

#####

Block Cipher Modes of Operation

Cipher FeedBack (CFB)

IV is

00010203 04050607 08090A0B 0C0D0E0F

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A
AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
30C81C46 A35CE411 E5FBC119 1A0A52EF
F69F2445 DF4F9B17 AD2B417B E66C3710

#####

CFB-AES128 (Encryption)

Segment Length = 128

Key is

2B7E1516 28AED2A6 ABF71588 09CF4F3C

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A
AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
30C81C46 A35CE411 E5FBC119 1A0A52EF
F69F2445 DF4F9B17 AD2B417B E66C3710

Ciphertext is

3B3FD92E B72DAD20 333449F8 E83CFB4A
C8A64537 A0B3A93F CDE3CDAD 9F1CE58B
26751F67 A3CBB140 B1808CF1 87A4F4DF
C04B0535 7C5D1C0E EAC4C66F 9FF7F2E6

=====

CFB-AES128 (Decryption)

Segment Length = 128

Key is

2B7E1516 28AED2A6 ABF71588 09CF4F3C

Ciphertext is

3B3FD92E B72DAD20 333449F8 E83CFB4A
C8A64537 A0B3A93F CDE3CDAD 9F1CE58B
26751F67 A3CBB140 B1808CF1 87A4F4DF
C04B0535 7C5D1C0E EAC4C66F 9FF7F2E6

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A
AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
30C81C46 A35CE411 E5FBC119 1A0A52EF
F69F2445 DF4F9B17 AD2B417B E66C3710

CFB-AES128 (Encryption)

Segment Length = 8

Key is

2B7E1516 28AED2A6 ABF71588 09CF4F3C

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A

Ciphertext is

3B79424C 9C0DD436 BACE9E0E D4586A4F

CFB-AES128 (Decryption)

Segment Length = 8

Key is

2B7E1516 28AED2A6 ABF71588 09CF4F3C

Ciphertext is
3B79424C 9C0DD436 BACE9E0E D4586A4F

Plaintext is
6BC1BEE2 2E409F96 E93D7E11 7393172A

=====

CFB-AES128 (Encryption)

Segment Length = 1

Key is
2B7E1516 28AED2A6 ABF71588 09CF4F3C

Plaintext is
6BC1

Ciphertext is
69C8

=====

CFB-AES128 (Decryption)

Segment Length = 1

Key is
2B7E1516 28AED2A6 ABF71588 09CF4F3C

Ciphertext is
69C8

Plaintext is
6A59

=====

CFB-AES192 (Encryption)

Segment Length = 128

Key is

8E73B0F7 DA0E6452 C810F32B 809079E5
62F8EAD2 522C6B7B

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A
AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
30C81C46 A35CE411 E5FBC119 1A0A52EF
F69F2445 DF4F9B17 AD2B417B E66C3710

Ciphertext is

CDC80D6F DDF18CAB 34C25909 C99A4174
67CE7F7F 81173621 961A2B70 171D3D7A
2E1E8A1D D59B88B1 C8E60FED 1EFAC4C9
C05F9F9C A9834FA0 42AE8FBA 584B09FF

CFB-AES192 (Decryption)

Segment Length = 128

Key is

8E73B0F7 DA0E6452 C810F32B 809079E5
62F8EAD2 522C6B7B

Ciphertext is

CDC80D6F DDF18CAB 34C25909 C99A4174
67CE7F7F 81173621 961A2B70 171D3D7A
2E1E8A1D D59B88B1 C8E60FED 1EFAC4C9
C05F9F9C A9834FA0 42AE8FBA 584B09FF

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A
AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51

30C81C46 A35CE411 E5FBC119 1A0A52EF
F69F2445 DF4F9B17 AD2B417B E66C3710

=====
CFB-AES192 (Encryption)

Segment Length = 8

Key is

8E73B0F7 DA0E6452 C810F32B 809079E5
62F8EAD2 522C6B7B

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A

Ciphertext is

CDA2521E F0A905CA 44CD057C BF0D47A0

=====
CFB-AES192 (Decryption)

Segment Length = 8

Key is

8E73B0F7 DA0E6452 C810F32B 809079E5
62F8EAD2 522C6B7B

Ciphertext is

CDA2521E F0A905CA 44CD057C BF0D47A0

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A

=====
CFB-AES192 (Encryption)

Segment Length = 1

Key is

8E73B0F7 DA0E6452 C810F32B 809079E5
62F8EAD2 522C6B7B

Plaintext is

6BC1

Ciphertext is

9776

=====
CFB-AES192 (Decryption)

Segment Length = 1

Key is

8E73B0F7 DA0E6452 C810F32B 809079E5
62F8EAD2 522C6B7B

Ciphertext is

9776

Plaintext is

6EE0

=====
CFB-AES256 (Encryption)

Segment Length = 128

Key is

603DEB10 15CA71BE 2B73AEF0 857D7781
1F352C07 3B6108D7 2D9810A3 0914DFF4

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A
AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
30C81C46 A35CE411 E5FBC119 1A0A52EF
F69F2445 DF4F9B17 AD2B417B E66C3710

Ciphertext is

DC7E84BF DA79164B 7ECD8486 985D3860
39FFED14 3B28B1C8 32113C63 31E5407B
DF101324 15E54B92 A13ED0A8 267AE2F9
75A38574 1AB9CEF8 2031623D 55B1E471

=====
CFB-AES256 (Decryption)

Segment Length = 128

Key is

603DEB10 15CA71BE 2B73AEF0 857D7781
1F352C07 3B6108D7 2D9810A3 0914DFF4

Ciphertext is

DC7E84BF DA79164B 7ECD8486 985D3860
39FFED14 3B28B1C8 32113C63 31E5407B
DF101324 15E54B92 A13ED0A8 267AE2F9
75A38574 1AB9CEF8 2031623D 55B1E471

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A
AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
30C81C46 A35CE411 E5FBC119 1A0A52EF
F69F2445 DF4F9B17 AD2B417B E66C3710

=====
CFB-AES256 (Encryption)

Segment Length = 8

Key is

603DEB10 15CA71BE 2B73AEF0 857D7781
1F352C07 3B6108D7 2D9810A3 0914DFF4

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A

Ciphertext is

DC1F1A85 20A64DB5 5FCC8AC5 54844E88

=====
CFB-AES256 (Decryption)

Segment Length = 8

Key is

603DEB10 15CA71BE 2B73AEF0 857D7781
1F352C07 3B6108D7 2D9810A3 0914DFF4

Ciphertext is

DC1F1A85 20A64DB5 5FCC8AC5 54844E88

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A

=====
CFB-AES256 (Encryption)

Segment Length = 1

Key is

603DEB10 15CA71BE 2B73AEF0 857D7781
1F352C07 3B6108D7 2D9810A3 0914DFF4

Plaintext is

6BC1

Ciphertext is
93D0

=====

CFB-AES256 (Decryption)

Segment Length = 1

Key is
603DEB10 15CA71BE 2B73AEF0 857D7781
1F352C07 3B6108D7 2D9810A3 0914DFF4

Ciphertext is
93D0

Plaintext is
69F4
