

#####

## 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

TDES\_Core: BlockIn 6BC1BEE2 2E409F96

DES: BlockOut1 7277A00D C1C1C36B

DES: BlockOut2 F6C18AF6 58CC11D5

TDES\_Core: BlockOut 06EDE3D8 2884090A

Blockout 06EDE3D8 2884090A

Block #2

Blockin E93D7E11 7393172A

TDES\_Core: BlockIn E93D7E11 7393172A

DES: BlockOut1 2256338B 7A9F36EF

DES: BlockOut2 26026E68 9C91B1B5

TDES\_Core: BlockOut FF322C19 F0518486

Blockout FF322C19 F0518486

Block #3

Blockin AE2D8A57 1E03AC9C

TDES\_Core: BlockIn AE2D8A57 1E03AC9C

DES: BlockOut1 6E511022 CFEBEC48

DES: BlockOut2 8C6358D8 90CF31DF

TDES\_Core: BlockOut 73057697 2A666E58

Blockout 73057697 2A666E58

Block #4  
Blockin 9EB76FAC 45AF8E51  
TDES\_Core: BlockIn 9EB76FAC 45AF8E51  
DES: BlockOut1 9A4A53A1 C7D22E5B  
DES: BlockOut2 D9CE8344 2D0FA499  
TDES\_Core: BlockOut B6C88CF1 07340D3D  
Blockout B6C88CF1 07340D3D

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

=====  
ECB-TDES128 (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  
TDES\_Core: BlockIn 06EDE3D8 2884090A  
DES: BlockOut1 F6C18AF6 58CC11D5  
DES: BlockOut2 7277A00D C1C1C36B  
TDES\_Core: BlockOut 6BC1BEE2 2E409F96  
Blockout 6BC1BEE2 2E409F96

Block #2  
Blockin FF322C19 F0518486  
TDES\_Core: BlockIn FF322C19 F0518486  
DES: BlockOut1 26026E68 9C91B1B5  
DES: BlockOut2 2256338B 7A9F36EF  
TDES\_Core: BlockOut E93D7E11 7393172A  
Blockout E93D7E11 7393172A

Block #3

Blockin 73057697 2A666E58  
TDES\_Core: BlockIn 73057697 2A666E58  
DES: BlockOut1 8C6358D8 90CF31DF  
DES: BlockOut2 6E511022 CFEBEC48  
TDES\_Core: BlockOut AE2D8A57 1E03AC9C  
Blockout AE2D8A57 1E03AC9C

Block #4

Blockin B6C88CF1 07340D3D  
TDES\_Core: BlockIn B6C88CF1 07340D3D  
DES: BlockOut1 D9CE8344 2D0FA499  
DES: BlockOut2 9A4A53A1 C7D22E5B  
TDES\_Core: BlockOut 9EB76FAC 45AF8E51  
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

456789AB CDEF0123

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A

AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51

Block #1

Blockin 6BC1BEE2 2E409F96

TDES\_Core: BlockIn 6BC1BEE2 2E409F96

DES: BlockOut1 7277A00D C1C1C36B

DES: BlockOut2 F6C18AF6 58CC11D5

TDES\_Core: BlockOut 714772F3 39841D34

Blockout 714772F3 39841D34

Block #2

Blockin E93D7E11 7393172A

TDES\_Core: BlockIn E93D7E11 7393172A

DES: BlockOut1 2256338B 7A9F36EF

DES: BlockOut2 26026E68 9C91B1B5

TDES\_Core: BlockOut 267FCC4B D2949CC3

Blockout 267FCC4B D2949CC3

Block #3

Blockin AE2D8A57 1E03AC9C

TDES\_Core: BlockIn AE2D8A57 1E03AC9C

DES: BlockOut1 6E511022 CFEBEC48

DES: BlockOut2 8C6358D8 90CF31DF

TDES\_Core: BlockOut EE11C22A 576A3038

Blockout EE11C22A 576A3038

Block #4

Blockin 9EB76FAC 45AF8E51  
TDES\_Core: BlockIn 9EB76FAC 45AF8E51  
DES: BlockOut1 9A4A53A1 C7D22E5B  
DES: BlockOut2 D9CE8344 2D0FA499  
TDES\_Core: BlockOut 76183F99 C0B6DE87  
Blockout 76183F99 C0B6DE87

Ciphertext is

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

=====

ECB-TDES128 (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  
TDES\_Core: BlockIn 714772F3 39841D34  
DES: BlockOut1 F6C18AF6 58CC11D5  
DES: BlockOut2 7277A00D C1C1C36B  
TDES\_Core: BlockOut 6BC1BEE2 2E409F96  
Blockout 6BC1BEE2 2E409F96

Block #2

Blockin 267FCC4B D2949CC3  
TDES\_Core: BlockIn 267FCC4B D2949CC3  
DES: BlockOut1 26026E68 9C91B1B5  
DES: BlockOut2 2256338B 7A9F36EF  
TDES\_Core: BlockOut E93D7E11 7393172A  
Blockout E93D7E11 7393172A

Block #3

Blockin EE11C22A 576A3038

TDES\_Core: BlockIn EE11C22A 576A3038  
DES: BlockOut1 8C6358D8 90CF31DF  
DES: BlockOut2 6E511022 CFEBEC48  
TDES\_Core: BlockOut AE2D8A57 1E03AC9C  
Blockout AE2D8A57 1E03AC9C

Block #4

Blockin 76183F99 C0B6DE87  
TDES\_Core: BlockIn 76183F99 C0B6DE87  
DES: BlockOut1 D9CE8344 2D0FA499  
DES: BlockOut2 9A4A53A1 C7D22E5B  
TDES\_Core: BlockOut 9EB76FAC 45AF8E51  
Blockout 9EB76FAC 45AF8E51

Plaintext is

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

\*\*\*\*\*