Cryptography and Network Security

BLOCK CIPHER MODES OF OPERATION

Session Meta Data

Author	**Dr T Sree Sharmila**
Reviewer	
Version Number	1.0
Release Date	3 July 2018

Revision History

Revision Date	Details	Version no.
		1.0

Agenda

- Introduction
- Modes of operations
  - Electronic Codebook Mode
  - Cipher block Chaining Mode
  - Cipher feedback mode
  - Output feedback Mode
  - Counter Mode
- Summary
- Test your understanding
- References

Introduction

- DES – Modes of Operation
- Advantages & Limitations of different Modes
- The Five Different Modes are:
  - Electronic Codebook Mode
  - Cipher block Chaining Mode
  - Cipher feedback mode
  - Output feedback Mode
  - Counter Mode

Agenda

- Introduction
- Modes of operations
  - Electronic Codebook Mode
  - Cipher block Chaining Mode
  - Cipher feedback mode
  - Output feedback Mode
  - Counter Mode
- Summary
- Test your understanding
- References

Modes of Operation

- block ciphers encrypt fixed size blocks
  - eg. DES encrypts 64-bit blocks with 56-bit key
- need some way to en/decrypt arbitrary amounts of data in practise
- **ANSI X3.106-1983 Modes of Use** (now FIPS 81) defines 4 possible modes
- subsequently 5 defined for AES & DES
- have **block** and **stream** modes

Modes of Operation

- Block modes:
  - Electronic Codebook Book (ECB)
    - Message is broken into independent blocks of 64 bits
  - Cipher Block Chaining (CBC)
    - Message is broken in independent blocks of 64 bits, but next input depends of previous output
    - Ci= Ek (Pi⊕Ci-1), with C-1=IV

Modes of Operation

- Stream Modes
  - Cipher FeedBack (CFB)
    - The message is xored with the feedback of encrypting the previous block
    - $C_i = P_i \oplus E_k(C_{i-1})$, with $C_{-1} = IV$
  - Output feedback
    - The feedback is independent of the message
    - $C_i = P_i \oplus E_k(O_{i-1})$, with $O_{-1} = IV$

Agenda

- Introduction
- Modes of operations
  - Electronic Codebook Mode
  - Cipher block Chaining Mode
  - Cipher feedback mode
  - Output feedback Mode
  - Counter Mode
- Summary
- Test your understanding
- References

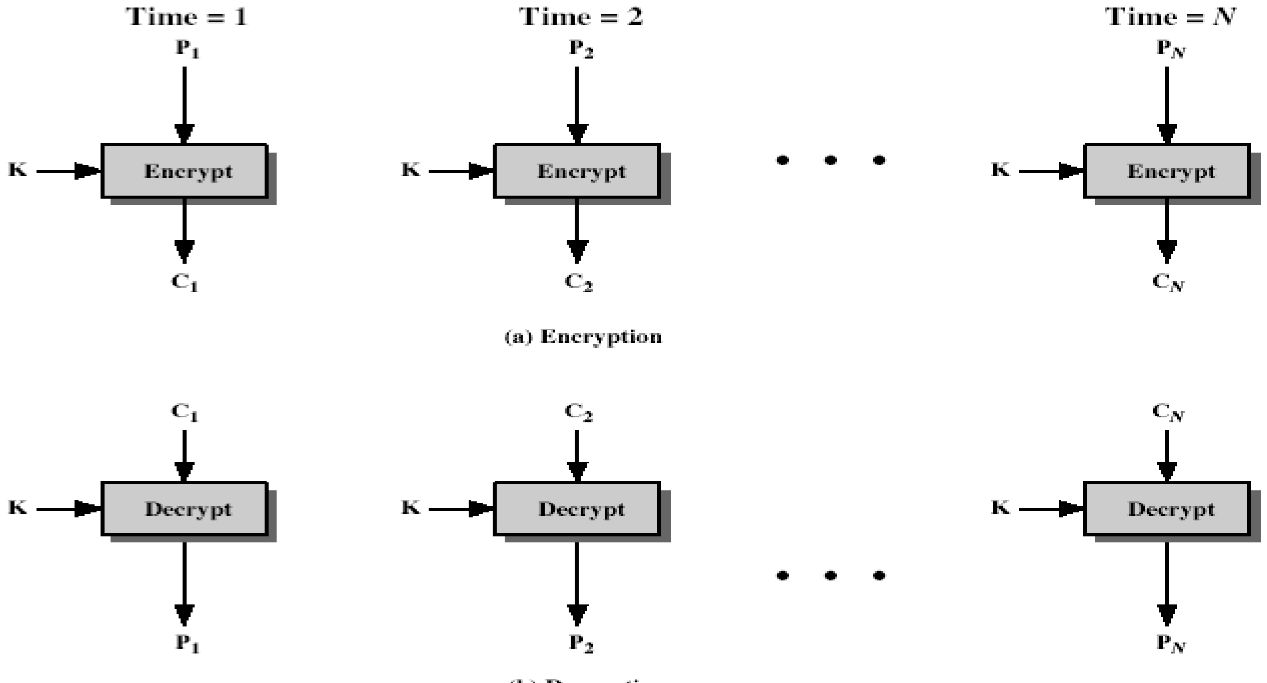
Electronic Codebook Book (ECB)

- message is broken into independent blocks which are encrypted
- each block is a value which is substituted, like a codebook, hence name
- each block is encoded independently of the other blocks

  $C_i = DES_{K1}(P_i)$

- uses: secure transmission of single values

Electronic Codebook Mode(ECB)



(a) Encryption

(b) Decryption

Advantages and Limitations of ECB

- message repetitions may show in ciphertext
  - if aligned with message block
  - particularly with data such graphics
  - or with messages that change very little, which become a code-book analysis problem
- weakness is due to the encrypted message blocks being independent
- main use is sending a few blocks of data

Agenda

- Introduction
- Modes of operations
  - Electronic Codebook Mode
  - Cipher block Chaining Mode
  - Cipher feedback mode
  - Output feedback Mode
  - Counter Mode
- Summary
- Test your understanding
- References

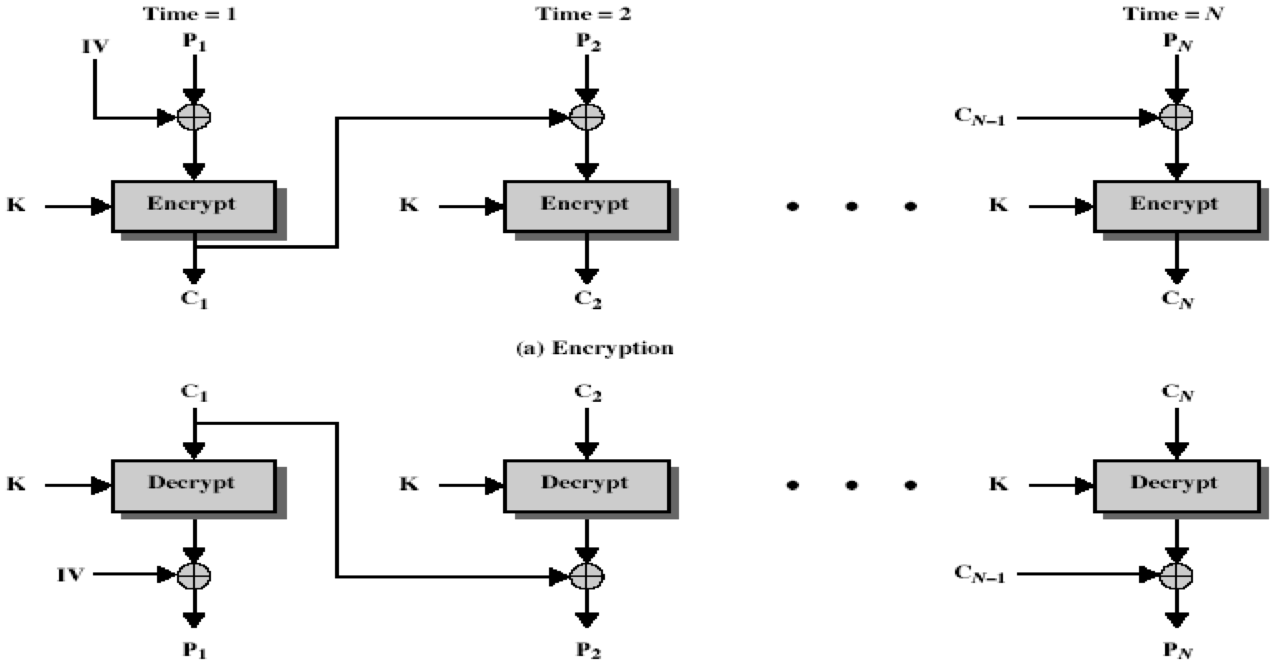
Cipher Block Chaining (CBC)

- message is broken into blocks
- linked together in encryption operation
- each previous cipher blocks is chained with current plaintext block, hence name
- use Initial Vector (IV) to start process

  $C_i = DES_{K1}(P_i \text{ XOR } C_{i-1})$

  $C_{-1} = IV$
- uses: bulk data encryption, authentication

Cipher Block Chaining (CBC)



(a) Encryption

(b) Decryption

Message Padding

- at end of message must handle a possible last short block
  - which is not as large as blocksize of cipher
  - pad either with known non-data value (eg nulls)
  - or pad last block along with count of pad size
    - eg. [b1 b2 b3 0 0 0 0 5]
    - means have 3 data bytes, then 5 bytes pad+count
  - this may require an extra entire block over those in message
- there are other, more esoteric modes, which avoid the need for an extra block

Advantages and Limitations of CBC

- a ciphertext block depends on **all** blocks before it
- any change to a block affects all following ciphertext blocks
- need **Initialization Vector** (IV)
  - which must be known to sender & receiver
  - if sent in clear, attacker can change bits of first block, and change IV to compensate
  - hence IV must either be a fixed value

Agenda

- Introduction
- Modes of operations
  - Electronic Codebook Mode
  - Cipher block Chaining Mode
  - Cipher feedback mode
  - Output feedback Mode
  - Counter Mode
- Summary
- Test your understanding
- References

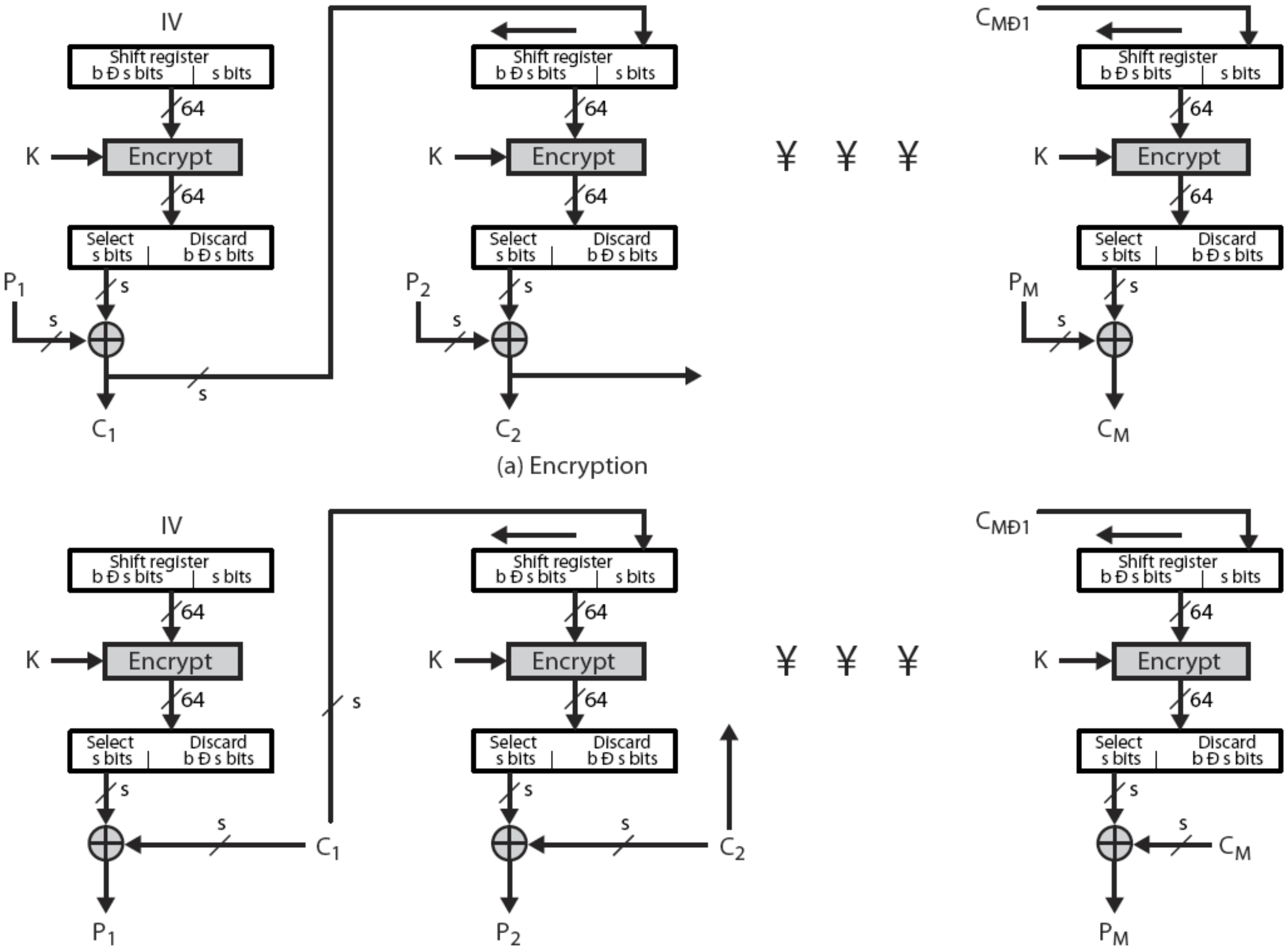
Cipher FeedBack (CFB)

- message is treated as a stream of bits
- added to the output of the block cipher
- result is feed back for next stage (hence name)
- standard allows any number of bit (1,8, 64 or 128 etc) to be feed back
  - denoted CFB-1, CFB-8, CFB-64, CFB-128 etc
- most efficient to use all bits in block (64 or 128)

  $C_i = P_i \text{ XOR } DES_{K1}(C_{i-1})$

  $C_{-1} = IV$
- uses: stream data encryption, authentication

Cipher FeedBack (CFB)



(a) Encryption

(b) Decryption

Advantages and Limitations of CFB

- appropriate when data arrives in bits/bytes
- most common stream mode
- limitation is need to stall while do block encryption after every n-bits
- note that the block cipher is used in **encryption** mode at **both** ends
- errors propogate for several blocks after the error

Agenda

- Introduction
- Modes of operations
  - Electronic Codebook Mode
  - Cipher block Chaining Mode
  - Cipher feedback mode
  - Output feedback Mode
  - Counter Mode
- Summary
- Test your understanding
- References

Output FeedBack (OFB)

- message is treated as a stream of bits
- output of cipher is added to message
- output is then feed back (hence name)
- feedback is independent of message
- can be computed in advance

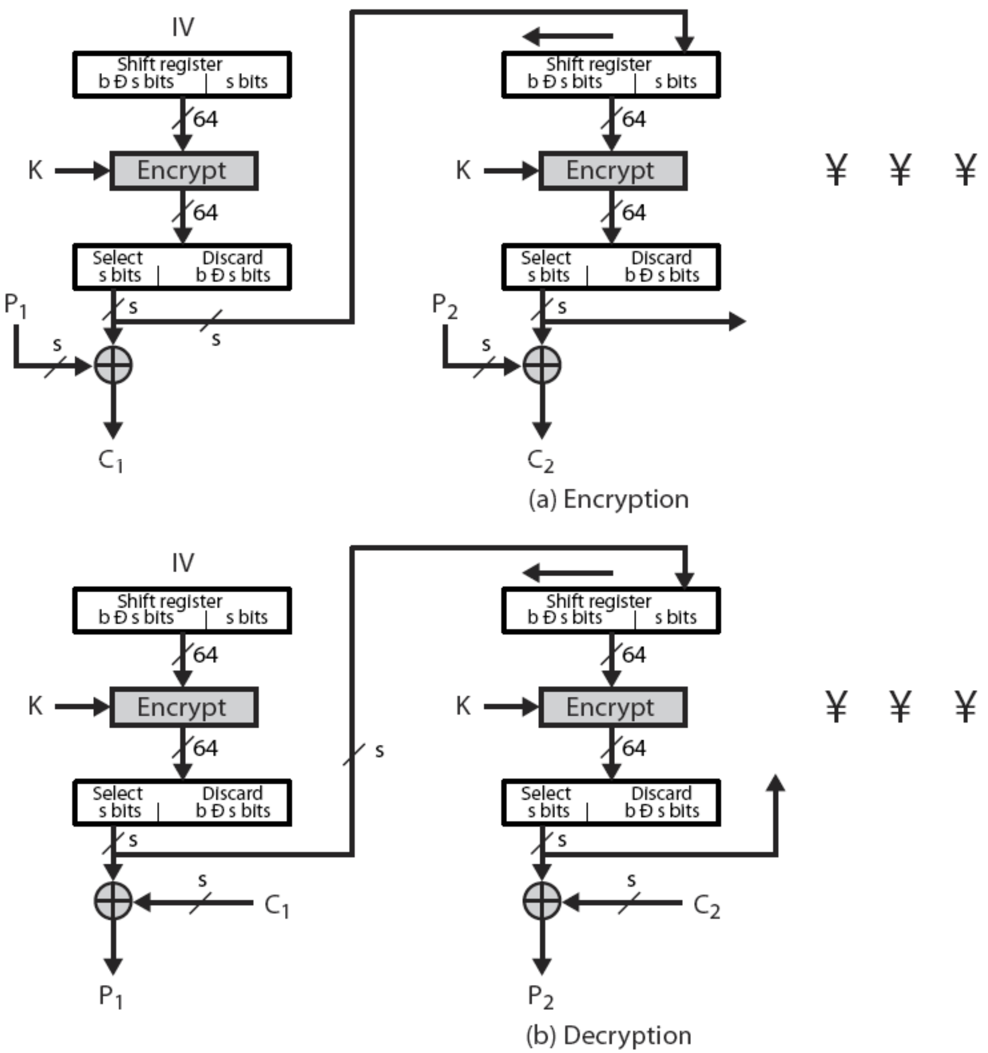
  $C_i = P_i \text{ XOR } O_i$

  $O_i = DES_{K1}(O_{i-1})$

  $O_{-1} = IV$

- uses: stream encryption on noisy channels

Output FeedBack (OFB)



(a) Encryption

(b) Decryption

Advantages and Limitations of OFB

- bit errors do not propagate
- more vulnerable to message stream modification
- a variation of a Vernam cipher
  - hence must **never** reuse the same sequence (key+IV)
- sender & receiver must remain in sync
- originally specified with m-bit feedback
- subsequent research has shown that only **full block feedback** (ie CFB-64 or CFB-128) should ever be used

Agenda

- Introduction
- Modes of operations
  - Electronic Codebook Mode
  - Cipher block Chaining Mode
  - Cipher feedback mode
  - Output feedback Mode
  - Counter Mode
- Summary
- Test your understanding
- References

Counter (CTR)

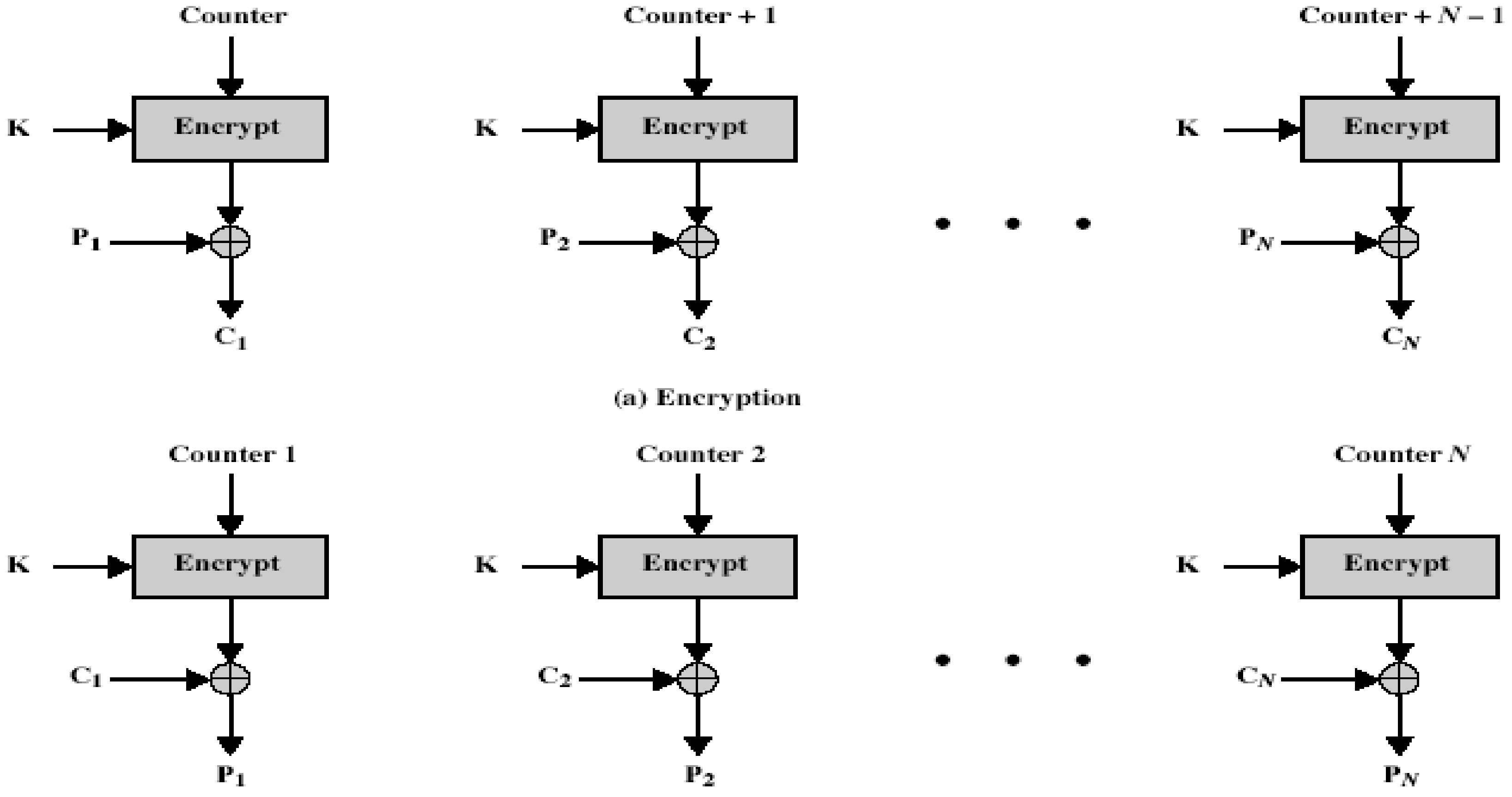
- a “new” mode, though proposed early on
- similar to OFB but encrypts counter value rather than any feedback value
- must have a different key & counter value for every plaintext block (never reused)

$C_i = P_i \text{ XOR } O_i$

$O_i = DES_{K1}(i)$

- uses: high-speed network encryptions

Counter (CTR)



(a) Encryption

(b) Decryption

Advantages and Limitations of CTR

- efficiency
  - can do parallel encryptions in h/w or s/w
  - can preprocess in advance of need
  - good for bursty high speed links
- random access to encrypted data blocks
- provable security (good as other modes)
- but must ensure never reuse key/counter values, otherwise could break (cf OFB)

Agenda

- Introduction
- Modes of operations
  - Electronic Codebook Mode
  - Cipher block Chaining Mode
  - Cipher feedback mode
  - Output feedback Mode
  - Counter Mode
- Summary
- Test your understanding
- References

Summary

- Studied Five Different Modes of operation
  - Electronic Codebook Mode
  - Cipher block Chaining Mode
  - Cipher feedback mode
  - Output feedback Mode
  - Counter Mode

Agenda

- Introduction
- Modes of operations
  - Electronic Codebook Mode
  - Cipher block Chaining Mode
  - Cipher feedback mode
  - Output feedback Mode
  - Counter Mode
- Summary
- Test your understanding
- References

Test your understanding

1. Explain different block cipher modes of operations.
2. What are the advantages and disadvantages of cipher block chaining mode?
3. List out the limitations of cipher feedback mode.

Agenda

- Introduction
- Modes of operations
  - Electronic Codebook Mode
  - Cipher block Chaining Mode
  - Cipher feedback mode
  - Output feedback Mode
  - Counter Mode
- Summary
- Test your understanding
- References

References

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security”, Prentice Hall of India, 2002.