Department of CSE(HONORS)

CRYPTANALYSIS & CYBER DEFENSE 21CS3041RA

Topic:

MODES OF OPERATION

Session -9

AIM OF THE SESSION

To make the students well versed with the basic concepts of various Modes of operation in block cipher.

INSTRUCTIONAL OBJECTIVES

The objective of this session is to introduce basic concepts of various Modes of operation in block cipher and demonstrate Block Cipher Modes of Operation.

LEARNING OUTCOMES

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

- Define Block Cipher
- Demonstrate CFB, OFB & Counter Block Cipher Modes of Operation

Module Description

This module demonstrates block cipher modes of operation. It also helps to identify which ciphers operate as block ciphers and stream ciphers. Principles of Pseudorandom Number Generators are listed and types of Pseudorandom Number Generators are discussed. Finally, Stream Ciphers and its example RC4 algorithm are demonstrated.

SESSION INTRODUCTION

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

Cipher Feedback Mode

- In CFB mode, the previous ciphertext block is used to encrypt the next plaintext block, creating a feedback loop that enables the encryption and decryption processes. CFB mode operates on individual bits or bytes of data and converts a block cipher into a stream cipher.
- To begin, an Initialization Vector (IV) is generated, which acts as the initial input for the encryption process. The IV should be unique for each encryption session and must be kept secret.
- In the feedback mechanism, the IV (or the previous ciphertext block) is encrypted using the block cipher algorithm. The resulting ciphertext is then XORed with the corresponding plaintext bits (or bytes) to produce the encrypted output.

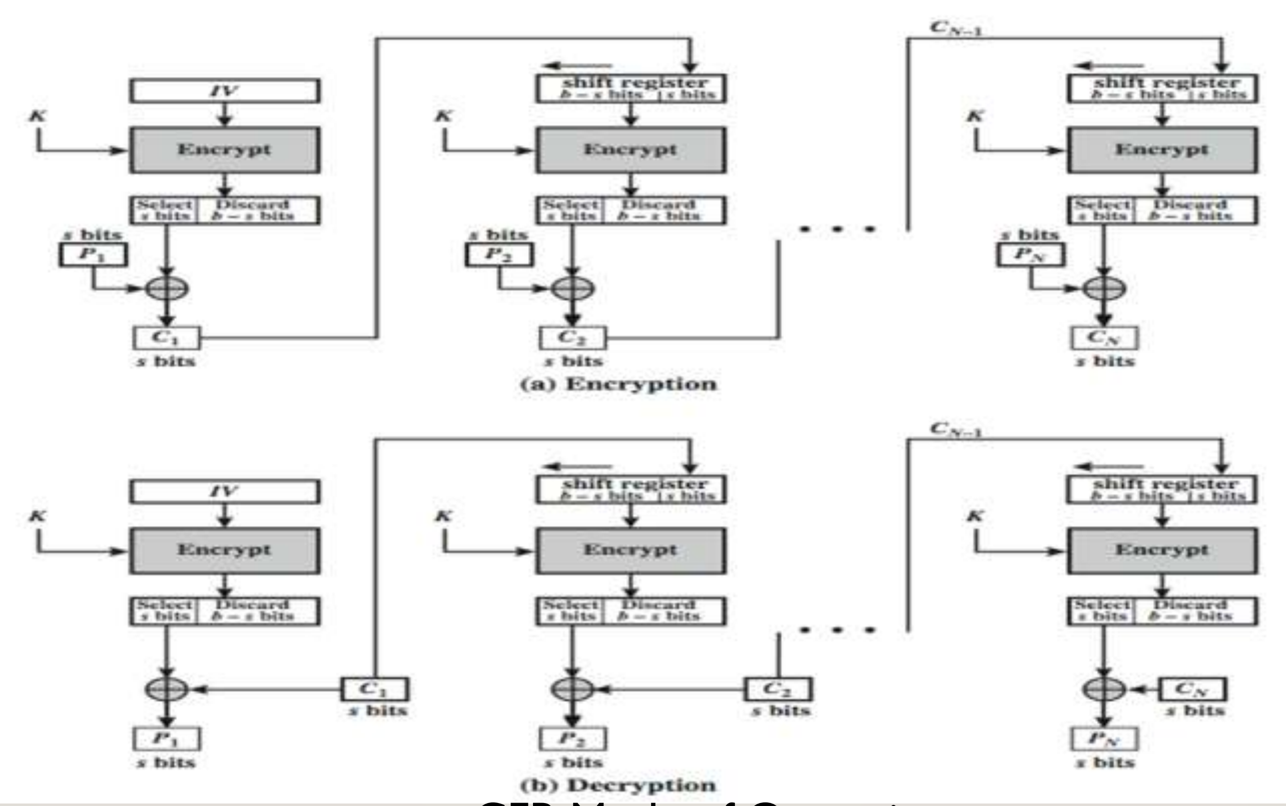
MODES OF OPERATION

Cipher Feedback Mode

- The encryption process starts with the IV, and the block cipher algorithm takes the IV as input, generating a block of ciphertext. This ciphertext is XORed with the first plaintext bits (or bytes), producing the encrypted output.
- In subsequent iterations, the previous ciphertext block becomes the input for the block cipher algorithm. The block cipher encrypts the previous ciphertext block, and the resulting ciphertext is XORed with the next plaintext bits (or bytes) to produce the next encrypted output. This feedback loop ensures that each block of plaintext is encrypted using the previous ciphertext block.
- During decryption, the same process is followed, using the IV (or the previous ciphertext block) as the input for the block cipher algorithm. The ciphertext is XORed with the corresponding encrypted bits (or bytes) to produce the decrypted output.

SESSION DESCRIPTION

MODES OF OPERATION



CFB Mode of Operation

Copy rights of this diagram belongs to original author

MODES OF OPERATION

Advantages and Limitations of CFB

- With 8-bit CFB, if a byte is lost, one byte of plaintext will be lost and the next 8 bytes will be garbled. After that, the plaintext will decrypt properly.
- If a byte is added to the ciphertext, a byte of garbage will be added, and the following 8 bytes will be garbled, the rest will be ok.
- Random stream can no longer be computed in advance
- Since, there is some data loss due to use of shift register, thus it is difficult for applying cryptanalysis.

SESSION DESCRIPTION

MODES OF OPERATION

Output feedback Mode of Operation

- Initialization: An IV (Initialization Vector) is generated, which serves as the initial input for the encryption process. The IV should be unique for each encryption session and must be kept secret. A secret key is also chosen, which remains constant throughout the encryption and decryption process.

MODES OF OPERATION

Keystream Generation:

The IV is encrypted using the block cipher algorithm, producing the initial keystream block. The keystream block is stored. To generate subsequent keystream blocks, the previous keystream block is encrypted using the block cipher algorithm, creating a feedback loop. The keystream blocks are generated independently of the plaintext, allowing for parallel encryption and decryption.

MODES OF OPERATION

Encryption Process:

- The keystream blocks are XORed with the corresponding plaintext blocks to produce the ciphertext. Each bit or byte of the plaintext is combined with the corresponding bit or byte of the keystream using the XOR operation.
- The resulting ciphertext is stored. Decryption Process: The same keystream generation process is followed as in encryption, using the IV and the secret key. The keystream blocks are XORed with the corresponding ciphertext blocks to produce the plaintext. Each bit or byte of the ciphertext is combined with the corresponding bit or byte of the keystream using the XOR operation.

MODES OF OPERATION

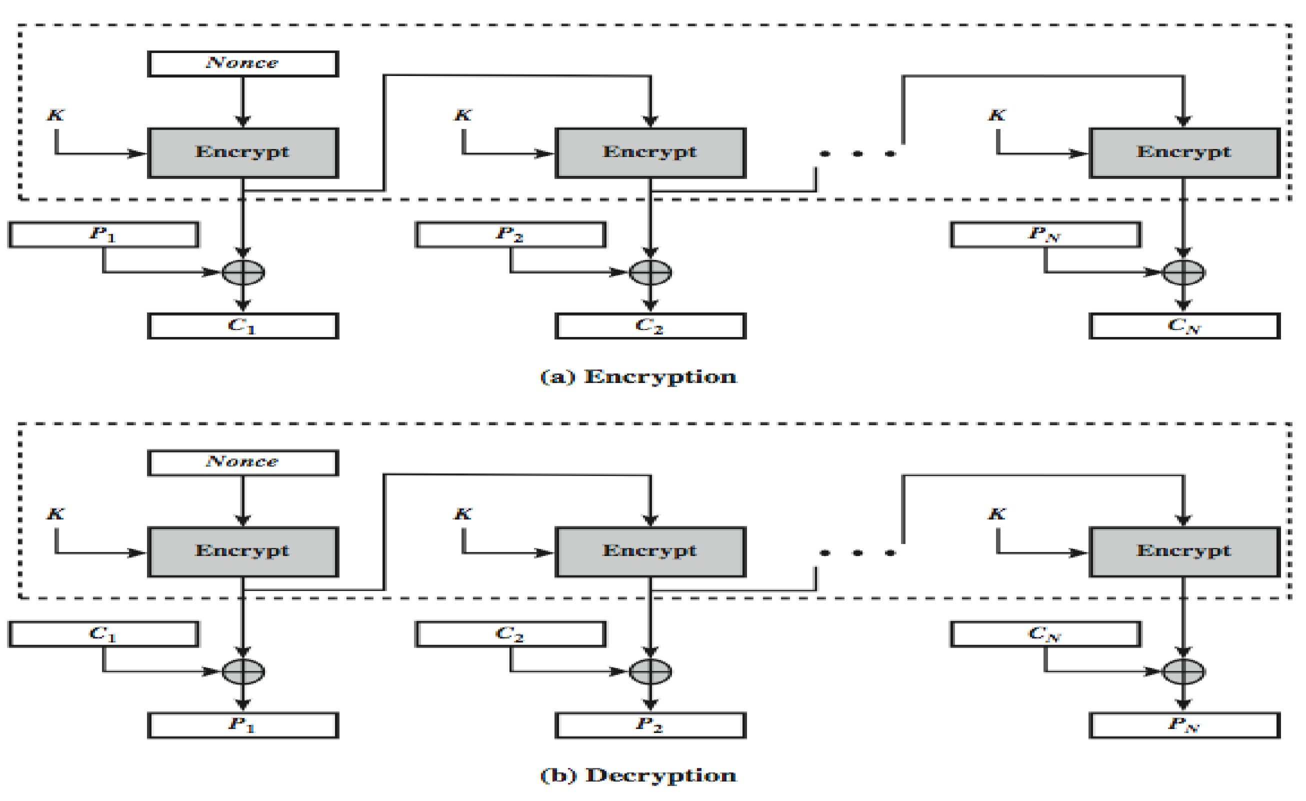
Random access encryption and decryption:

Any ciphertext block can be decrypted without the need for preceding blocks. Efficient parallel processing:

- The keystream blocks can be generated independently, allowing for efficient parallel encryption and decryption.

SESSION DESCRIPTION

MODES OF OPERATION



OFB Mode of Operation

Copy rights of this diagram belongs to original author

MODES OF OPERATION

Advantages and Limitations of OFB

- One advantage of the OFB method is that bit errors in transmission do not propagate. For example, if a bit error occurs in C1, only the recovered value of P1 is affected; subsequent plaintext units are not corrupted.

- With CFB, C1 also serves as input to the shift register and therefore causes additional corruption downstream.

- The disadvantage of OFB is that it is more vulnerable to a message stream modification attack than is CFB.

SESSION DESCRIPTION

MODES OF OPERATION

Counter Mode of Operation

- Counter (CTR) mode of operation is a cryptographic technique used to transform a block cipher into a stream cipher.
- It operates by encrypting a unique counter value for each plaintext block, generating a stream of pseudorandom bits or bytes that are then XORed with the plaintext to produce the ciphertext.
- The key idea behind CTR mode is to create a unique counter value for each block, ensuring that the encryption process remains deterministic and allowing for parallel encryption and decryption.

SESSION DESCRIPTION

MODES OF OPERATION

Counter Mode of Operation

Here's how CTR mode works:

- Initialization: An Initialization Vector (IV) is generated, which serves as the initial value for the counter. The IV should be unique for each encryption session and must be kept secret. A secret key is chosen, which remains constant during the encryption and decryption process.
- Counter Generation: A counter value is created for each plaintext block. The counter value can be a simple incrementing value or a more complex scheme, depending on the specific implementation. The counter value is usually combined with the IV and the block index to ensure uniqueness.

SESSION DESCRIPTION

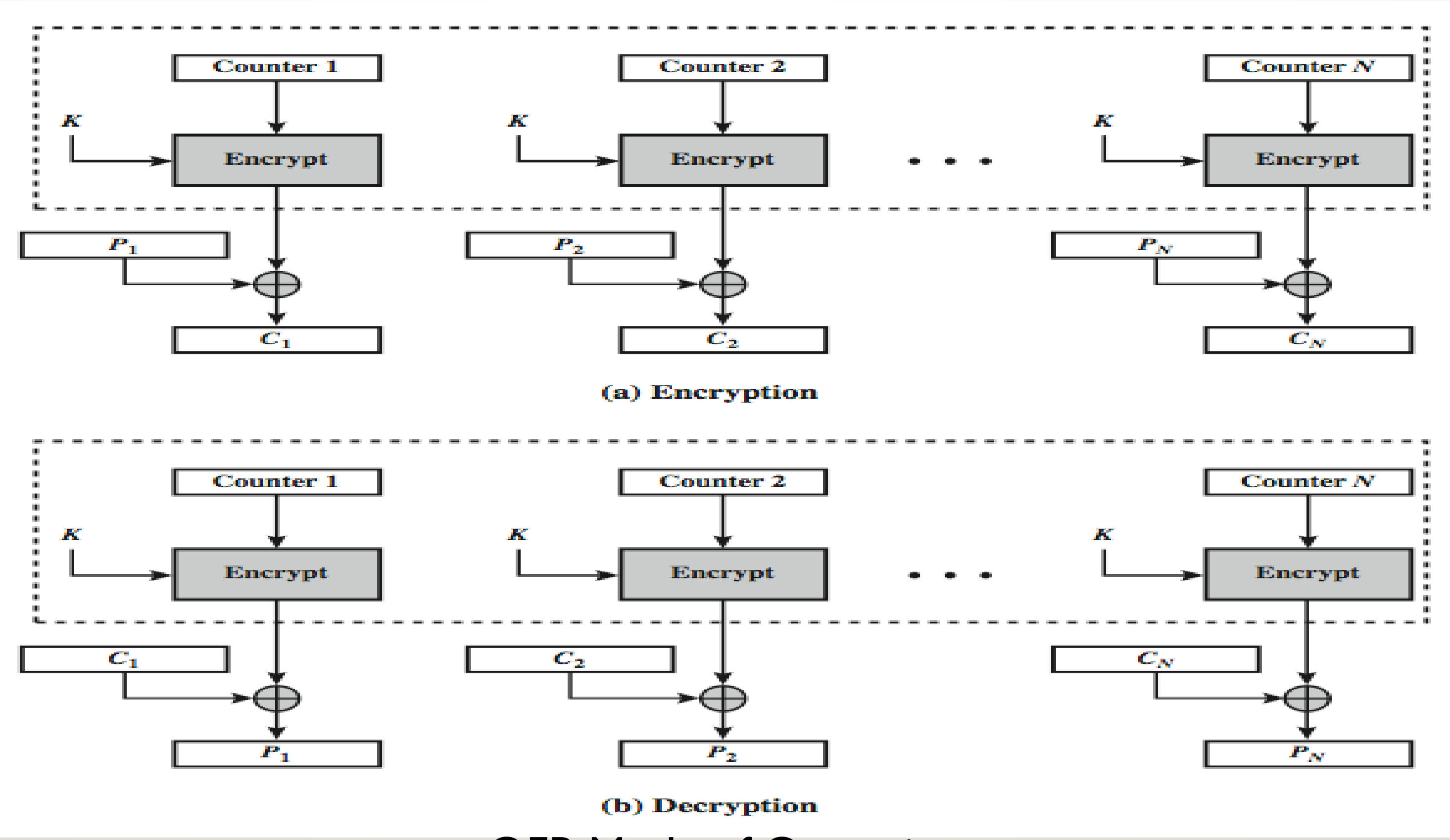
MODES OF OPERATION

Counter Mode of Operation

- Encryption Process: The counter value is encrypted using the block cipher algorithm, generating a pseudorandom keystream block. The keystream block is XORed with the corresponding plaintext block, producing the ciphertext. Each bit or byte of the plaintext is combined with the corresponding bit or byte of the keystream using the XOR operation. The resulting ciphertext is stored.
- Decryption Process: The same counter generation process is followed as in encryption, using the IV and the secret key. The counter value is encrypted using the block cipher algorithm, generating the keystream block. The keystream block is XORed with the corresponding ciphertext block, retrieving the original plaintext. Each bit or byte of the ciphertext is combined with the corresponding bit or byte of the keystream using the XOR operation. The resulting plaintext is stored.

SESSION DESCRIPTION

MODES OF OPERATION



OFB Mode of Operation

Copy rights of this diagram belongs to original author

MODES OF OPERATION

Advantages and Limitations of CTR

- The advantages are
- Can do parallel encryptions in h/w or s/w
- Can preprocess in advance of need
- Good for bursty high speed links
- It is simple and secure like other modes
- The disadvantage is the counter values must be made available at receiver for decryption.

SELF-ASSESSMENT QUESTIONS

1. CFB mode, how are the ciphertext blocks generated ?

a. By encrypting the previous ciphertext block

b. By encrypting the current plaintext block

c. By encrypting the IV (Initialization Vector)

d. By encrypting the secret key

2. Which of the following is a characteristic of CFB mode?

a. Random access encryption and decryption
b. Error propagation
c. Parallel encryption and decryption
d. All of the above

SELF-ASSESSMENT QUESTIONS

3. In CFB mode, what is the role of the XOR operation?

a. It combines the ciphertext block with the plaintext block

b. It combines the ciphertext block with the IV

c. It combines the ciphertext block with the secret key

d. It combines the keystream with the plaintext block or ciphertext block

4. What happens if there is an error in a ciphertext block in CFB mode?

a. The error propagates to the subsequent blocks
b. The error affects only the corresponding bits of the plaintext
c. The encryption process fails
d. The error affects the entire ciphertext

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 CFB Mode of Operation.

2. List advantages & limitations of CFB

3. Illustrate OFB Mode of Operation with a neat diagram

4. List the advantages & limitations of OFB

5. Demonstrate CTR Mode with a neat diagram

6. List advantages & limitations of CTR mode.

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, Algorthms, 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