Cryptography And Network Security

UNIT-III

Session 20

Dr. V. K. Pachghare

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Modes of Operation

Output Feedback Mode (OFB)

- Similar to CFB mode, except that the ciphertext output of DES is fed back into the Shift Register, rather than the actual final ciphertext

Output Feedback Mode (OFB)

- Similar to CFB mode, except that the ciphertext output of DES is fed back into the Shift Register, rather than the actual final ciphertext
- The Shift Register is set to an arbitrary initial value, and passed through the DES algorithm

Encryption

- Select 64-bit random for IV as input to the 64-bit shift register.

Encryption

- Select 64-bit random for IV as input to the 64-bit shift register.
- Encrypt the output of shift register with the key.

Encryption

- Select 64-bit random for IV as input to the 64-bit shift register.
- Encrypt the output of shift register with the key.
- Select “s” (value of “s” is equal to the size of plaintext block) bits from the encrypted output and discard 64-s bits.

- Performed XOR operation between the selected “s” bit and the plaintext block.

- Performed XOR operation between the selected “s” bit and the plaintext block.
- The output is ciphertext.

- Performed XOR operation between the selected “s” bit and the plaintext block.
- The output is ciphertext.
- The selected “s” bits are used as input for the shift register on the next step.

Encryption

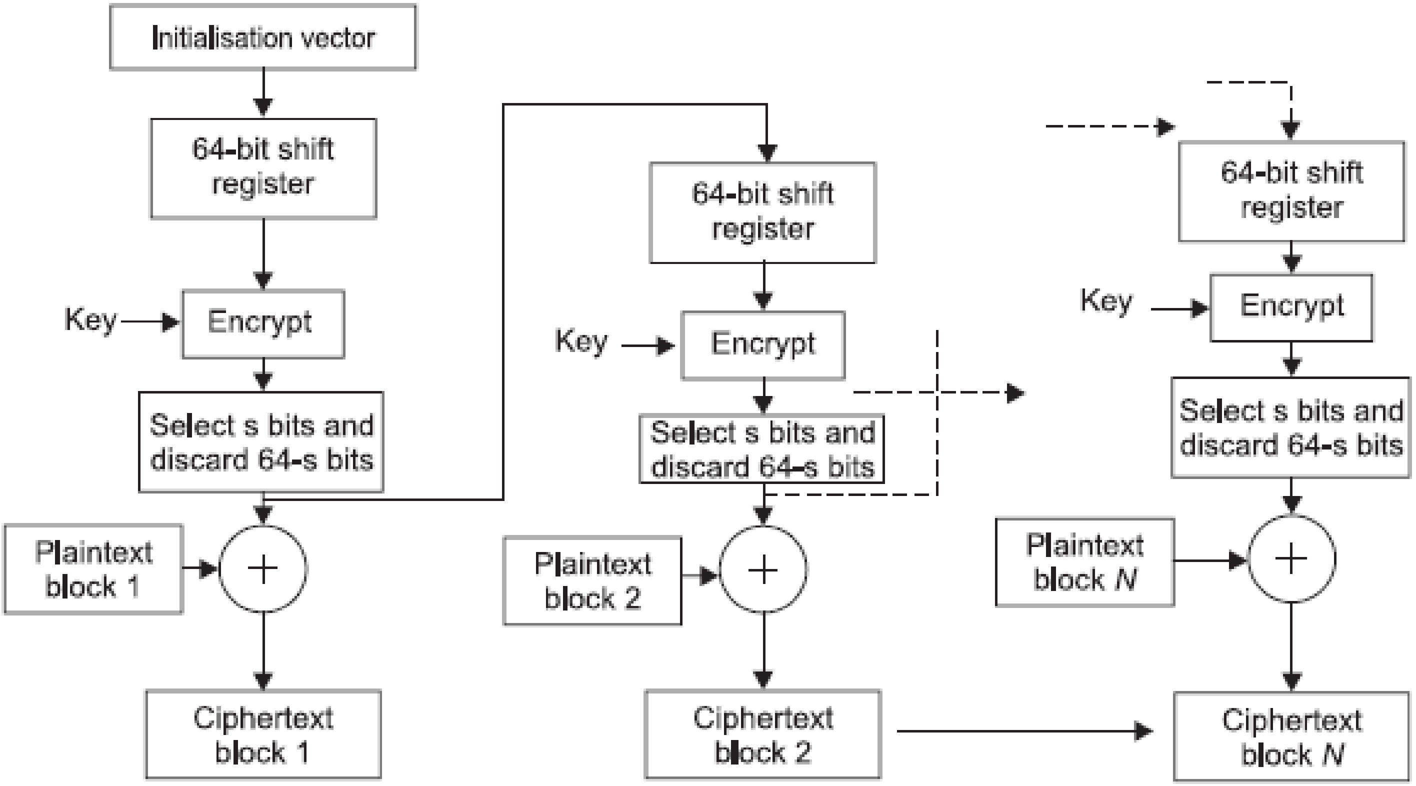

Figure 3.7 Output feedback mode: Encryption.

Decryption

- Similar to encryption.

Decryption

- Similar to encryption.
- Instead of plaintext block, corresponding ciphertext block is used for XOR operation

Decryption

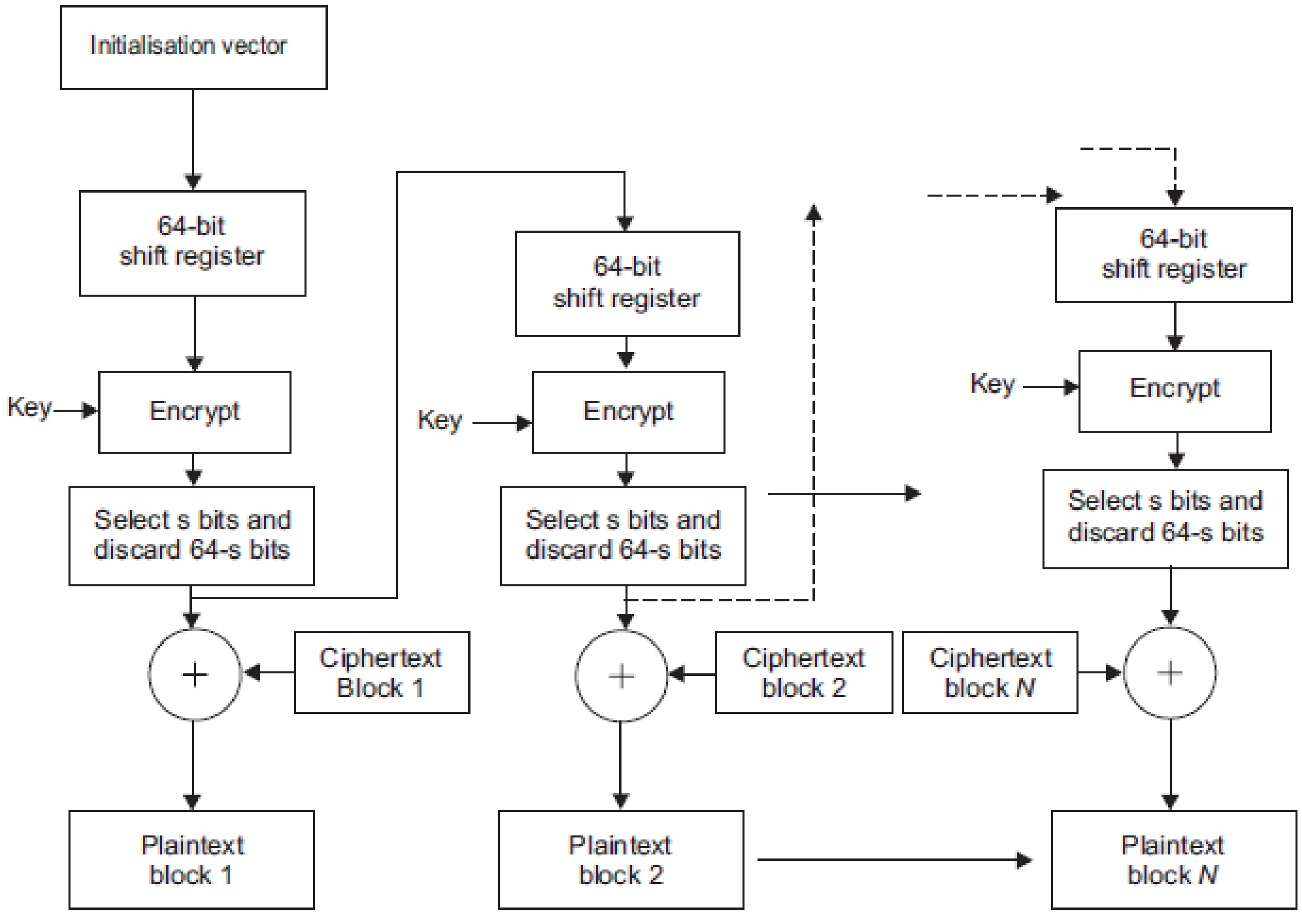

Figure 3.8 Output feedback mode: Decryption.

Disadvantages

- Cryptanalysis of output feedback mode is easy

Disadvantages

- Cryptanalysis of output feedback mode is easy
- Only a ciphertext block and encrypted “s” bits are sufficient to get the plaintext block.

Disadvantages

- Cryptanalysis of output feedback mode is easy
- Only a ciphertext block and encrypted “s” bits are sufficient to get the plaintext block.
- Here information about the key is not required, which help the cryptanalyst to break the cipher easily.

Disadvantages

- Cryptanalysis of output feedback mode is easy
- Only a ciphertext block and encrypted “s” bits are sufficient to get the plaintext block.
- Here information about the key is not required, which help the cryptanalyst to break the cipher easily.
- Therefore, this mode is less secure than cipher feedback mode.

Counter mode

Introduction

- A block cipher is worked like a stream cipher.

Introduction

- A block cipher is worked like a stream cipher.
- The counter is used whose value is changed in each round.

Introduction

- A block cipher is worked like a stream cipher.
- The counter is used whose value is changed in each round.
- Initially, the user has to set some value to the counter.

Introduction

- A block cipher is worked like a stream cipher.
- The counter is used whose value is changed in each round.
- Initially, the user has to set some value to the counter.
- Encrypt the counter value and the key.

Introduction

- A block cipher is worked like a stream cipher.
- The counter is used whose value is changed in each round.
- Initially, the user has to set some value to the counter.
- Encrypt the counter value and the key.
- This encrypted value is XOR with the block of plaintext. The result is a block of ciphertext.

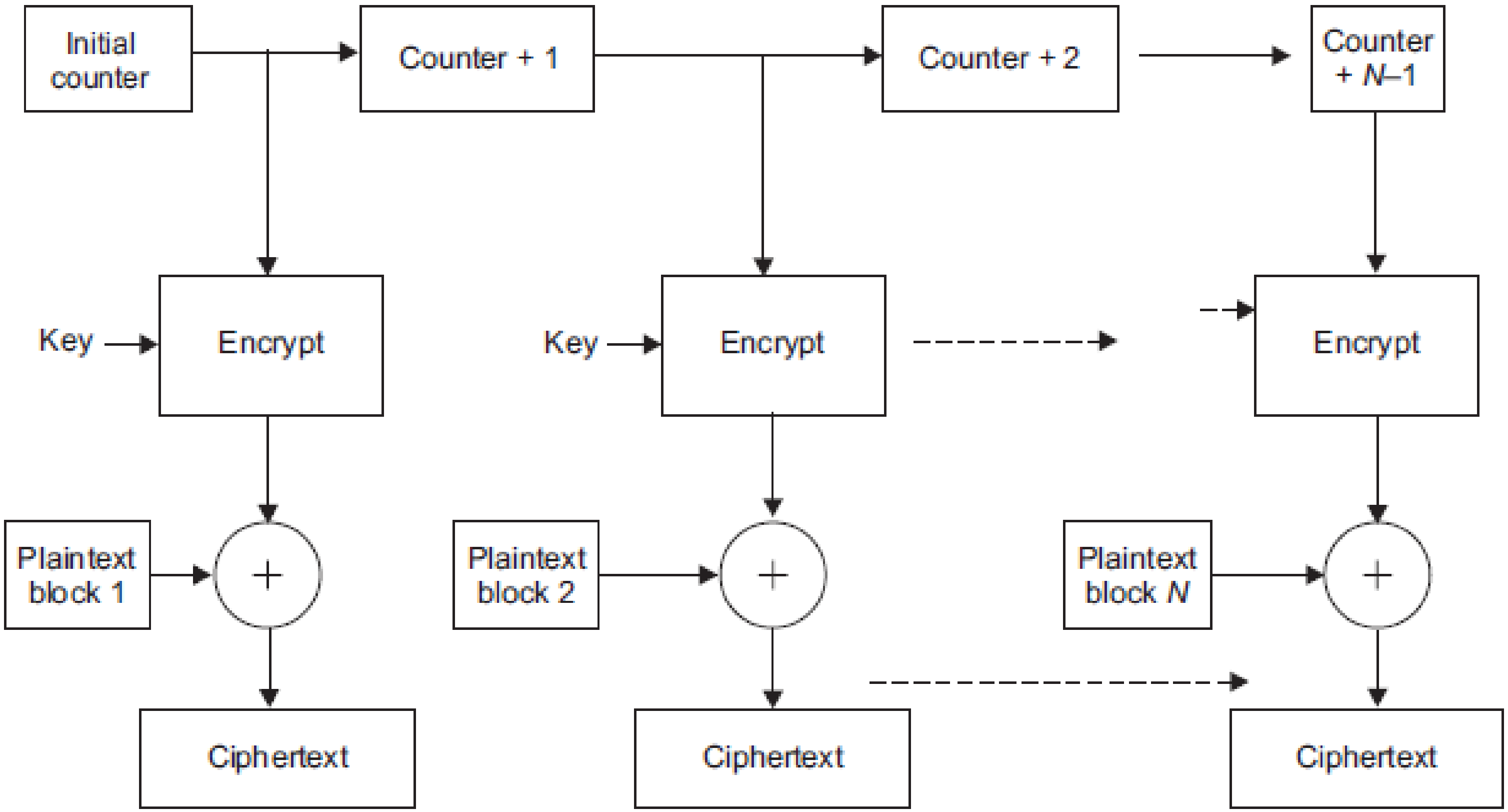

Figure 3.9 Counter mode: Encryption.

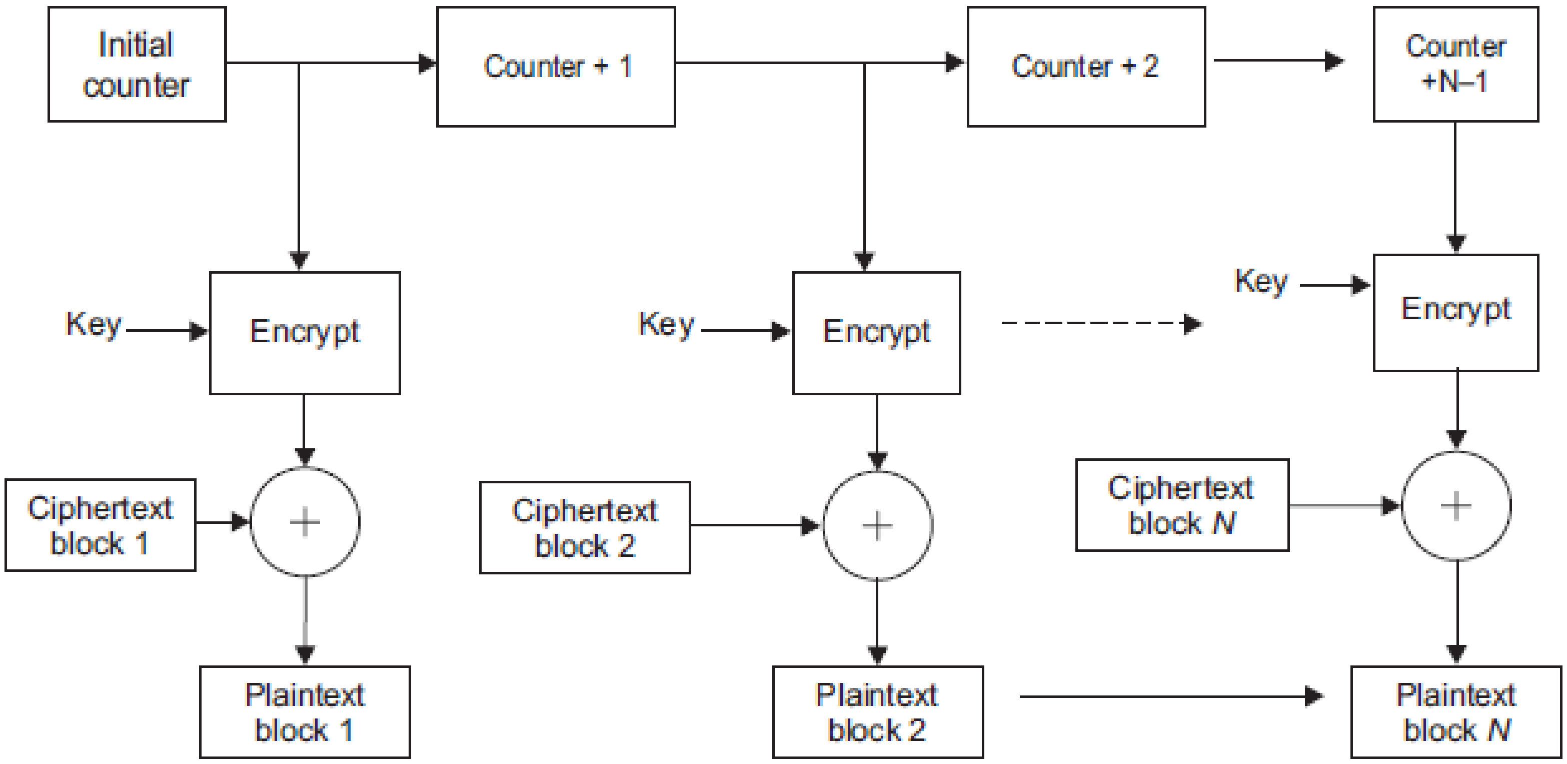

Figure 3.10 Counter mode: Decryption.

Advantages

- Faster than of cipher block chaining mode.

Advantages

- Faster than of cipher block chaining mode.
- Encryption can be done in parallel.

Advantages

- Faster than of cipher block chaining mode.
- Encryption can be done in parallel.
- Padding is not required.

Advantages

- Faster than of cipher block chaining mode.
- Encryption can be done in parallel.
- Padding is not required.
- Processing of plaintext blocks can be done randomly.

Advantages

- Faster than of cipher block chaining mode.
- Encryption can be done in parallel.
- Padding is not required.
- Processing of plaintext blocks can be done randomly.
- Only encryption algorithm is required.

Advantages

- Faster than of cipher block chaining mode.
- Encryption can be done in parallel.
- Padding is not required.
- Processing of plaintext blocks can be done randomly.
- Only encryption algorithm is required.
- It is as secure as the other modes.

Disadvantages

- Integrity of the message is not maintained.

Disadvantages

- Integrity of the message is not maintained.
- Reuse of counter value, compromise the security.