

#####

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
