

#####

Block Cipher Modes of Operation

Output FeedBack (OFB)

IV is

00010203 04050607 08090A0B 0C0D0E0F

Plaintext is

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

#####

OFB-AES128 (Encryption)

Key is

2B7E1516 28AED2A6 ABF71588 09CF4F3C

Plaintext is

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

Block #1

InputBlock 00010203 04050607 08090A0B 0C0D0E0F
OutputBlock 50FE67CC 996D32B6 DA0937E9 9BAFEC60
Text-In 6BC1BEE2 2E409F96 E93D7E11 7393172A
Text-Out 3B3FD92E B72DAD20 333449F8 E83CFB4A

Block #2

InputBlock 50FE67CC 996D32B6 DA0937E9 9BAFEC60
OutputBlock D9A4DADA 0892239F 6B8B3D76 80E15674
Text-In AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
Text-Out 7789508D 16918F03 F53C52DA C54ED825

Block #3

InputBlock D9A4DADA 0892239F 6B8B3D76 80E15674
OutputBlock A7881958 3F0308E7 A6BF36B1 386ABF23
Text-In 30C81C46 A35CE411 E5FBC119 1A0A52EF
Text-Out 9740051E 9C5FECF6 4344F7A8 2260EDCC

Block #4

InputBlock A7881958 3F0308E7 A6BF36B1 386ABF23

OutputBlock	C6D3416D	29165C6F	CB8E51A2	27BA994E
Text-In	F69F2445	DF4F9B17	AD2B417B	E66C3710
Text-Out	304C6528	F659C778	66A510D9	C1D6AE5E

Ciphertext is

3B3FD92E	B72DAD20	333449F8	E83CFB4A
7789508D	16918F03	F53C52DA	C54ED825
9740051E	9C5FECF6	4344F7A8	2260EDCC
304C6528	F659C778	66A510D9	C1D6AE5E

=====

OFB-AES128 (Decryption)

Key is

2B7E1516 28AED2A6 ABF71588 09CF4F3C

Ciphertext is

3B3FD92E	B72DAD20	333449F8	E83CFB4A
7789508D	16918F03	F53C52DA	C54ED825
9740051E	9C5FECF6	4344F7A8	2260EDCC
304C6528	F659C778	66A510D9	C1D6AE5E

Block #1

InputBlock	00010203	04050607	08090A0B	0C0D0E0F
OutputBlock	50FE67CC	996D32B6	DA0937E9	9BAFEC60
Text-In	3B3FD92E	B72DAD20	333449F8	E83CFB4A
Text-Out	6BC1BEE2	2E409F96	E93D7E11	7393172A

Block #2

InputBlock	50FE67CC	996D32B6	DA0937E9	9BAFEC60
OutputBlock	D9A4DADA	0892239F	6B8B3D76	80E15674
Text-In	7789508D	16918F03	F53C52DA	C54ED825
Text-Out	AE2D8A57	1E03AC9C	9EB76FAC	45AF8E51

Block #3

InputBlock	D9A4DADA	0892239F	6B8B3D76	80E15674
OutputBlock	A7881958	3F0308E7	A6BF36B1	386ABF23
Text-In	9740051E	9C5FECF6	4344F7A8	2260EDCC
Text-Out	30C81C46	A35CE411	E5FBC119	1A0A52EF

Block #4

InputBlock	A7881958	3F0308E7	A6BF36B1	386ABF23
OutputBlock	C6D3416D	29165C6F	CB8E51A2	27BA994E
Text-In	304C6528	F659C778	66A510D9	C1D6AE5E
Text-Out	F69F2445	DF4F9B17	AD2B417B	E66C3710

Plaintext is

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

=====

OFB-AES192 (Encryption)

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

Block #1

InputBlock	00010203	04050607	08090A0B	0C0D0E0F
OutputBlock	A609B38D	F3B1133D	DDFF2718	BA09565E
Text-In	6BC1BEE2	2E409F96	E93D7E11	7393172A
Text-Out	CDC80D6F	DDF18CAB	34C25909	C99A4174

Block #2

InputBlock	A609B38D	F3B1133D	DDFF2718	BA09565E
OutputBlock	52EF01DA	52602FE0	975F78AC	84BF8A50
Text-In	AE2D8A57	1E03AC9C	9EB76FAC	45AF8E51
Text-Out	FCC28B8D	4C63837C	09E81700	C1100401

Block #3

InputBlock	52EF01DA	52602FE0	975F78AC	84BF8A50
OutputBlock	BD5286AC	63AABD7E	B067AC54	B553F71D
Text-In	30C81C46	A35CE411	E5FBC119	1A0A52EF
Text-Out	8D9A9AEA	C0F6596F	559C6D4D	AF59A5F2

Block #4

InputBlock	BD5286AC	63AABD7E	B067AC54	B553F71D
OutputBlock	9B00044D	8885F729	31871330	3FC0FE3A
Text-In	F69F2445	DF4F9B17	AD2B417B	E66C3710
Text-Out	6D9F2008	57CA6C3E	9CAC524B	D9ACC92A

Ciphertext is

CDC80D6F DDF18CAB 34C25909 C99A4174
FCC28B8D 4C63837C 09E81700 C1100401

8D9A9AEA C0F6596F 559C6D4D AF59A5F2
6D9F2008 57CA6C3E 9CAC524B D9ACC92A

=====

OFB-AES192 (Decryption)

Key is

8E73B0F7 DA0E6452 C810F32B 809079E5
62F8EAD2 522C6B7B

Ciphertext is

CDC80D6F DDF18CAB 34C25909 C99A4174
FCC28B8D 4C63837C 09E81700 C1100401
8D9A9AEA C0F6596F 559C6D4D AF59A5F2
6D9F2008 57CA6C3E 9CAC524B D9ACC92A

Block #1

InputBlock	00010203	04050607	08090A0B	0C0D0E0F
OutputBlock	A609B38D	F3B1133D	DDFF2718	BA09565E
Text-In	CDC80D6F	DDF18CAB	34C25909	C99A4174
Text-Out	6BC1BEE2	2E409F96	E93D7E11	7393172A

Block #2

InputBlock	A609B38D	F3B1133D	DDFF2718	BA09565E
OutputBlock	52EF01DA	52602FE0	975F78AC	84BF8A50
Text-In	FCC28B8D	4C63837C	09E81700	C1100401
Text-Out	AE2D8A57	1E03AC9C	9EB76FAC	45AF8E51

Block #3

InputBlock	52EF01DA	52602FE0	975F78AC	84BF8A50
OutputBlock	BD5286AC	63AABD7E	B067AC54	B553F71D
Text-In	8D9A9AEA	C0F6596F	559C6D4D	AF59A5F2
Text-Out	30C81C46	A35CE411	E5FBC119	1A0A52EF

Block #4

InputBlock	BD5286AC	63AABD7E	B067AC54	B553F71D
OutputBlock	9B00044D	8885F729	31871330	3FC0FE3A
Text-In	6D9F2008	57CA6C3E	9CAC524B	D9ACC92A
Text-Out	F69F2445	DF4F9B17	AD2B417B	E66C3710

Plaintext is

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

=====

OFB-AES256 (Encryption)

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

Block #1

InputBlock	00010203	04050607	08090A0B	0C0D0E0F
OutputBlock	B7BF3A5D	F43989DD	97F0FA97	EBCE2F4A
Text-In	6BC1BEE2	2E409F96	E93D7E11	7393172A
Text-Out	DC7E84BF	DA79164B	7ECD8486	985D3860

Block #2

InputBlock	B7BF3A5D	F43989DD	97F0FA97	EBCE2F4A
OutputBlock	E1C65630	5ED1A7A6	56380574	6FE03EDC
Text-In	AE2D8A57	1E03AC9C	9EB76FAC	45AF8E51
Text-Out	4FEBDC67	40D20B3A	C88F6AD8	2A4FB08D

Block #3

InputBlock	E1C65630	5ED1A7A6	56380574	6FE03EDC
OutputBlock	41635BE6	25B48AFC	1666DD42	A09D96E7
Text-In	30C81C46	A35CE411	E5FBC119	1A0A52EF
Text-Out	71AB47A0	86E86EED	F39D1C5B	BA97C408

Block #4

InputBlock	41635BE6	25B48AFC	1666DD42	A09D96E7
OutputBlock	F7B93058	B8BCE0FF	FEA41BF0	012CD394
Text-In	F69F2445	DF4F9B17	AD2B417B	E66C3710
Text-Out	0126141D	67F37BE8	538F5A8B	E740E484

Ciphertext is

DC7E84BF DA79164B 7ECD8486 985D3860
4FEBDC67 40D20B3A C88F6AD8 2A4FB08D
71AB47A0 86E86EED F39D1C5B BA97C408
0126141D 67F37BE8 538F5A8B E740E484

=====

OFB-AES256 (Decryption)

Key is

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

Ciphertext is

DC7E84BF DA79164B 7ECD8486 985D3860
4FEBDC67 40D20B3A C88F6AD8 2A4FB08D
71AB47A0 86E86EED F39D1C5B BA97C408
0126141D 67F37BE8 538F5A8B E740E484

Block #1

InputBlock	00010203	04050607	08090A0B	0C0D0E0F
OutputBlock	B7BF3A5D	F43989DD	97F0FA97	EBCE2F4A
Text-In	DC7E84BF	DA79164B	7ECD8486	985D3860
Text-Out	6BC1BEE2	2E409F96	E93D7E11	7393172A

Block #2

InputBlock	B7BF3A5D	F43989DD	97F0FA97	EBCE2F4A
OutputBlock	E1C65630	5ED1A7A6	56380574	6FE03EDC
Text-In	4FEBDC67	40D20B3A	C88F6AD8	2A4FB08D
Text-Out	AE2D8A57	1E03AC9C	9EB76FAC	45AF8E51

Block #3

InputBlock	E1C65630	5ED1A7A6	56380574	6FE03EDC
OutputBlock	41635BE6	25B48AFC	1666DD42	A09D96E7
Text-In	71AB47A0	86E86EED	F39D1C5B	BA97C408
Text-Out	30C81C46	A35CE411	E5FBC119	1A0A52EF

Block #4

InputBlock	41635BE6	25B48AFC	1666DD42	A09D96E7
OutputBlock	F7B93058	B8BCE0FF	FEA41BF0	012CD394
Text-In	0126141D	67F37BE8	538F5A8B	E740E484
Text-Out	F69F2445	DF4F9B17	AD2B417B	E66C3710

Plaintext is

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