



Department of CSE(HONORS)

CRYPTANALYSIS & CYBER DEFENSE 21CS304IRA

Topic:

MODES OF OPERATION

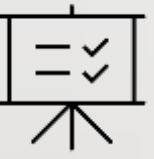
Session -8

AIM OF THE SESSION



To familiarize students with the basic concepts of various Modes of operation in block cipher.


INSTRUCTIONAL OBJECTIVES



The objective of this session is to introduce

1. Basic concepts of various Modes of operation in block cipher.
2. Demonstrate Block Cipher Modes of Operation
3. Describe Block Cipher Modes of Operation List out the Block
4. Describe the Modes of Operation

LEARNING OUTCOMES



At the end of this session, students are expected to know

- Define Block Cipher
- Summarize Block Cipher Modes of Operation

In this module we will discuss basic concepts of different modes of operation in cryptography. This module cover in depth analysis of working principle of these mode of operation with their computational complexity.

This Session provides an overview of modes of operation. Much of the theory of public-key cryptosystems is based on number theory. This session is designed to provide a comprehensive understanding of different modes of operation used in block ciphers. Block ciphers are widely used cryptographic algorithms that encrypt fixed-size blocks of data. The proper selection and understanding of block cipher modes of operation are essential for secure and efficient encryption of data.

SESSION DESCRIPTION

MODES OF OPERATION

- Modes of operation are methods used to transform a block cipher into a stream cipher or a hashing algorithm.
- These modes allow a block cipher to process larger amounts of data than the block size of the cipher, by dividing the data into blocks and applying the block cipher to each block in turn.
- Some commonly used modes of operation include Electronic Codebook (ECB), Cipher Block Chaining (CBC), Counter (CTR), and Galois/Counter Mode (GCM).

SESSION DESCRIPTION

BLOCK CIPHER MODES OF OPERATION

➤ Electronic Codebook (ECB)

- In the Electronic Codebook (ECB) mode of operation:
- The plaintext is divided into fixed-size blocks, such as "Block 1," "Block 2," and so on.
- Each block is encrypted independently using the encryption algorithm "E" with the same key "K," producing the corresponding ciphertext block.

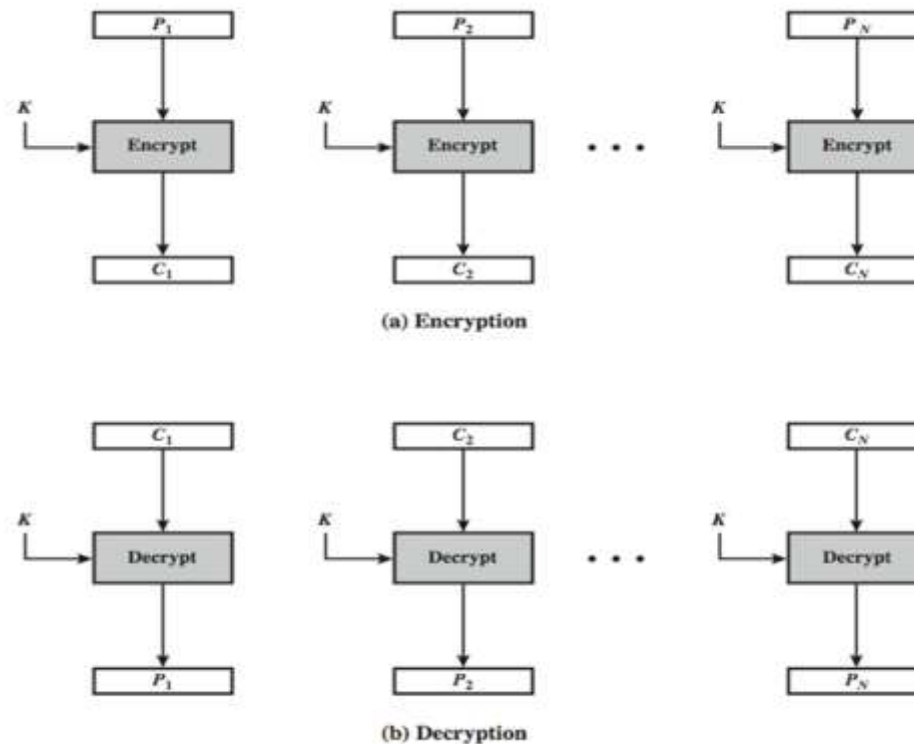
SESSION DESCRIPTION

BLOCK CIPHER MODES OF OPERATION

- This encryption process is repeated for each block of the plaintext, resulting in a series of ciphertext blocks.
- During decryption, each ciphertext block is decrypted independently using the decryption algorithm "D" with the same key "K," yielding the corresponding plaintext block.
- The decryption process is performed for each ciphertext block, allowing for the reconstruction of the original plaintext blocks.

SESSION DESCRIPTION

BLOCK CIPHER MODES OF OPERATION



ECB Mode of Operation.

Note: Copy Rights of this figure are reserved for the original author

SESSION DESCRIPTION

BLOCK CIPHER MODES OF OPERATION

- **Advantages and Limitations of ECB**
 - The ECB method is ideal for a short amount of data, such as an encryption key.
 - The most significant characteristic of ECB is that if the same b-bit block of plaintext appears more than once in the message, it always produces the same ciphertext.
 - Parallel encryption of blocks of bits is possible, thus it is a faster way of encryption.

SESSION DESCRIPTION

BLOCK CIPHER MODES OF OPERATION

- Simple way of block cipher.
- For lengthy messages, the ECB mode may not be secure. If the message is highly structured, it may be possible for a cryptanalyst to exploit these regularities.
- Prone to cryptanalysis since there is a direct relationship between plaintext and ciphertext.

SESSION DESCRIPTION

BLOCK CIPHER MODES OF OPERATION

- Cipher Block Chaining Mode (CBC)
 - The plaintext is divided into fixed-size blocks, such as "Block 1," "Block 2," and so on.
 - An Initialization Vector (IV) is generated, serving as the initial input for the encryption process.
 - For each plaintext block, the XOR operation is performed between the plaintext block and the previous ciphertext block or the IV.

SESSION DESCRIPTION

BLOCK CIPHER MODES OF OPERATION

- The result of the XOR operation is then encrypted using the encryption algorithm "E" with the same key "K," producing the ciphertext block.
- The ciphertext block becomes the input for the XOR operation in the next iteration.
- This process is repeated for each block of the plaintext, resulting in a series of ciphertext blocks.

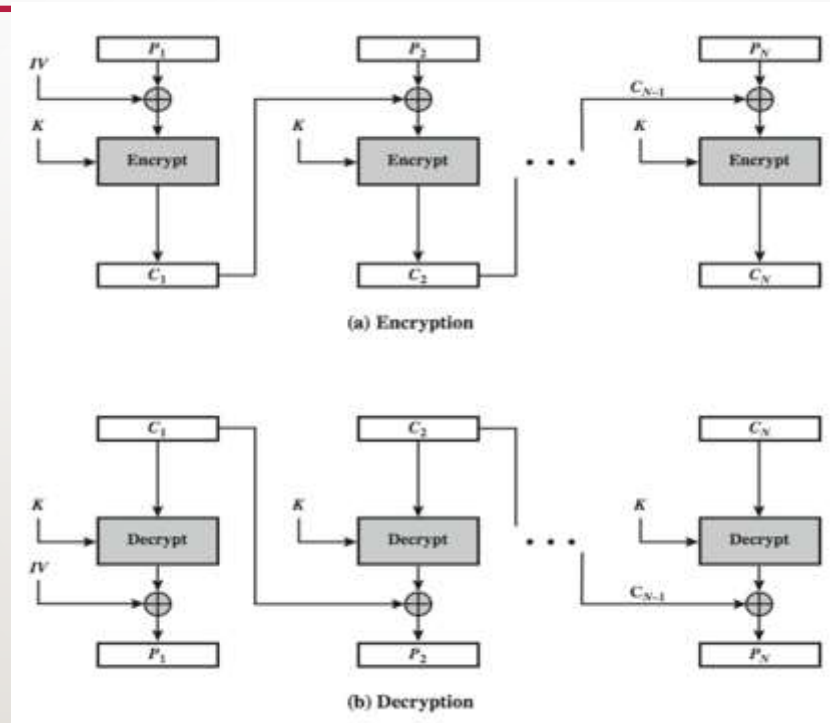
SESSION DESCRIPTION

BLOCK CIPHER MODES OF OPERATION

- During decryption, the ciphertext blocks are decrypted using the decryption algorithm "D" with the same key "K."
- The decrypted ciphertext blocks are then XORed with the previous ciphertext block or the IV to obtain the corresponding plaintext blocks.
- The decryption process is performed for each ciphertext block, allowing for the reconstruction of the original plaintext blocks.

SESSION DESCRIPTION

BLOCK CIPHER MODES OF OPERATION



CBC Mode of Operation.

Note: Copy Rights of this figure are reserved for the original author

SESSION DESCRIPTION

BLOCK CIPHER MODES OF OPERATION

➤ Advantages and Limitations of CBC

- CBC works well for input greater than b bits.
- CBC is a good authentication mechanism.
- Better resistive nature towards cryptanalysis than ECB.
- Parallel encryption is not possible since every encryption requires previous cipher.

SELF-ASSESSMENT QUESTIONS

1. In ECB mode, how is the plaintext divided for encryption?

- a) Into fixed-size blocks
- b) Into variable-sized blocks
- c) Into a single block
- d) It is not divided

2. What is the primary disadvantage of ECB mode?

- a) Lack of parallelism
- b) Vulnerability to plaintext attacks
- c) Slow encryption process
- d) None of the above

SELF-ASSESSMENT QUESTIONS

3. In ECB mode, how are the blocks encrypted?

- a) Each block is encrypted independently using the same key
- b) Each block is encrypted using a different key
- c) Blocks are not encrypted individually
- d) Encryption depends on the size of the block

4. In ECB mode, what happens if two plaintext blocks are identical?

- a) Both blocks are encrypted differently
- b) Both blocks are encrypted with the same ciphertext
- c) Only the first block is encrypted
- d) Encryption fails

SUMMARY

Throughout the session, students will gain hands-on experience with implementing and analyzing various block cipher modes of operation through practical exercises and programming assignments. By the end of the course, students will have a solid understanding of different block cipher modes and be able to make informed decisions regarding their selection and use in real-world cryptographic applications.

TERMINAL QUESTIONS

1. Demonstrate the basic concept of the ECB mode of operation.
2. Summarize how the plaintext is divided and encrypted in the ECB mode.
3. List the advantages of using ECB mode for encryption?
4. Illustrate the basic concept of the CBC (Cipher Block Chaining) mode of operation in cryptography.
5. List the advantages of using CBC mode for encryption?

REFERENCES FOR FURTHER LEARNING OF THE SESSION

1. Cryptography and Network Security Principles and Practice, by William Stallings, Pearson, 5th edition.
2. Applied Cryptography: Protocols, Algorithms, and Source Code in C, by Bruce Schneier, Second Edition, John Wiley & Sons, Inc., 2015.
3. Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, by Hamid R. Nemati and Li Yang, IGI Global, 2011
4. Forouzon B, "Cryptography and Network Security," Indian Edition, TMH (2010).

THANK YOU



Team – CACD