

#####

Block Cipher Modes of Operation

Electronic Codebook (ECB)

#####

ECB-TDES (Encryption)

Key1 is

01234567 89ABCDEF

Key2 is

23456789 ABCDEF01

Key3 is

456789AB CDEF0123

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A

AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51

Block #1

Blockin 6BC1BEE2 2E409F96

Blockout 714772F3 39841D34

Block #2

Blockin E93D7E11 7393172A

Blockout 267FCC4B D2949CC3

Block #3

Blockin AE2D8A57 1E03AC9C

Blockout EE11C22A 576A3038

Block #4

Blockin 9EB76FAC 45AF8E51

Blockout 76183F99 C0B6DE87

Ciphertext is

714772F3 39841D34 267FCC4B D2949CC3

EE11C22A 576A3038 76183F99 C0B6DE87

=====

ECB-TDES (Decryption)

Key1 is
01234567 89ABCDEF
Key2 is
23456789 ABCDEF01
Key3 is
456789AB CDEF0123

Ciphertext is
714772F3 39841D34 267FCC4B D2949CC3
EE11C22A 576A3038 76183F99 C0B6DE87

Block #1
Blockin 714772F3 39841D34
Blockout 6BC1BEE2 2E409F96

Block #2
Blockin 267FCC4B D2949CC3
Blockout E93D7E11 7393172A

Block #3
Blockin EE11C22A 576A3038
Blockout AE2D8A57 1E03AC9C

Block #4
Blockin 76183F99 C0B6DE87
Blockout 9EB76FAC 45AF8E51

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

#####

Block Cipher Modes of Operation

Electronic Codebook (ECB)

#####

ECB-TDES (Encryption)

Key1 is
01234567 89ABCDEF
Key2 is
23456789 ABCDEF01
Key3 is
01234567 89ABCDEF
Plaintext is
6BC1BEE2 2E409F96 E93D7E11 7393172A
AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51

Block #1
Blockin 6BC1BEE2 2E409F96
Blockout 06EDE3D8 2884090A

Block #2
Blockin E93D7E11 7393172A
Blockout FF322C19 F0518486

Block #3
Blockin AE2D8A57 1E03AC9C
Blockout 73057697 2A666E58

Block #4
Blockin 9EB76FAC 45AF8E51
Blockout B6C88CF1 07340D3D

Ciphertext is
06EDE3D8 2884090A FF322C19 F0518486
73057697 2A666E58 B6C88CF1 07340D3D

=====

ECB-TDES (Decryption)

Key1 is
01234567 89ABCDEF
Key2 is
23456789 ABCDEF01
Key3 is
01234567 89ABCDEF
Ciphertext is
06EDE3D8 2884090A FF322C19 F0518486
73057697 2A666E58 B6C88CF1 07340D3D

Block #1
Blockin 06EDE3D8 2884090A
Blockout 6BC1BEE2 2E409F96

Block #2
Blockin FF322C19 F0518486
Blockout E93D7E11 7393172A

Block #3
Blockin 73057697 2A666E58
Blockout AE2D8A57 1E03AC9C

Block #4
Blockin B6C88CF1 07340D3D
Blockout 9EB76FAC 45AF8E51

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

#####

Block Cipher Modes of Operation

Cipher Block Chaining (CBC)

#####

CBC-TDES (Encryption)

Key1 is

01234567 89ABCDEF

Key2 is

23456789 ABCDEF01

Key3 is

456789AB CDEF0123

IV is

F69F2445 DF4F9B17

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A

AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51

Block #1

Plaintext 6BC1BEE2 2E409F96

InputBlock 9D5E9AA7 F10F0481

OutputBlock 2079C3D5 3AA763E1

Ciphertext 2079C3D5 3AA763E1

Block #2

Plaintext E93D7E11 7393172A

InputBlock C944BDC4 493474CB

OutputBlock 93B79E25 69AB5262

Ciphertext 93B79E25 69AB5262

Block #3

Plaintext AE2D8A57 1E03AC9C

InputBlock 3D9A1472 77A8FEFE

OutputBlock 51657048 1F25B50F

Ciphertext 51657048 1F25B50F

Block #4

Plaintext 9EB76FAC 45AF8E51

InputBlock CFD21FE4 5A8A3B5E

OutputBlock 73C0BDA8 5C8E0DA7

Ciphertext 73C0BDA8 5C8E0DA7

Ciphertext is
2079C3D5 3AA763E1 93B79E25 69AB5262
51657048 1F25B50F 73C0BDA8 5C8E0DA7

=====
CBC-TDES (Decryption)

Key1 is
01234567 89ABCDEF

Key2 is
23456789 ABCDEF01

Key3 is
456789AB CDEF0123

IV is
F69F2445 DF4F9B17

Ciphertext is
2079C3D5 3AA763E1 93B79E25 69AB5262
51657048 1F25B50F 73C0BDA8 5C8E0DA7

Block #1
Ciphertext 2079C3D5 3AA763E1
InputBlock 2079C3D5 3AA763E1
OutputBlock 9D5E9AA7 F10F0481
Plaintext 6BC1BEE2 2E409F96

Block #2
Ciphertext 93B79E25 69AB5262
InputBlock 93B79E25 69AB5262
OutputBlock C944BDC4 493474CB
Plaintext E93D7E11 7393172A

Block #3
Ciphertext 51657048 1F25B50F
InputBlock 51657048 1F25B50F
OutputBlock 3D9A1472 77A8FEFE
Plaintext AE2D8A57 1E03AC9C

Block #4
Ciphertext 73C0BDA8 5C8E0DA7
InputBlock 73C0BDA8 5C8E0DA7
OutputBlock CFD21FE4 5A8A3B5E
Plaintext 9EB76FAC 45AF8E51

Plaintext is

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

#####

Block Cipher Modes of Operation

Cipher Block Chaining (CBC)

#####

CBC-TDES (Encryption)

Key1 is

01234567 89ABCDEF

Key2 is

23456789 ABCDEF01

Key3 is

01234567 89ABCDEF

IV is

F69F2445 DF4F9B17

Plaintext is

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

Block #1

Plaintext	6BC1BEE2 2E409F96
InputBlock	9D5E9AA7 F10F0481
OutputBlock	7401CE1E AB6D003C
Ciphertext	7401CE1E AB6D003C

Block #2

Plaintext	E93D7E11 7393172A
InputBlock	9D3CB00F D8FE1716
OutputBlock	AFF84BF4 7B36CC21
Ciphertext	AFF84BF4 7B36CC21

Block #3

Plaintext	AE2D8A57 1E03AC9C
InputBlock	01D5C1A3 653560BD

OutputBlock 54F0238F 9FFECD8F
Ciphertext 54F0238F 9FFECD8F

Block #4

Plaintext 9EB76FAC 45AF8E51
InputBlock CA474C23 DA5143DE
OutputBlock 6ACF1183 92B45581
Ciphertext 6ACF1183 92B45581

Ciphertext is

7401CE1E AB6D003C AFF84BF4 7B36CC21
54F0238F 9FFECD8F 6ACF1183 92B45581

=====
CBC-TDES (Decryption)

Key1 is

01234567 89ABCDEF

Key2 is

23456789 ABCDEF01

Key3 is

01234567 89ABCDEF

IV is

F69F2445 DF4F9B17

Ciphertext is

7401CE1E AB6D003C AFF84BF4 7B36CC21
54F0238F 9FFECD8F 6ACF1183 92B45581

Block #1

Ciphertext 7401CE1E AB6D003C
InputBlock 7401CE1E AB6D003C
OutputBlock 9D5E9AA7 F10F0481
Plaintext 6BC1BEE2 2E409F96

Block #2

Ciphertext AFF84BF4 7B36CC21
InputBlock AFF84BF4 7B36CC21
OutputBlock 9D3CB00F D8FE1716
Plaintext E93D7E11 7393172A

Block #3

Ciphertext 54F0238F 9FFECD8F
InputBlock 54F0238F 9FFECD8F

OutputBlock 01D5C1A3 653560BD
Plaintext AE2D8A57 1E03AC9C

Block #4

Ciphertext 6ACF1183 92B45581
InputBlock 6ACF1183 92B45581
OutputBlock CA474C23 DA5143DE
Plaintext 9EB76FAC 45AF8E51

Plaintext is

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

#####

Block Cipher Modes of Operation

Cipher Feedback (CFB)

#####

CFB-TDES (Encryption)

Key1 is

01234567 89ABCDEF

Key2 is

23456789 ABCDEF01

Key3 is

456789AB CDEF0123

IV is

F69F2445 DF4F9B17

Plaintext is

6B

Segment Length = 1

Segment #1

InputBlock F69F2445 DF4F9B17

OutputBlock 6C4A09AC 778EE140

Plaintext 0

Ciphertext 0

Segment #2

InputBlock ED3E488B BE9F362E

OutputBlock 2FBAD050 3CEB5412

Plaintext 1

Ciphertext 1

Segment #3

InputBlock DA7C9117 7D3E6C5D

OutputBlock BE9A7EB4 DA9131E1

Plaintext 1

Ciphertext 0

Segment #4

InputBlock B4F9222E FA7CD8BA

OutputBlock 986D65A9 8F72D62F

Plaintext 0

Ciphertext 1

Segment #5

InputBlock 69F2445D F4F9B175

OutputBlock 6D87A6C5 42C50EB6

```

    Plaintext      1
    Ciphertext     1
Segment #6
    InputBlock    D3E488BB E9F362EB
    OutputBlock   EDD759BC 745036D7
    Plaintext     0
    Ciphertext    1
Segment #7
    InputBlock    A7C91177 D3E6C5D7
    OutputBlock   DE45381C F86ADC5F
    Plaintext     1
    Ciphertext    0
Segment #8
    InputBlock    4F9222EF A7CD8BAE
    OutputBlock   A41E3F9F 5329A6F5
    Plaintext     1
    Ciphertext    0

```

Ciphertext is
5C

=====

CFB-TDES (Decryption)

Key1 is
01234567 89ABCDEF

Key2 is
23456789 ABCDEF01

Key3 is
456789AB CDEF0123

IV is
F69F2445 DF4F9B17

Ciphertext is
5C

Segment Length = 1

```

Segment #1
    InputBlock    F69F2445 DF4F9B17
    OutputBlock   6C4A09AC 778EE140
    Ciphertext    0
    Plaintext     0
Segment #2
    InputBlock    ED3E488B BE9F362E
    OutputBlock   2FBAD050 3CEB5412

```

```

Ciphertext 1
Plaintext 1
Segment #3
InputBlock DA7C9117 7D3E6C5D
OutputBlock BE9A7EB4 DA9131E1
Ciphertext 0
Plaintext 1
Segment #4
InputBlock B4F9222E FA7CD8BA
OutputBlock 986D65A9 8F72D62F
Ciphertext 1
Plaintext 0
Segment #5
InputBlock 69F2445D F4F9B175
OutputBlock 6D87A6C5 42C50EB6
Ciphertext 1
Plaintext 1
Segment #6
InputBlock D3E488BB E9F362EB
OutputBlock EDD759BC 745036D7
Ciphertext 1
Plaintext 0
Segment #7
InputBlock A7C91177 D3E6C5D7
OutputBlock DE45381C F86ADC5F
Ciphertext 0
Plaintext 1
Segment #8
InputBlock 4F9222EF A7CD8BAE
OutputBlock A41E3F9F 5329A6F5
Ciphertext 0
Plaintext 1

```

Plaintext is
6B

#####

Block Cipher Modes of Operation

Cipher Feedback (CFB)

#####

CFB-TDES (Encryption)

Key1 is

01234567 89ABCDEF

Key2 is

23456789 ABCDEF01

Key3 is

456789AB CDEF0123

IV is

F69F2445 DF4F9B17

Plaintext is

6BC1BEE2 2E409F96

Segment Length = 8

Segment #1

InputBlock F69F2445 DF4F9B17

OutputBlock 6C4A09AC 778EE140

Plaintext 6B

Ciphertext 07

Segment #2

InputBlock 9F2445DF 4F9B1707

OutputBlock 549B701C 6F79E12F

Plaintext C1

Ciphertext 95

Segment #3

InputBlock 2445DF4F 9B170795

OutputBlock A54A6F7E D46328D6

Plaintext BE

Ciphertext 1B

Segment #4

InputBlock 45DF4F9B 1707951B

OutputBlock 90540AC2 76832F20

Plaintext E2

Ciphertext 72

Segment #5

InputBlock DF4F9B17 07951B72

OutputBlock B3FCFC0C 2B4792F2

Plaintext 2E

Ciphertext 9D

Segment #6

InputBlock 4F9B1707 951B729D

OutputBlock 828C80DE A7E31594

Plaintext 40

Ciphertext C2

Segment #7

InputBlock	9B170795	1B729DC2
OutputBlock	A5CB99BF	469D1281
Plaintext	9F	
Ciphertext	3A	
Segment #8		
InputBlock	1707951B	729DC23A
OutputBlock	2226EAE7	D45A1ED7
Plaintext	96	
Ciphertext	B4	

Ciphertext is
07951B72 9DC23AB4

=====
CFB-TDES (Decryption)

Key1 is
01234567 89ABCDEF
Key2 is
23456789 ABCDEF01
Key3 is
456789AB CDEF0123
IV is
F69F2445 DF4F9B17
Ciphertext is
07951B72 9DC23AB4
Segment Length = 8

Segment #1		
InputBlock	F69F2445	DF4F9B17
OutputBlock	6C4A09AC	778EE140
Ciphertext	07	
Plaintext	6B	
Segment #2		
InputBlock	9F2445DF	4F9B1707
OutputBlock	549B701C	6F79E12F
Ciphertext	95	
Plaintext	C1	
Segment #3		
InputBlock	2445DF4F	9B170795
OutputBlock	A54A6F7E	D46328D6
Ciphertext	1B	
Plaintext	BE	
Segment #4		

InputBlock	45DF4F9B 1707951B
OutputBlock	90540AC2 76832F20
Ciphertext	72
Plaintext	E2
Segment #5	
InputBlock	DF4F9B17 07951B72
OutputBlock	B3FCFC0C 2B4792F2
Ciphertext	9D
Plaintext	2E
Segment #6	
InputBlock	4F9B1707 951B729D
OutputBlock	828C80DE A7E31594
Ciphertext	C2
Plaintext	40
Segment #7	
InputBlock	9B170795 1B729DC2
OutputBlock	A5CB99BF 469D1281
Ciphertext	3A
Plaintext	9F
Segment #8	
InputBlock	1707951B 729DC23A
OutputBlock	2226EAE7 D45A1ED7
Ciphertext	B4
Plaintext	96

Plaintext is
6BC1BEE2 2E409F96

#####

Block Cipher Modes of Operation

Cipher Feedback (CFB)

#####

CFB-TDES (Encryption)

Key1 is
01234567 89ABCDEF
Key2 is
23456789 ABCDEF01
Key3 is

456789AB CDEF0123
IV is
F69F2445 DF4F9B17
Plaintext is
6BC1BEE2 2E409F96 E93D7E11 7393172A
AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
Segment Length = 64

Segment #1
Plaintext 6BC1BEE2 2E409F96
InputBlock F69F2445 DF4F9B17
OutputBlock 6C4A09AC 778EE140
Ciphertext 078BB74E 59CE7ED6

Segment #2
Plaintext E93D7E11 7393172A
InputBlock 078BB74E 59CE7ED6
OutputBlock 9F5BA08D 8ACDB815
Ciphertext 7666DE9C F95EAF3F

Segment #3
Plaintext AE2D8A57 1E03AC9C
InputBlock 7666DE9C F95EAF3F
OutputBlock 47C0E1E3 7EF7FDCE
Ciphertext E9ED6BB4 60F45152

Segment #4
Plaintext 9EB76FAC 45AF8E51
InputBlock E9ED6BB4 60F45152
OutputBlock 14E8F048 A8DE8749
Ciphertext 8A5F9FE4 ED710918

Ciphertext is
078BB74E 59CE7ED6 7666DE9C F95EAF3F
E9ED6BB4 60F45152 8A5F9FE4 ED710918

=====

CFB-TDES (Decryption)

Key1 is
01234567 89ABCDEF
Key2 is
23456789 ABCDEF01
Key3 is
456789AB CDEF0123
IV is
F69F2445 DF4F9B17

Ciphertext is
078BB74E 59CE7ED6 7666DE9C F95EAF3F
E9ED6BB4 60F45152 8A5F9FE4 ED710918
Segment Length = 64

Segment #1
Ciphertext 078BB74E 59CE7ED6
InputBlock F69F2445 DF4F9B17
OutputBlock 6C4A09AC 778EE140
Plaintext 6BC1BEE2 2E409F96

Segment #2
Ciphertext 7666DE9C F95EAF3F
InputBlock 078BB74E 59CE7ED6
OutputBlock 9F5BA08D 8ACDB815
Plaintext E93D7E11 7393172A

Segment #3
Ciphertext E9ED6BB4 60F45152
InputBlock 7666DE9C F95EAF3F
OutputBlock 47C0E1E3 7EF7FDCE
Plaintext AE2D8A57 1E03AC9C

Segment #4
Ciphertext 8A5F9FE4 ED710918
InputBlock E9ED6BB4 60F45152
OutputBlock 14E8F048 A8DE8749
Plaintext 9EB76FAC 45AF8E51

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

#####

Block Cipher Modes of Operation

Cipher Feedback (CFB)

#####

CFB-TDES (Encryption)

Key1 is
01234567 89ABCDEF
Key2 is

23456789 ABCDEF01
Key3 is
01234567 89ABCDEF
IV is
F69F2445 DF4F9B17
Plaintext is
6B
Segment Length = 1

Segment #1
InputBlock F69F2445 DF4F9B17
OutputBlock 0A540720 EDD99653
Plaintext 0
Ciphertext 0

Segment #2
InputBlock ED3E488B BE9F362E
OutputBlock 5DB181E5 86EFE4EB
Plaintext 1
Ciphertext 1

Segment #3
InputBlock DA7C9117 7D3E6C5D
OutputBlock 646D31A0 DC8A7579
Plaintext 1
Ciphertext 1

Segment #4
InputBlock B4F9222E FA7CD8BB
OutputBlock 3BC130FD CEE8ACF5
Plaintext 0
Ciphertext 0

Segment #5
InputBlock 69F2445D F4F9B176
OutputBlock EADA0BA2 AEDA060E
Plaintext 1
Ciphertext 0

Segment #6
InputBlock D3E488BB E9F362EC
OutputBlock A3F96AFE 9BD123FA
Plaintext 0
Ciphertext 1

Segment #7
InputBlock A7C91177 D3E6C5D9
OutputBlock 1B39FBE2 D035FFCA
Plaintext 1
Ciphertext 1

Segment #8
InputBlock 4F9222EF A7CD8BB3

OutputBlock AB282627 9BF068CC
Plaintext 1
Ciphertext 0

Ciphertext is
66

CFB-TDES (Decryption)

Key1 is
01234567 89ABCDEF
Key2 is
23456789 ABCDEF01
Key3 is
01234567 89ABCDEF
IV is
F69F2445 DF4F9B17
Ciphertext is
66
Segment Length = 1

Segment #1
InputBlock F69F2445 DF4F9B17
OutputBlock 0A540720 EDD99653
Ciphertext 0
Plaintext 0

Segment #2
InputBlock ED3E488B BE9F362E
OutputBlock 5DB181E5 86EFE4EB
Ciphertext 1
Plaintext 1

Segment #3
InputBlock DA7C9117 7D3E6C5D
OutputBlock 646D31A0 DC8A7579
Ciphertext 1
Plaintext 1

Segment #4
InputBlock B4F9222E FA7CD8BB
OutputBlock 3BC130FD CEE8ACF5
Ciphertext 0
Plaintext 0

Segment #5
InputBlock 69F2445D F4F9B176

```

    OutputBlock  EADA0BA2 AEDA060E
    Ciphertext   0
    Plaintext    1
Segment #6
    InputBlock   D3E488BB E9F362EC
    OutputBlock  A3F96AFE 9BD123FA
    Ciphertext   1
    Plaintext    0
Segment #7
    InputBlock   A7C91177 D3E6C5D9
    OutputBlock  1B39FBE2 D035FFCA
    Ciphertext   1
    Plaintext    1
Segment #8
    InputBlock   4F9222EF A7CD8BB3
    OutputBlock  AB282627 9BF068CC
    Ciphertext   0
    Plaintext    1

```

Plaintext is
6B

#####

Block Cipher Modes of Operation

Cipher Feedback (CFB)

#####

CFB-TDES (Encryption)

```

Key1 is
    01234567 89ABCDEF
Key2 is
    23456789 ABCDEF01
Key3 is
    01234567 89ABCDEF
IV is
    F69F2445 DF4F9B17
Plaintext is
    6BC1BEE2 2E409F96
Segment Length = 8

```

Segment #1	
InputBlock	F69F2445 DF4F9B17
OutputBlock	0A540720 EDD99653
Plaintext	6B
Ciphertext	61
Segment #2	
InputBlock	9F2445DF 4F9B1761
OutputBlock	1945D01C C907BB02
Plaintext	C1
Ciphertext	D8
Segment #3	
InputBlock	2445DF4F 9B1761D8
OutputBlock	D35BBB58 8942DFDD
Plaintext	BE
Ciphertext	6D
Segment #4	
InputBlock	45DF4F9B 1761D86D
OutputBlock	784F700F C357E253
Plaintext	E2
Ciphertext	9A
Segment #5	
InputBlock	DF4F9B17 61D86D9A
OutputBlock	C0D6CB0C 186B591C
Plaintext	2E
Ciphertext	EE
Segment #6	
InputBlock	4F9B1761 D86D9AEE
OutputBlock	D6E571D3 C0FF2B27
Plaintext	40
Ciphertext	96
Segment #7	
InputBlock	9B1761D8 6D9AEE96
OutputBlock	0C42BEBD DB7CCFA3
Plaintext	9F
Ciphertext	93
Segment #8	
InputBlock	1761D86D 9AEE9693
OutputBlock	6B9A60FE B302F83F
Plaintext	96
Ciphertext	FD

Ciphertext is
61D86D9A EE9693FD

=====

CFB-TDES (Decryption)

Key1 is

01234567 89ABCDEF

Key2 is

23456789 ABCDEF01

Key3 is

01234567 89ABCDEF

IV is

F69F2445 DF4F9B17

Ciphertext is

61D86D9A EE9693FD

Segment Length = 8

Segment #1

InputBlock F69F2445 DF4F9B17

OutputBlock 0A540720 EDD99653

Ciphertext 61

Plaintext 6B

Segment #2

InputBlock 9F2445DF 4F9B1761

OutputBlock 1945D01C C907BB02

Ciphertext D8

Plaintext C1

Segment #3

InputBlock 2445DF4F 9B1761D8

OutputBlock D35BBB58 8942DFDD

Ciphertext 6D

Plaintext BE

Segment #4

InputBlock 45DF4F9B 1761D86D

OutputBlock 784F700F C357E253

Ciphertext 9A

Plaintext E2

Segment #5

InputBlock DF4F9B17 61D86D9A

OutputBlock C0D6CB0C 186B591C

Ciphertext EE

Plaintext 2E

Segment #6

InputBlock 4F9B1761 D86D9AEE

OutputBlock D6E571D3 C0FF2B27

Ciphertext 96

Plaintext 40

Segment #7
InputBlock 9B1761D8 6D9AEE96
OutputBlock 0C42BEBD DB7CCFA3
Ciphertext 93
Plaintext 9F

Segment #8
InputBlock 1761D86D 9AEE9693
OutputBlock 6B9A60FE B302F83F
Ciphertext FD
Plaintext 96

Plaintext is
6BC1BEE2 2E409F96

#####

Block Cipher Modes of Operation

Cipher Feedback (CFB)

#####

CFB-TDES (Encryption)

Key1 is
01234567 89ABCDEF
Key2 is
23456789 ABCDEF01
Key3 is
01234567 89ABCDEF
IV is
F69F2445 DF4F9B17
Plaintext is
6BC1BEE2 2E409F96 E93D7E11 7393172A
AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
Segment Length = 64

Segment #1
Plaintext 6BC1BEE2 2E409F96
InputBlock F69F2445 DF4F9B17
OutputBlock 0A540720 EDD99653
Ciphertext 6195B9C2 C39909C5
Segment #2

Plaintext	E93D7E11	7393172A
InputBlock	6195B9C2	C39909C5
OutputBlock	C7CE6D77	08C97185
Ciphertext	2EF31366	7B5A66AF
Segment #3		
Plaintext	AE2D8A57	1E03AC9C
InputBlock	2EF31366	7B5A66AF
OutputBlock	C6ABF8F4	87394679
Ciphertext	688672A3	993AEAE5
Segment #4		
Plaintext	9EB76FAC	45AF8E51
InputBlock	688672A3	993AEAE5
OutputBlock	C524754E	0B4DC20D
Ciphertext	5B931AE2	4EE24C5C

Ciphertext is

6195B9C2 C39909C5 2EF31366 7B5A66AF
688672A3 993AEAE5 5B931AE2 4EE24C5C

=====
CFB-TDES (Decryption)

Key1 is

01234567 89ABCDEF

Key2 is

23456789 ABCDEF01

Key3 is

01234567 89ABCDEF

IV is

F69F2445 DF4F9B17

Ciphertext is

6195B9C2 C39909C5 2EF31366 7B5A66AF
688672A3 993AEAE5 5B931AE2 4EE24C5C

Segment Length = 64

Segment #1

Ciphertext	6195B9C2	C39909C5
InputBlock	F69F2445	DF4F9B17
OutputBlock	0A540720	EDD99653
Plaintext	6BC1BEE2	2E409F96

Segment #2

Ciphertext	2EF31366	7B5A66AF
InputBlock	6195B9C2	C39909C5
OutputBlock	C7CE6D77	08C97185

Plaintext	E93D7E11	7393172A
Segment #3		
Ciphertext	688672A3	993AEAE5
InputBlock	2EF31366	7B5A66AF
OutputBlock	C6ABF8F4	87394679
Plaintext	AE2D8A57	1E03AC9C
Segment #4		
Ciphertext	5B931AE2	4EE24C5C
InputBlock	688672A3	993AEAE5
OutputBlock	C524754E	0B4DC20D
Plaintext	9EB76FAC	45AF8E51

Plaintext is

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

#####

Block Cipher Modes of Operation

Output Feedback (OFB)

#####

OFB-TDES (Encryption)

Key1 is

01234567 89ABCDEF

Key2 is

23456789 ABCDEF01

Key3 is

456789AB CDEF0123

IV is

F69F2445 DF4F9B17

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A

AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51

Block #1

InputBlock F69F2445 DF4F9B17

OutputBlock 6C4A09AC 778EE140

Text-In 6BC1BEE2 2E409F96

Text-Out 078BB74E 59CE7ED6

Block #2

InputBlock 6C4A09AC 778EE140

OutputBlock CF436C17 E1F56A8B

Text-In E93D7E11 7393172A

Text-Out 267E1206 92667DA1

Block #3

InputBlock CF436C17 E1F56A8B

OutputBlock 0BABE880 FE4F10F8

Text-In AE2D8A57 1E03AC9C

Text-Out A58662D7 E04CBC64

Block #4

InputBlock 0BABE880 FE4F10F8

OutputBlock BFF3BAF0 4674D4BF

Text-In 9EB76FAC 45AF8E51

Text-Out 2144D55C 03DB5AEE

Ciphertext is

078BB74E 59CE7ED6 267E1206 92667DA1

A58662D7 E04CBC64 2144D55C 03DB5AEE

=====

OFB-TDES (Decryption)

Key1 is

01234567 89ABCDEF

Key2 is

23456789 ABCDEF01

Key3 is

456789AB CDEF0123

IV is

F69F2445 DF4F9B17

Ciphertext is

078BB74E 59CE7ED6 267E1206 92667DA1

A58662D7 E04CBC64 2144D55C 03DB5AEE

Block #1

InputBlock F69F2445 DF4F9B17

OutputBlock 6C4A09AC 778EE140

Text-In 078BB74E 59CE7ED6

Text-Out 6BC1BEE2 2E409F96

Block #2

InputBlock 6C4A09AC 778EE140

OutputBlock CF436C17 E1F56A8B

Text-In 267E1206 92667DA1

Text-Out E93D7E11 7393172A

Block #3

InputBlock CF436C17 E1F56A8B

OutputBlock 0BABE880 FE4F10F8

Text-In A58662D7 E04CBC64

Text-Out AE2D8A57 1E03AC9C

Block #4

InputBlock 0BABE880 FE4F10F8

OutputBlock BFF3BAF0 4674D4BF

Text-In 2144D55C 03DB5AEE

Text-Out 9EB76FAC 45AF8E51

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A

AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51

#####

Block Cipher Modes of Operation

Output Feedback (OFB)

#####

OFB-TDES (Encryption)

Key1 is

01234567 89ABCDEF

Key2 is

23456789 ABCDEF01

Key3 is

01234567 89ABCDEF

IV is

F69F2445 DF4F9B17

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A

AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51

Block #1

InputBlock F69F2445 DF4F9B17

OutputBlock 0A540720 EDD99653

Text-In 6BC1BEE2 2E409F96

Text-Out 6195B9C2 C39909C5

Block #2

InputBlock 0A540720 EDD99653

OutputBlock DA09C466 8C4FDBAA

Text-In E93D7E11 7393172A

Text-Out 3334BA77 FFDCCC80

Block #3

InputBlock DA09C466 8C4FDBAA

OutputBlock 4AA86208 14604BF8

Text-In AE2D8A57 1E03AC9C

Text-Out E485E85F 0A63E764

Block #4

InputBlock 4AA86208 14604BF8

OutputBlock F33A1C82 768B91C5

Text-In 9EB76FAC 45AF8E51

Text-Out 6D8D732E 33241F94

Ciphertext is

6195B9C2 C39909C5 3334BA77 FFDCCC80

E485E85F 0A63E764 6D8D732E 33241F94

=====

OFB-TDES (Decryption)

Key1 is

01234567 89ABCDEF

Key2 is

23456789 ABCDEF01

Key3 is

01234567 89ABCDEF

IV is

F69F2445 DF4F9B17

Ciphertext is

6195B9C2 C39909C5 3334BA77 FFDCCC80
E485E85F 0A63E764 6D8D732E 33241F94

Block #1

InputBlock F69F2445 DF4F9B17

OutputBlock 0A540720 EDD99653

Text-In 6195B9C2 C39909C5

Text-Out 6BC1BEE2 2E409F96

Block #2

InputBlock 0A540720 EDD99653

OutputBlock DA09C466 8C4FDBAA

Text-In 3334BA77 FFDCCC80

Text-Out E93D7E11 7393172A

Block #3

InputBlock DA09C466 8C4FDBAA

OutputBlock 4AA86208 14604BF8

Text-In E485E85F 0A63E764

Text-Out AE2D8A57 1E03AC9C

Block #4

InputBlock 4AA86208 14604BF8

OutputBlock F33A1C82 768B91C5

Text-In 6D8D732E 33241F94

Text-Out 9EB76FAC 45AF8E51

Plaintext is

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

#####

Block Cipher Modes of Operation

Counter (CTR)

#####

CTR-TDES (Encryption)

Key1 is

01234567 89ABCDEF

Key2 is

23456789 ABCDEF01

Key3 is

456789AB CDEF0123

Initial Counter Value is

F69F2445 DF4F9B17

Plaintext is

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

Block #1

InputBlock	F69F2445 DF4F9B17
OutputBlock	6C4A09AC 778EE140
Text-In	6BC1BEE2 2E409F96
Text-Out	078BB74E 59CE7ED6

Block #2

InputBlock	F69F2445 DF4F9B18
OutputBlock	F0976FC3 2397EC4F
Text-In	E93D7E11 7393172A
Text-Out	19AA11D2 5004FB65

Block #3

InputBlock	F69F2445 DF4F9B19
OutputBlock	0E1167A6 A408A526
Text-In	AE2D8A57 1E03AC9C
Text-Out	A03CEDF1 BA0B09BA

Block #4

InputBlock	F69F2445 DF4F9B1A
OutputBlock	3D0BEE14 B33393F8
Text-In	9EB76FAC 45AF8E51
Text-Out	A3BC81B8 F69C1DA9

Ciphertext is

078BB74E 59CE7ED6 19AA11D2 5004FB65

A03CEDF1 BA0B09BA A3BC81B8 F69C1DA9

=====
CTR-TDES (Decryption)

Key1 is

01234567 89ABCDEF

Key2 is

23456789 ABCDEF01

Key3 is

456789AB CDEF0123

Initial Counter Value is

F69F2445 DF4F9B17

Ciphertext is

078BB74E 59CE7ED6 19AA11D2 5004FB65
A03CEDF1 BA0B09BA A3BC81B8 F69C1DA9

Block #1

InputBlock F69F2445 DF4F9B17

OutputBlock 6C4A09AC 778EE140

Text-In 078BB74E 59CE7ED6

Text-Out 6BC1BEE2 2E409F96

Block #2

InputBlock F69F2445 DF4F9B18

OutputBlock F0976FC3 2397EC4F

Text-In 19AA11D2 5004FB65

Text-Out E93D7E11 7393172A

Block #3

InputBlock F69F2445 DF4F9B19

OutputBlock 0E1167A6 A408A526

Text-In A03CEDF1 BA0B09BA

Text-Out AE2D8A57 1E03AC9C

Block #4

InputBlock F69F2445 DF4F9B1A

OutputBlock 3D0BEE14 B33393F8

Text-In A3BC81B8 F69C1DA9

Text-Out 9EB76FAC 45AF8E51

Plaintext is

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

#####

Block Cipher Modes of Operation

Counter (CTR)

#####

CTR-TDES (Encryption)

Key1 is

01234567 89ABCDEF

Key2 is

23456789 ABCDEF01

Key3 is

01234567 89ABCDEF

Initial Counter Value is

F69F2445 DF4F9B17

Plaintext is

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

Block #1

InputBlock	F69F2445 DF4F9B17
OutputBlock	0A540720 EDD99653
Text-In	6BC1BEE2 2E409F96
Text-Out	6195B9C2 C39909C5

Block #2

InputBlock	F69F2445 DF4F9B18
OutputBlock	32E2ECCB A83E4D77
Text-In	E93D7E11 7393172A
Text-Out	DBDF92DA DBAD5A5D

Block #3

InputBlock	F69F2445 DF4F9B19
OutputBlock	BB45C27C EC5FEE55
Text-In	AE2D8A57 1E03AC9C
Text-Out	1568482B F25C42C9

Block #4

InputBlock	F69F2445 DF4F9B1A
OutputBlock	F38F3C04 A2B48F5F
Text-In	9EB76FAC 45AF8E51
Text-Out	6D3853A8 E71B010E

Ciphertext is

6195B9C2 C39909C5 DBDF92DA DBAD5A5D

1568482B F25C42C9 6D3853A8 E71B010E

=====
CTR-TDES (Decryption)

Key1 is

01234567 89ABCDEF

Key2 is

23456789 ABCDEF01

Key3 is

01234567 89ABCDEF

Initial Counter Value is

F69F2445 DF4F9B17

Ciphertext is

6195B9C2 C39909C5 DBDF92DA DBAD5A5D
1568482B F25C42C9 6D3853A8 E71B010E

Block #1

InputBlock F69F2445 DF4F9B17

OutputBlock 0A540720 EDD99653

Text-In 6195B9C2 C39909C5

Text-Out 6BC1BEE2 2E409F96

Block #2

InputBlock F69F2445 DF4F9B18

OutputBlock 32E2ECCB A83E4D77

Text-In DBDF92DA DBAD5A5D

Text-Out E93D7E11 7393172A

Block #3

InputBlock F69F2445 DF4F9B19

OutputBlock BB45C27C EC5FEE55

Text-In 1568482B F25C42C9

Text-Out AE2D8A57 1E03AC9C

Block #4

InputBlock F69F2445 DF4F9B1A

OutputBlock F38F3C04 A2B48F5F

Text-In 6D3853A8 E71B010E

Text-Out 9EB76FAC 45AF8E51

Plaintext is

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