

#####

## 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

\*\*\*\*\*

