06 d4 93 01
29 18 10 0a 56 2b 4f d9 49 df 63 fe ae 5c 20 56 a6 ae 37 60 ee c9 06
9b 06 30 40

OFB-16 mode  : 41 71 c2 24 0c e5 c9 fb 76 ab 40 91 1c d8 7e 47 45 b5
f6 3e b4 46 28 1b 33 44 85 8e 85 4d 8d c5 04 71 7d 21 01 51 9f 11 10
ec ce 00 1b 4b 42 37 6b 0d 36 5c 8a ce a1 58 a7 fa a9 42 2b be fa f9
86 58 cb 5d c9 bc ff 97 9e 5b 8e 48 be 56 f0 58 76 7d d8 72 84 ef a1
12 65 fd 21 2e 44 66 b5 90 4b 63 eb 79 b4 11 f3 df b4 5a 25 f9 2a 33
0e 88 b3 7e f7 9f a1 73 cf 67 41 7e fe 99 a2 32 d1 eb 80 89 fc 7e 39
28 60 9f 98 86 3b 76 89 ad 25 07 36 7d fd 89 69 80 8b 42 85 5b 17 ee
4e df 2f d9

OFB-8 mode   : 41 c2 b7 72 cd fb 0d 6f 45 f6 69 f5 99 2f e3 eb 37 4e
ba 24 fe 20 6c 35 58 05 57 7c 58 56 2b fa 97 da 41 77 07 17 af e1 67
c9 6a 4f ed a9 22 d3 2d 8d 3c 7b 3c ad 5d 79 d5 91 4f 21 d8 67 a2 d1
e6 9a a0 f9 67 c4 98 34 50 9b 96 74 6b f9 28 49 c9 f8 77 6a 3b d0 4e
```

```
3d 34 4c 8b cc 43 19 27 4b 10 5d c0 89 c1 09 d5 d7 f0 ed e8 d3 c2 37
8b 85 c4 94 d4 b8 15 2c 73 90 63 86 78 62 8f 59 1b 9b 48 61 61 b9 8e
d5 81 fc 38 7f 93 45 9b 49 08 64 37 ee 4c 12 33 2e d6 f0 39 18 e2 da
5f bd 35 e1

CTR mode   : 08 62 5c a8 fe 56 9c 19 ba 7a f3 76 0a 6e d1 ce
           : f4 d1 99 26 3e 99 9d de 14 08 2d bb a7 56 0b 79
           : a4 c6 b4 56 b8 70 7d ce 75 1f 98 54 f1 88 93 df
           : db 3f 4e 5a fa 53 97 33 e6 f1 e7 0b 98 ba 37 89
           : 1f 8f 81 e9 5d f8 ef c2 6c 7c e0 43 50 4c b1 89
           : 58 b8 65 e4 e3 16 cd 2a a1 c9 7f 31 bf 23 dc 04
           : 6e f3 26 b9 5a 69 2a 19 1b a0 f2 a4 1c 5f e9 ae
           : 07 0f 23 6f f7 07 8e 70 3b 42 66 6c aa fb dd 20
           : ba d7 4a c4 c2 0c 0f 46 c7 ca 24 c1 51 71 65 75
           : c9 47 da 16 c9 0c fe 1b f2 17 a4 1c fe be 75 31
```

제 3 절 256 비트 암호키에 대한 테스트 벡터

256 비트 암호키에 대하여 다음의 키와 평문을 사용했을 때의 각 라운드 키와 라운드 출력값을 제시하도록 한다.

- 256 비트 암호키

```
key         : 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff
              00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff
```

- 128 비트 평문

```
plaintext  : 11 11 11 11 aa aa aa aa 11 11 11 11 bb bb bb bb
```

- 암/복호화 라운드 키

```
Encryption keys:
 1 round key : fb a8 40 05 a4 87 5e 48 d3 57 34 2f 94 df 1f ae
 2 round key : 4d d0 a2 3d 60 74 8e 4b d0 fe 3f b4 1a 85 a2 39
 3 round key : 21 db 65 bb c9 89 f9 38 c1 f9 15 fb 16 38 04 a8
 4 round key : f3 95 a3 84 fa bf 8f a6 01 89 bc 44 09 ff 5c 68
 5 round key : 15 0e 99 a5 67 3b 6b 54 0b 6c 16 52 25 98 6e d0
 6 round key : ee 92 c0 eb 8b 30 c6 91 f7 50 85 d8 70 b6 dd 6c
 7 round key : 5c 35 47 94 1d 6d a5 ea 40 ef 4e 0a a5 1c 79 93
 8 round key : d7 f1 9e 78 de db a3 4a 25 ed 81 b8 2d 9b 70 84
 9 round key : 9e 85 7a 31 b5 04 9d ce ea af 4a 69 f4 e2 b5 31
10 round key : ee 14 96 9b be 08 82 13 50 0e 61 99 da b0 f9 97
11 round key : b0 cd e5 d8 66 6c 26 59 94 d5 c8 23 24 4d df d8
12 round key : bf 59 76 d1 a7 62 5a f3 4d 45 69 11 54 22 89 3d
13 round key : e0 ec 4d 09 3e 04 06 7c 4d de 44 5e 44 06 6d b7
```

```
14 round key : 51 4b 97 e2 3f 74 9e 5d 0b 6b b1 89 18 3d 5b f2
15 round key : 4a 19 ff e4 d7 5a 84 4c 63 48 92 aa 58 b7 c2 fe
16 round key : ec 60 f0 bd 1a b5 32 71 4b 29 ba 28 bc a0 b4 ea
             : 34 9f 2d e5 b7 f2 c3 61 88 25 fe c5 22 85 63 47

Decryption keys:
 1 round key : 34 9f 2d e5 b7 f2 c3 61 88 25 fe c5 22 85 63 47
 2 round key : e3 00 8c ae 94 0a e2 90 17 2b cb 07 6e 43 4b 24
 3 round key : e9 64 d4 11 1a cc cc 5f 13 bd ef 52 94 20 03 64
 4 round key : 45 34 38 26 99 e5 64 90 06 3a 5b 3f e5 f7 41 df
 5 round key : c9 55 3d e9 60 9b 09 b2 bb 79 ba f1 1f 9c 3e 25
 6 round key : 8f 86 b5 fd 43 b7 60 f8 c4 12 cd 6b 86 c1 76 f3
 7 round key : 4b 6d 9a fc 89 69 78 ed 1f ef 76 2c 85 06 4b a6
 8 round key : b0 9e 9d 44 d7 30 6e ae 11 ca f0 8d 5e 65 ad 92
 9 round key : 0b 30 4b 20 e7 60 d9 bc f9 aa eb de 9e be 6d df
10 round key : 26 6e 1c 94 fb cf d9 01 2c bb a4 c2 fe 79 8f 4a
11 round key : e6 59 ff fa d6 f7 e9 f7 5f 77 d4 17 7d 95 24 9f
12 round key : 6a da 9e 79 80 96 ac 56 39 ff f0 cc fd 96 eb f7
13 round key : 38 64 b3 c8 50 08 1f 24 76 52 2f 28 b3 0a bc 06
14 round key : da 53 79 b1 9e ea 35 2d 11 47 81 a7 db 1c a3 a6
15 round key : 8f 52 bb 42 5b e9 be 8d 8e 63 ff c4 6b b7 dc 82
16 round key : da 90 96 de 64 d7 fa 98 35 6b 09 f2 e7 df 8c b0
             : fb a8 40 05 a4 87 5e 48 d3 57 34 2f 94 df 1f ae
```

- 라운드 별 출력값

```
Encryption:
 1 round : 43 92 f8 2a 2b 8d bb d3 7d 74 57 8f ec 1d 29 46
 2 round : 96 fc 55 0b ea 12 03 d6 2a 3a 6e 32 a2 75 50 55
 3 round : a9 86 f2 fe ac b3 76 58 55 1f ad c3 0b ae 69 31
 4 round : dd 6e 99 53 51 ac 3c 26 5f db be 75 29 b7 4b 30
 5 round : 75 f3 85 81 09 56 78 41 e8 52 43 44 a7 dd 7f 70
 6 round : c3 36 d5 79 7e 0a 63 7c b3 43 fe 00 b2 cb b7 09
 7 round : 4c ac b0 f3 7a be f6 72 2c 6f 3e a9 ae b6 51 6d
 8 round : 9e f1 2b 0a a8 13 27 d0 fe 1d b4 28 59 69 e7 8a
 9 round : d1 0f 34 a5 87 43 d1 9e ab b3 99 85 d7 46 ce e2
10 round : 1b a3 37 36 a0 f3 f6 cf 07 07 f6 84 dd 22 67 60
11 round : bc 13 9f f9 54 d3 72 f0 31 bd f0 63 49 b7 86 90
12 round : 6b d3 06 99 a9 8b bb 40 82 2c 93 29 f5 53 a3 90
13 round : a0 78 b4 96 94 44 5b 1e 1a fa f2 6c d7 18 9c 32
14 round : 93 04 64 d9 82 82 bb fa 58 6d ca 1b 08 04 fa c2
15 round : bc 84 ae a6 77 c5 a9 e3 0b 1e 7f 49 64 d1 89 e0
16 round : 58 a8 75 e6 04 4a d7 ff fa 4f 58 42 0f 7f 44 2d

Decryption:
 1 round : d6 19 64 5a 68 57 c7 ec f5 db 95 68 3d b6 3d 28
```

```
 2 round : c2 87 f2 d5 14 0c 6a 76 f0 fa f5 08 cb bd c5 54
 3 round : 78 df f4 c6 11 39 a9 9c 8c da 56 26 2d 74 ad 19
 4 round : 1c 53 23 03 1e f4 3d 4e ba 8e 54 fd c1 d7 48 53
 5 round : ed 6f ca c0 f7 52 00 cc 18 b0 1c db 1f 70 ec a9
 6 round : 6e db a0 ec d2 aa 95 f2 7c 6c 37 ff 76 c1 d1 f0
 7 round : d3 5a ed dc 73 1b ae 6a eb 1a fc af cb 2a e5 bd
 8 round : e3 e8 7a 6f fa f7 25 86 b9 67 e3 24 df fe 90 7e
 9 round : fd 92 68 64 00 87 1e 35 21 45 58 19 0e e6 63 ed
10 round : 0e b1 91 cd c7 c5 47 11 94 ee 60 ff 70 b6 1e 4c
11 round : 82 25 cc be 85 f3 76 8a 19 cb 9f 0a 03 2d 29 05
12 round : 7e ea 62 a8 e9 7a 86 91 8b 66 ad 2c d9 c8 2a dd
13 round : 73 3a 71 5a b8 d4 21 10 f8 0c 82 22 56 33 5e 04
14 round : 58 24 05 69 97 a5 28 b6 96 d8 ba 6e bd ce e1 c2
15 round : 5d 95 e6 2f cf 08 40 98 10 c6 cb 69 f2 e9 91 10
16 round : 11 11 11 11 aa aa aa aa 11 11 11 11 bb bb bb bb
```

다음으로 각 운영 모드에 대한 출력값을 제시하도록 한다. 먼저 사용할 암호키, 초기치, 그리고 평문 10 블록은 다음과 같다.

- 256 비트 암호키

```
key         : 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff
              00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff
```

- 128 비트 초기 벡터(IV)

```
IV          : 0f 1e 2d 3c 4b 5a 69 78 87 96 a5 b4 c3 d2 e1 f0
```

- 평문 10 블록

```
plaintext   : 11 11 11 11 aa aa aa aa 11 11 11 11 bb bb bb bb
            : 11 11 11 11 cc cc cc cc 11 11 11 11 dd dd dd dd
            : 22 22 22 22 aa aa aa aa 22 22 22 22 bb bb bb bb
            : 22 22 22 22 cc cc cc cc 22 22 22 22 dd dd dd dd
            : 33 33 33 33 aa aa aa aa 33 33 33 33 bb bb bb bb
            : 33 33 33 33 cc cc cc cc 33 33 33 33 dd dd dd dd
            : 44 44 44 44 aa aa aa aa 44 44 44 44 bb bb bb bb
            : 44 44 44 44 cc cc cc cc 44 44 44 44 dd dd dd dd
            : 55 55 55 55 aa aa aa aa 55 55 55 55 bb bb bb bb
            : 55 55 55 55 cc cc cc cc 55 55 55 55 dd dd dd dd
```

이제 각 운영 모드에 의한 위의 평문의 암호화 결과는 다음과 같다. (Counter 모드의 경우 카운터는 0으로 출발하여 1씩 증가시켰다.)

```
ECB mode    : 58 a8 75 e6 04 4a d7 ff fa 4f 58 42 0f 7f 44 2d
            : 8e 19 10 16 f2 8e 79 ae fc 01 e2 04 77 32 80 d7
            : 01 8e 5f 7a 93 8e c3 07 11 71 99 53 ba e8 65 42
```

```
            : cd 7e bc 75 24 74 c1 a5 f6 ea aa ce 2a 7e 29 46
            : 2e e7 df a5 af db 84 17 7e ad 95 cc d4 b4 bb 6e
            : 1e d1 7b 95 34 cf f0 a5 fc 29 41 42 9c fe e2 ee
            : 49 c7 ad be b7 e9 d1 b0 d2 a8 53 1d 94 20 79 59
            : 6a 27 ed 79 f5 b1 dd 13 ec d6 04 b0 7a 48 88 5a
            : 3a fa 06 27 a0 e4 e6 0a 3c 70 3a f2 92 f1 ba a7
            : 7b 70 2f 16 c5 4a a7 4b c7 27 ea 95 c7 46 8b 00

CBC mode    : 52 3a 8a 80 6a e6 21 f1 55 fd d2 8d bc 34 e1 ab
            : 7b 9b 42 43 2a d8 b2 ef b9 6e 23 b1 3f 0a 6e 52
            : f3 61 85 d5 0a d0 02 c5 f6 01 be e5 49 3f 11 8b
            : 24 3e e2 e3 13 64 2b ff c3 90 2e 7b 2e fd 9a 12
            : fa 68 2e dd 2d 23 c8 b9 c5 f0 43 c1 8b 17 c1 ec
            : 4b 58 67 91 82 70 fb ec 10 27 c1 9e d6 af 83 3d
            : a5 d6 20 99 46 68 ca 22 f5 99 79 1d 29 2d d6 27
            : 3b 29 59 08 2a af b7 a9 96 16 7c ce 1e ec 5f 0c
            : fd 15 f6 10 d8 7e 2d da 9b a6 8c e1 26 0c a5 4b
            : 22 24 91 41 83 74 29 4e 79 09 b1 e8 55 1c d8 de

CFB-128 mode : 26 83 47 05 b0 f2 c0 e2 58 8d 4a 7f 09 00 96 35 f2 8b
b9 3d 8c 31 f8 70 ec 1e 0b db 08 2b 66 fa 40 2d d9 c2 02 be 30 0c 45
17 d1 96 b1 4d 4c e1 1d ce 97 f7 aa ba 54 34 1b 0d 87 2c c9 b6 37 53
a3 e8 55 6a 14 be 6f 7b 3e 27 e3 cf c3 9c af 80 f2 a3 55 aa 50 dc 83
c0 9c 7b 11 82 86 94 f8 e4 aa 72 6c 52 89 76 b5 3f 2c 87 7f 49 91 a3
a8 d2 8a db 63 bd 75 18 46 ff b2 35 02 65 e1 79 d4 99 07 53 ae 84 85
ff 9b 41 33 dd ad 58 75 b8 4a 90 cb cf a6 2a 04 5d 72 6d f7 1b 6b da
0e ec a0 be

CFB-64 mode  : 26 83 47 05 b0 f2 c0 e2 66 40 41 f4 d5 e7 40 3e 75 4a
e0 0b 4e ef ec 8d bf d1 ad 60 4a 65 83 f3 40 19 6c 32 c8 d1 aa 75 a1
dc 15 af 91 bc 01 52 ce ce da fb 51 37 89 74 ef 1f 0e bd f6 4d 96 96
23 ac 69 fb 33 b2 42 22 0b 4e 23 8f 59 2c 73 ca 1f cf f5 fe 31 8c 2e
10 63 e8 cb 52 17 12 6d d8 45 c6 ce 1b ee e4 7f 34 97 6d 1e 91 1b d2
99 f9 08 58 0d b2 14 0e 9c 4e 47 b2 2b 2d 49 a2 f9 ca 4b cb 04 e2 60
71 d2 e7 bb 12 c2 c0 ef da cd d6 31 56 ef 9c 59 dc 3e b7 35 55 8e bd
15 66 50 7b

CFB-16 mode  : 26 83 f2 73 06 4e 60 31 a4 54 b2 e0 b3 1b f0 40 4d f9
d3 3d c4 a8 45 3a 06 91 ad 11 cc 6c 06 37 c8 aa e1 31 ad 69 90 13 3b
43 3c fa 03 7b 13 ad 09 12 68 cc 13 60 21 68 ca 3d 45 e0 3c 10 35 17
ba 50 13 e3 c9 82 31 0a f1 7a 4f f7 ff ae 3d 28 fd db 89 52 14 22 1c
e1 4f ee 1c 52 a7 d8 56 4e 19 25 4e 44 c4 4f 91 ff 0c 54 3c 4c 33 f3
77 be 65 15 ea db 32 e9 68 5d ec d0 20 87 d8 12 d7 64 20 ea 9a fd 41
cc 49 4a 40 19 7c cc c8 2f 18 93 de 52 97 d5 49 bb fa 4a af b6 de a6
c0 f3 52 a6
```

```
CFB-8 mode   : 26 ba a3 36 51 e1 f6 64 34 fe c8 8e f2 7f d2 b9 a7 9e
24 6d d8 9a 3f fa 00 e8 bd b3 71 55 43 3e 6c 24 bd 0b 87 d9 a8 5b aa
9f 48 5c cb 98 4f 5e c2 4d 6a 3e f5 e3 c8 13 96 17 7f 03 9c f5 80 df
db 55 d6 e1 c4 7a 28 92 1d fe 36 9e 12 fd 35 7b 28 9a d3 a5 54 4e 1c
1b d6 16 d4 54 db 9c 5f 91 f6 03 37 3f 29 d5 b2 ed 1b 4b 51 de 80 f2
85 37 bb d4 3d 5e 3b 5d d0 71 dc 91 15 3c bb e7 32 df c3 25 82 1b 06
ed 8a ca ae 65 6d cf 2d a9 f1 3e 4f 29 db 67 14 76 f1 e6 44 ff 06 d9
b6 7d 6b d4

OFB-128 mode : 26 83 47 05 b0 f2 c0 e2 58 8d 4a 7f 09 00 96 35 84 c2
56 81 5c 42 92 b5 9f 8d 3f 96 6a 75 b5 23 45 b4 f5 f9 8c 78 5d 3f 36
8a 8d 5f f8 9b 7f 95 0c ea b3 cd 63 77 3c 26 21 d6 52 b8 ef 98 b4 19
6a fb 2c 2b 30 49 6b c5 b7 d9 e7 f9 08 4f 9d 85 5f 63 a5 11 75 1c 89
09 e7 a6 de ad be 0a 67 a4 fb 89 38 3c a5 d2 09 c6 f6 6f 79 3f c4 71
19 5c 47 6f b9 c1 ea b2 ac 91 e6 80 e4 54 b4 f3 ed 9a 67 fb 52 f0 9c
29 b9 65 b2 3c fa 6f 3f 6b bb 2a 86 c6 cd ba a2 85 7b f2 48 6f 54 32
31 89 2a 52

OFB-64 mode  : 26 83 47 05 b0 f2 c0 e2 84 c2 56 81 2b 35 e5 c2 76 87
c6 ca ea 1e 3b 59 3f d9 80 fe 72 66 2d 37 7b ea 3d 3a 30 49 6b c5 4e
72 b4 00 02 6b fe 7e 9d ef 5e 5a c3 b4 6f a0 21 09 df a7 fb a3 bd 80
01 9d 34 96 9c 29 b9 65 e0 a0 ab dc d5 f2 0c 85 9f 2d 4c 2f 47 38 99
48 66 11 fe b4 63 1f b0 66 12 ab 3f 9d d4 88 47 7b 4f 27 7c d6 08 30
c9 2b 02 df d4 36 e1 90 5d 2a 7c e6 9d 3d e7 7f d7 96 6e 9a 7e 6c e9
21 69 30 0b ff ec c8 53 55 bb a7 e0 55 5a 2b 61 f3 33 e4 05 47 0b bd
76 a2 5a f3

OFB-16 mode  : 26 83 84 c2 cd 3c 84 62 48 d9 7d 41 04 76 b8 90 23 bf
c2 82 60 d2 99 ee 47 fe 1a 72 9b 46 e5 7f 19 ed 7c 88 1f aa fa b8 ca
e3 76 a6 ab ef c3 75 cf fa 87 10 74 cb 2b 3f a3 0e ab 9c cc 3e a8 75
eb 32 a8 f5 7f e3 12 4d 11 d5 69 57 ab d3 09 40 05 3d 8f 1d 5e 7f 57
10 06 e4 50 dd 33 7b 91 76 58 38 23 d5 65 33 8b 7d 6e d6 cc 47 88 90
06 84 d1 5f ff 4d 3c f0 89 a7 8f ea 92 ec ff 72 75 26 89 3e da 2a f3
62 82 ca cb 7c eb ea 4f ec 96 3f a4 fa 84 4c 21 59 d4 00 37 dc 66 3d
51 78 a5 ca

OFB-8 mode   : 26 84 76 3f f3 c6 15 a9 23 c2 bd 44 ed b0 fd 83 2a 4f
a4 41 24 98 dc b4 fc b4 a9 f6 5c 54 cc a8 fa b9 f7 9a 88 f0 ba 18 14
9e b0 b9 8e d8 55 f7 3e 45 ed 03 e6 44 ff 71 b7 99 d2 67 16 0b ff 75
ef bc 6a 1b 34 14 5e 87 c2 e2 de 2b d9 88 37 c3 c4 6c 96 ce 64 2a 11
b6 71 56 af af 61 9d ec 2c 3a c4 42 40 a5 2e 1c e5 6c 83 c3 23 d8 46
07 8f 04 ff 4f a7 fa 51 09 db 42 8c b6 2e 76 c3 90 24 1d c5 eb 53 3e
57 0d 6d 84 b9 ba 7b 90 11 c1 94 6f 66 60 f9 81 00 27 b8 ac 3a 92 2b
3e bf a4 c7

CTR mode   : 30 02 6c 32 96 66 14 17 21 17 8b 99 c0 a1 f1 b2
```

```
: f0 69 40 25 3f 7b 30 89 e2 a3 0e a8 6a a3 c8 8f
: 59 40 f0 5a d7 ee 41 d7 13 47 bb 72 61 e3 48 f1
: 83 60 47 3f df 7d 4e 77 23 bf fb 44 11 cc 13 f6
: cd d8 9f 3b c7 b9 c7 68 14 50 22 c7 a7 4f 14 d7
: c3 05 cd 01 2a 10 f1 60 50 c2 3f 1a e5 c2 3f 45
: 99 8d 13 fb aa 04 1e 51 61 95 77 e0 77 27 64 89
: 6a 5d 45 16 d8 ff ce b3 bf 7e 05 f6 13 ed d9 a6
: 0c dc ed af f9 cf ca f4 e0 0d 44 5a 54 33 4f 73
: ab 2c ad 94 4e 51 d2 66 54 8e 61 c6 eb 0a a1 cd
```