وزارة التعليم العالي والبحث العلمي

قسم علوم الامن السيبراني

Department of Cyber Security

Subject

BLOCK CIPHER

Class: Second

Lecturer: 1

Teaching the subject

RAED ALSHMARY

introduction

Cryptography is the science of protecting information from unauthorized access. It aims to ensure confidentiality, integrity, and authentication of data. In the past, cryptography mainly focused on linguistic techniques, but modern cryptography relies heavily on mathematics and computer science.

Cryptography

The Art of Secure Communication

Confidentiality

Keeping information private, accessible only to authorised individuals.

Integrity

Ensuring that data remains unaltered and trustworthy throughout its lifecycle.

Authentication

Verifying the identity of users and the origin of information.

Cryptography is more than just secret codes; it's the science of safeguarding information from unauthorised access. It's about ensuring confidentiality, integrity, and authentication for all our data.

System Security Concept

The security of a system is only as strong as its weakest link. Even a strong cryptographic algorithm cannot protect a system if other security components are poorly designed or managed.

- Secure Hardware
- Vigilant Administrators
- Robust Software
- Solid Protocols

Symmetric Cipher Model

1

Plaintext

The original, unencrypted message.

2

Encryption Algorithm

The mathematical process that transforms plaintext into ciphertext.

3

Secret Key

A confidential value used by the algorithm for encryption and decryption.

4

Ciphertext

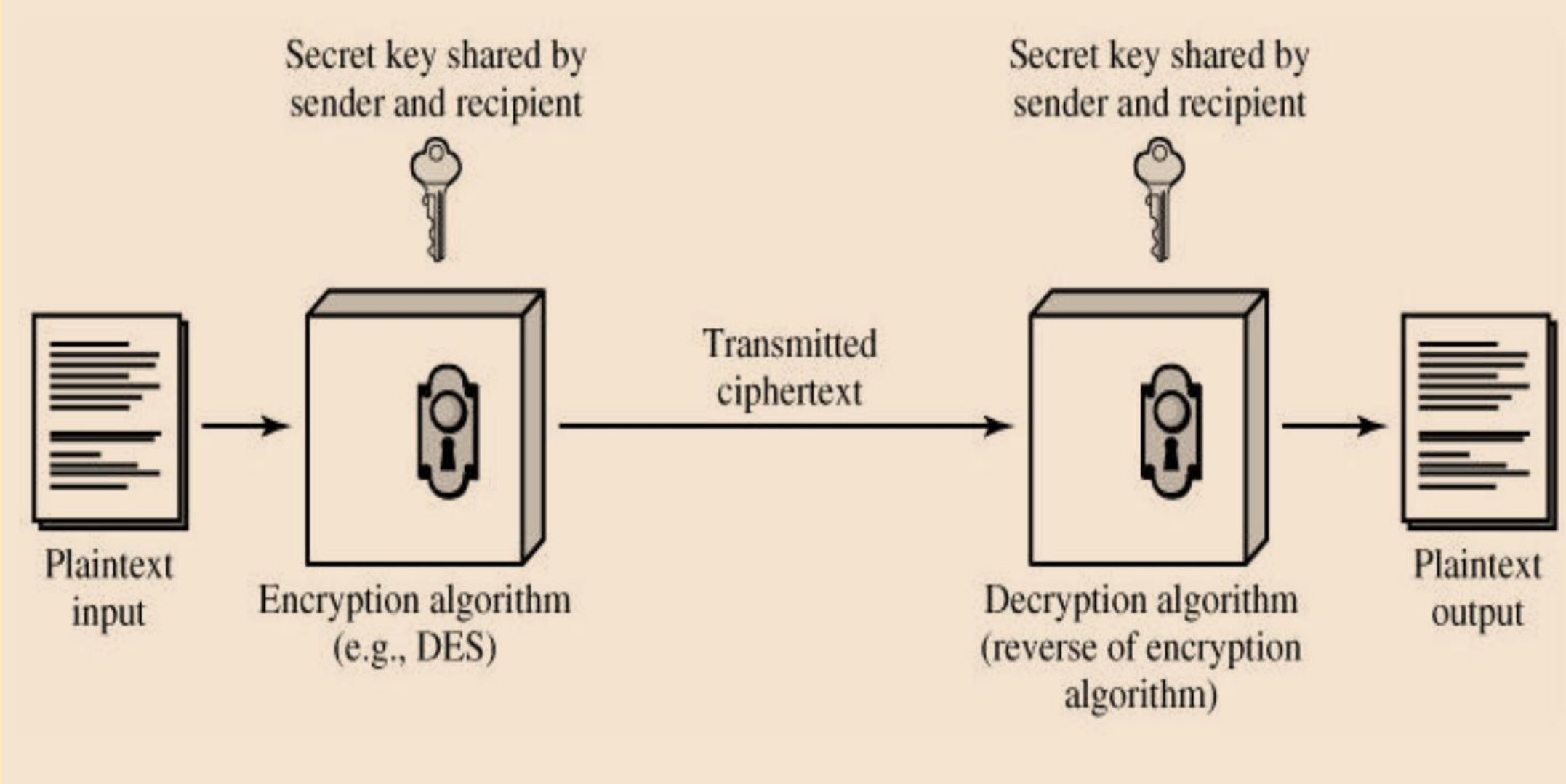
The encrypted, scrambled message.

5

Decryption Algorithm

The reverse process that transforms ciphertext back into plaintext.

A symmetric encryption system consists of the following elements: The same secret key is used for both encryption and decryption.


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Requirements for Secure Symmetric Encryption

1 - The encryption algorithm must be strong enough to resist cryptographic attacks, even if the attacker knows the algorithm.

2 - The secret key must be securely shared between the sender and receiver and kept confidential.

Evolution of Symmetric Block Ciphers

DES (1977)

The Data Encryption Standard, a foundational but now largely outdated cipher.

IDEA (1992)

International Data Encryption Algorithm, known for its strong design.

RC5 (1995)

Rivest Cipher 5, a block cipher notable for its simplicity and variable parameters.

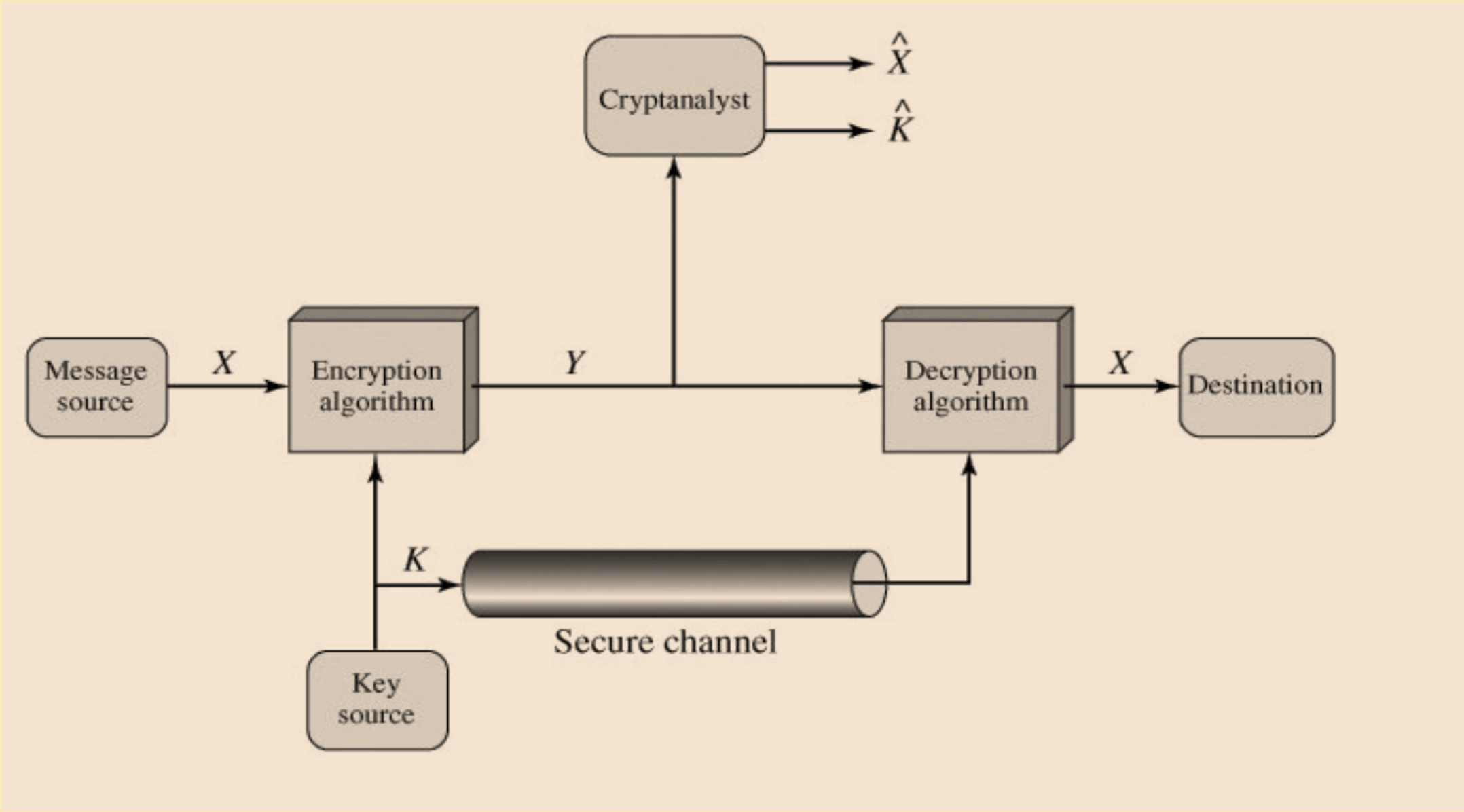
RC6 (1996)

Rivest Cipher 6, an improved version of RC5, a finalist for the AES standard.

AES (2001)

The Advanced Encryption Standard, currently the most widely used and highly secure standard globally.

AES stands as the cornerstone of modern symmetric encryption, protecting countless digital interactions daily.

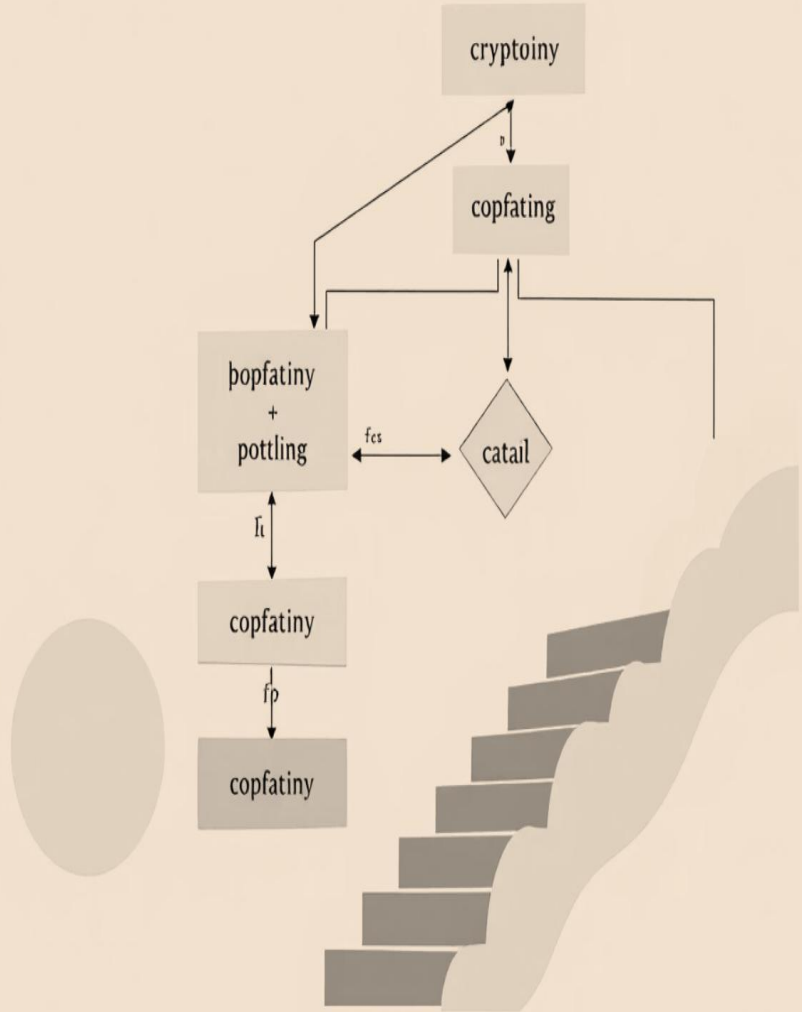

Cryptanalyst
$\hat{X}$
$\hat{K}$
Message source
X
Encryption algorithm
Y
Decryption algorithm
X
Destination
K
Secure channel
Key source

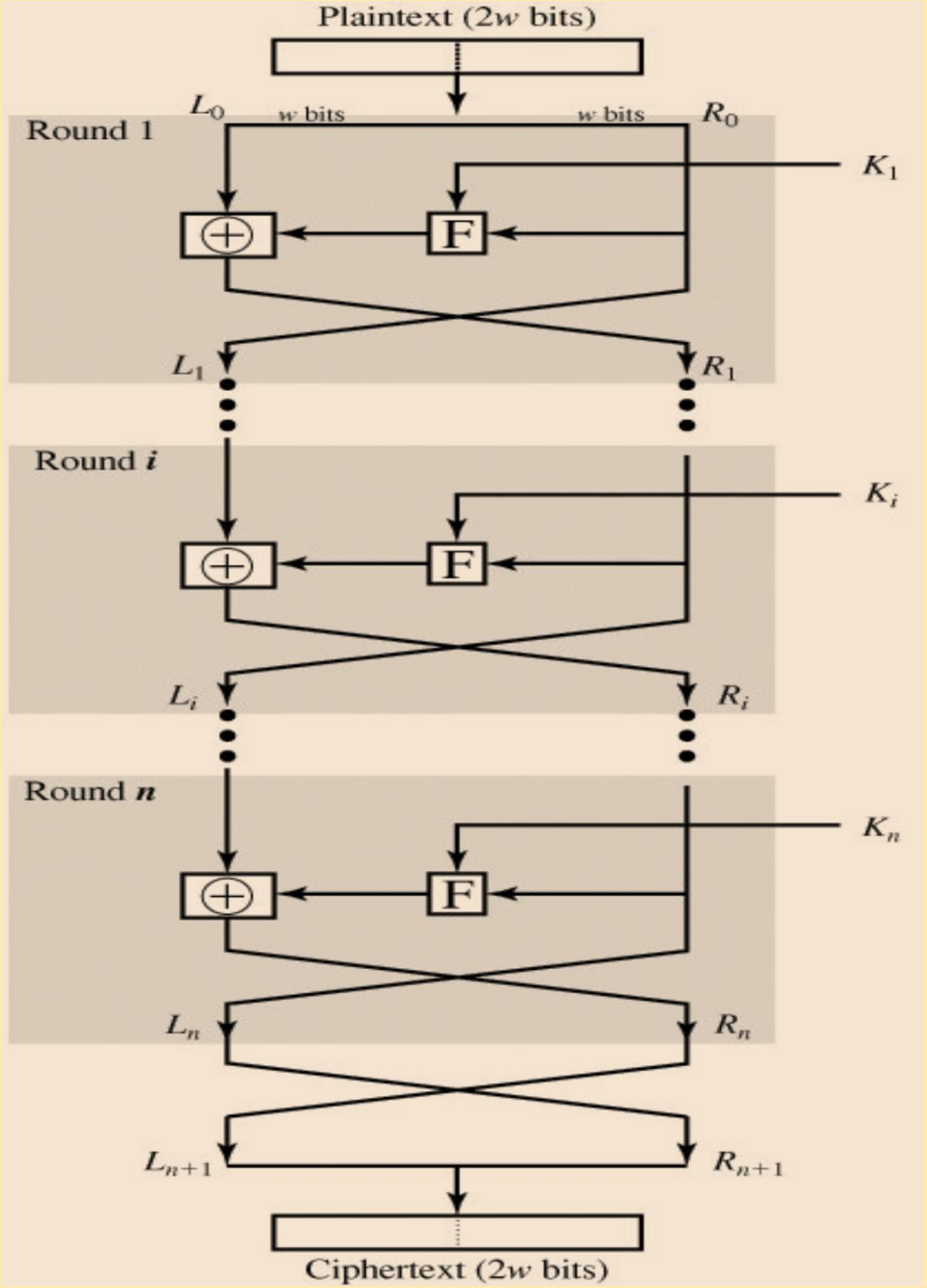
group activity

1- Discuss the main concern of cryptography?
2- Why was privacy of communication the original goal of cryptography?
3- Explain why modern cryptography relies on mathematics and computer science?
4- What are the main goals of cryptography and why is hardware maintenance not one of them?
5- Why is cryptography alone not sufficient for security?
6- Why is the same key used in symmetric decryption?
7- What are the requirements for secure symmetric encryption?
8- What happens if an attacker knows the secret key?
9- Why is AES an important symmetric algorithm?
10- Discuss the importance of adopting AES in 2001?
11- Why is DES considered outdated and insecure?

Feistel Cipher Structure

A Feistel cipher is a symmetric structure used in block cipher design. It divides the data block into two halves and processes them through multiple rounds. Encryption and decryption use the same structure, with the only difference being the order of the keys.
DES is a well-known example of a Feistel cipher.




Plaintext (2w bits)
Round 1
L_0
w bits
w bits
R_0
K_1
F
L_1
R_1
Round i
K_i
F
L_i
R_i
Round n
K_n
F
L_n
R_n
L_{n+1}
R_{n+1}
Ciphertext (2w bits)

Confusion and Diffusion

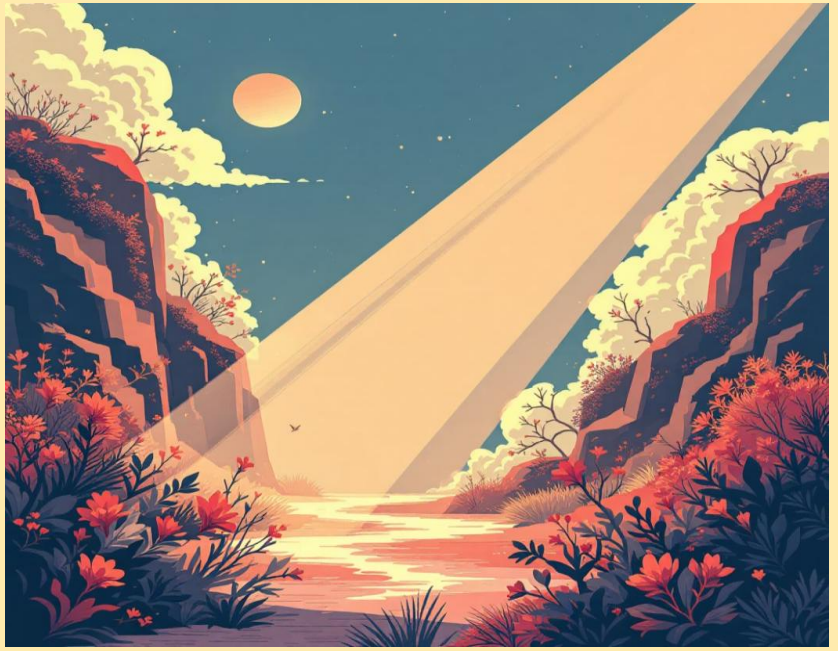
Confusion

the relationship between the plaintext and the ciphertext by using substitution operations.

Both concepts are essential for secure block cipher design.

Diffusion

the influence of each input bit over many output bits using permutation operations.



Substitution–Permutation Network (SPN)

An SP-network is a type of product cipher that consists of multiple rounds of:

Product Ciphers

These ciphers merge various cryptographic transformations, such as substitution and permutation, to significantly enhance overall security.

SP-Network

A type of product cipher featuring multiple rounds of substitution (S-boxes) for confusion and permutation (P-boxes) for diffusion. This combination creates a highly secure scrambling effect.

Substitution Operation

In substitution, a binary word is replaced with another binary word. This operation provides a high level of security and forms the basis of confusion.

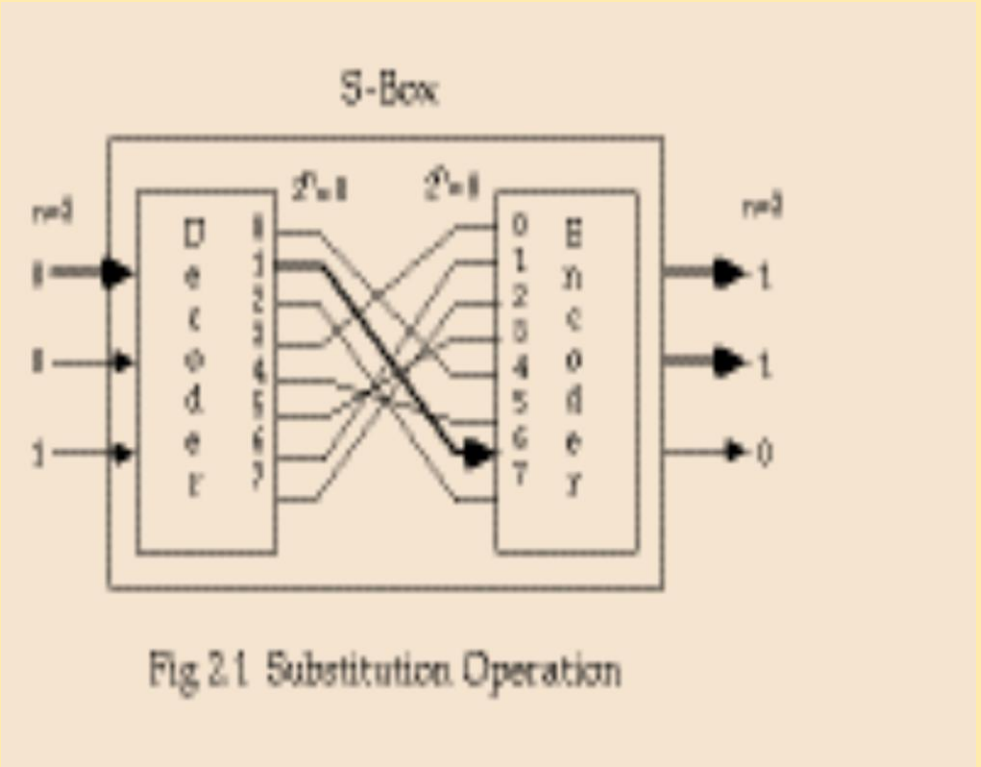
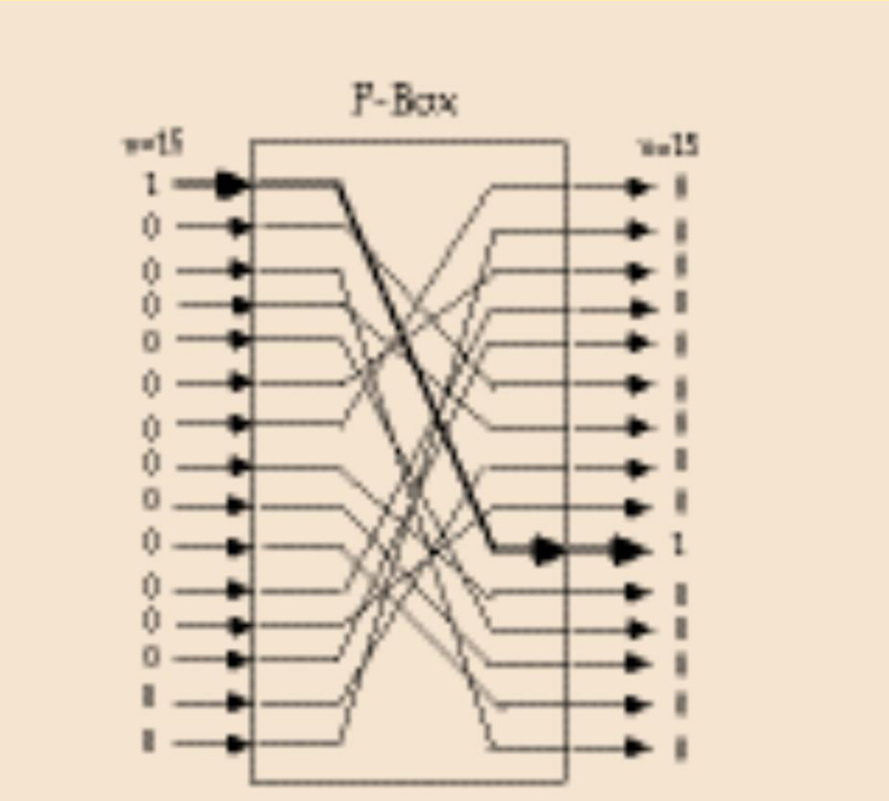


Fig 2.1 Substitution Operation

Permutation Operation

In permutation, the bits of a binary word are rearranged. This operation provides diffusion but is less secure when used alone.



group activity

1- Explain the use of the Feistel structure in cryptography?
2- **What is the main advantage of the Feistel structure?**
3- **Who introduced confusion and diffusion and why are they important?**
4- **How does confusion provide security?**
5- **What is meant by the avalanche effect?**
6- **What does an SP-Network consist of?**
7- **Why are S-boxes used in block cipher design?**

Conclusion

Block ciphers are a fundamental part of modern cryptography. Their security depends on strong algorithms, proper key management, and the effective use of confusion and diffusion. Cryptography must be combined with overall system security to provide full protection.

Background

At **AL-Mustaqbal University**, the registration department maintains an electronic system that stores sensitive student information such as:

- Student names
- University ID numbers
- Grades
- Academic status

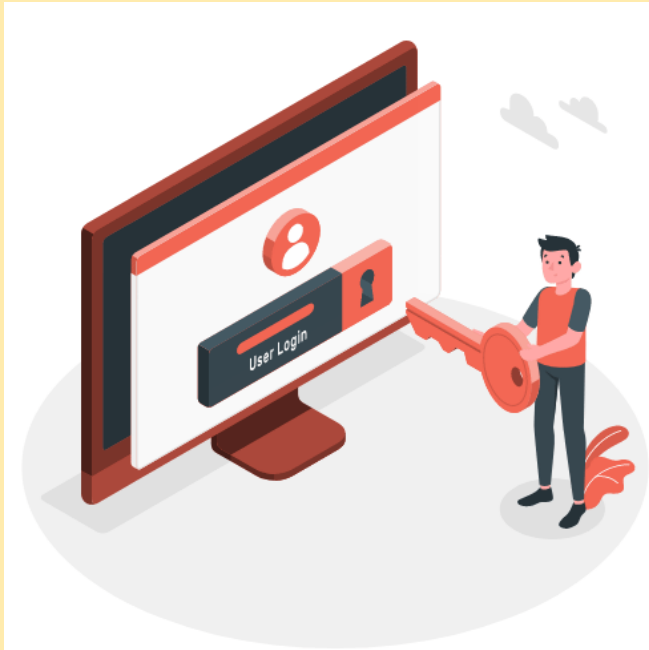
Protecting this data from unauthorized access is a critical requirement.

The Problem

If student data is stored in **plaintext**, any attacker who gains access to the database can:

- Read confidential information
- Modify grades
- Leak student records

Therefore, a secure encryption mechanism is required.




Thank you