# LEC3

## Encryption

- Encryption def.
- Encryption types
- Symmetric (one key) crypto systems
- Asymmetric (two key) crypto systems

2025-2026
Second semester
2026-2-18

Alaa Y. Taqa

# Encryption

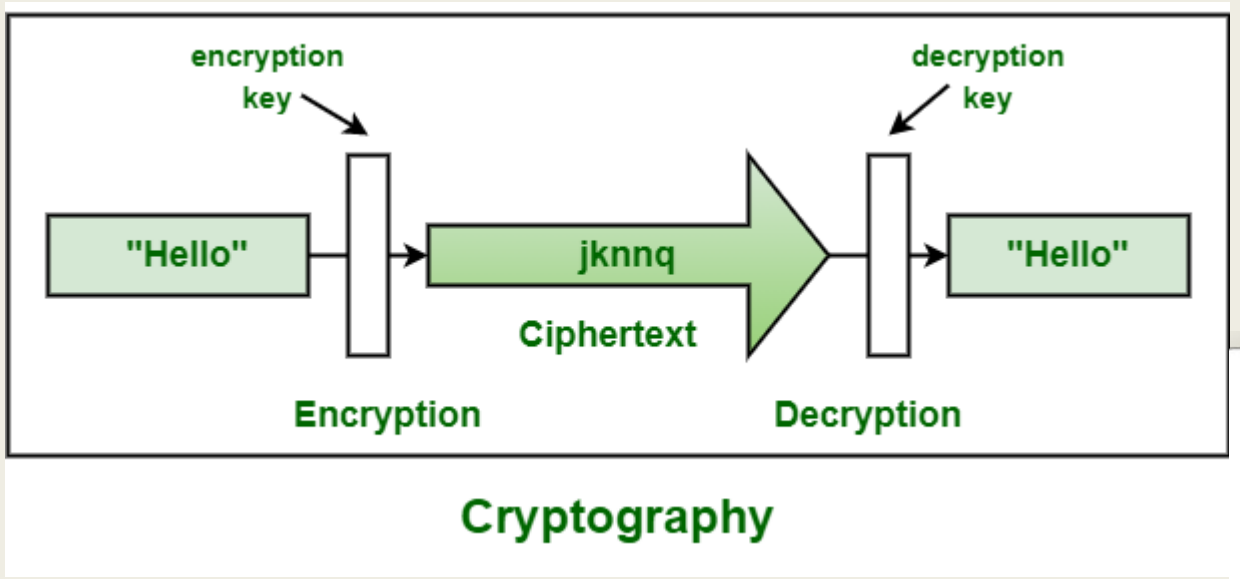
**Encryption** is the process of converting **readable data (plaintext)** into an **unreadable form (ciphertext)** using a mathematical algorithm and a **key**, so that only authorized users can access the original information.

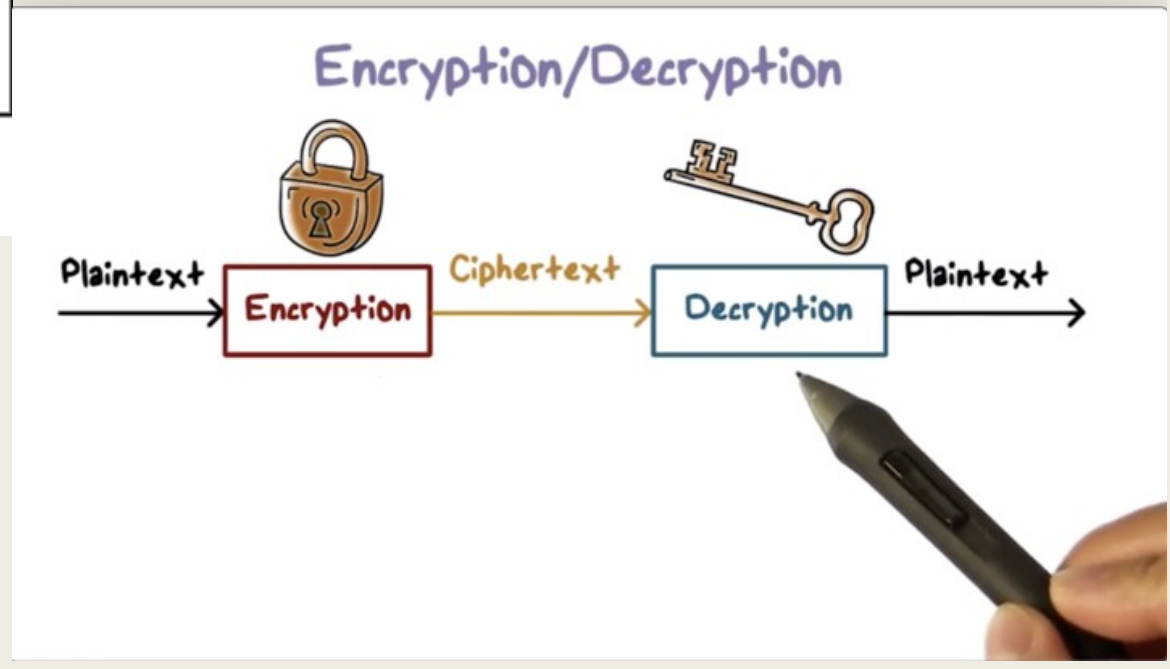
It is a fundamental concept in **Cryptography**, used to protect data confidentiality during storage or transmission.

**Purpose of encryption:**

- Protect sensitive information
- Prevent unauthorized access
- Secure communication over networks
- Ensure privacy and data integrity

Encryption is the overall process of transforming data into an unreadable format (ciphertext) to ensure security, while a cipher is the specific algorithm or set of rules (e.g., AES, RSA) used to perform that transformation

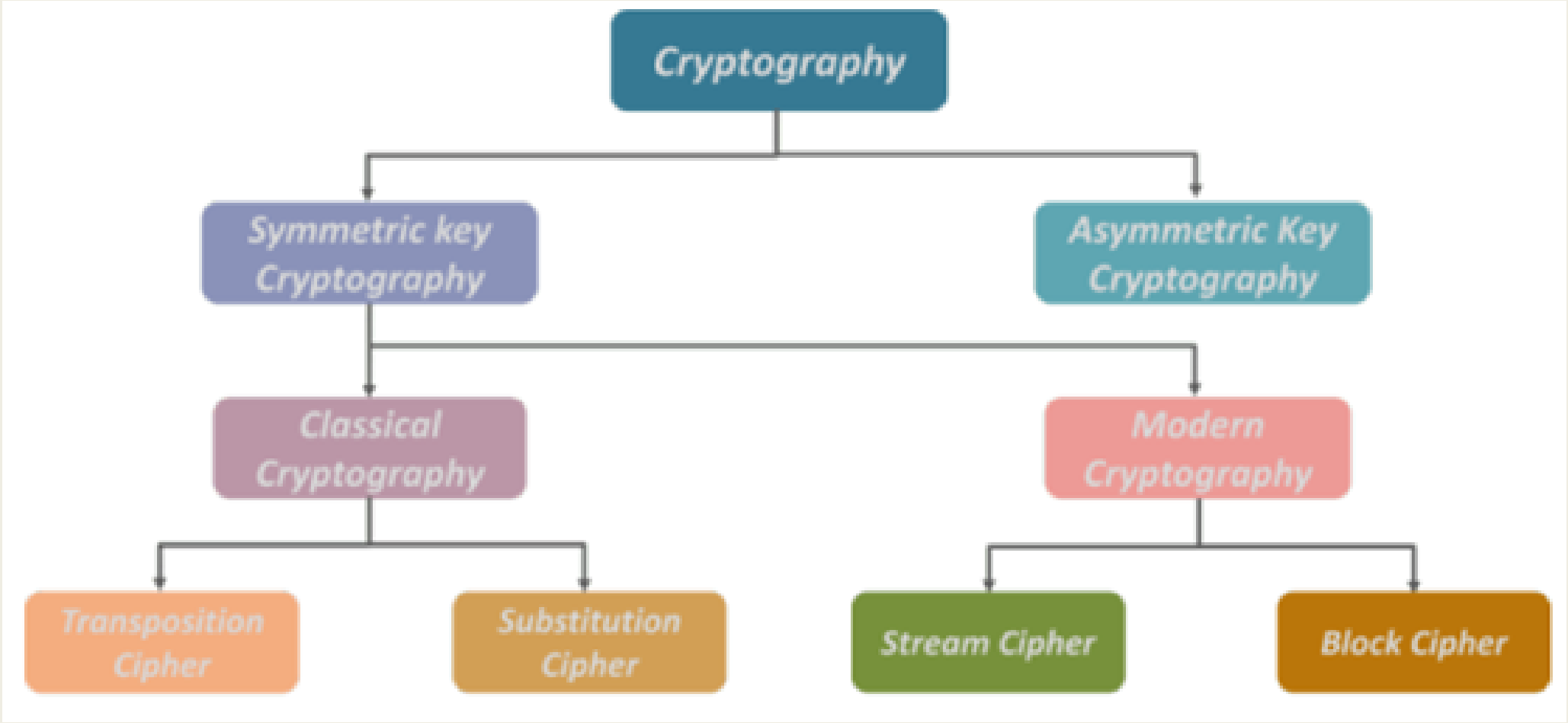


# Types of Encryption Systems

There are **two main types of cryptographic systems:**

**1.Symmetric Key Cryptography (One-Key System)**
**2.Asymmetric Key Cryptography (Two-Key System)**



## Plaintext (Plain Text)

**Plaintext** is the **original readable message** before any encryption is applied. Anyone can understand it easily.

**Example:**

**`HELLO`**

This message is readable and not protected, so it is **plaintext**.

## Ciphertext (Cipher Text)

**Ciphertext** is the **encrypted version of the plaintext** after applying an encryption algorithm. It looks random or meaningless to people who do not have the key.

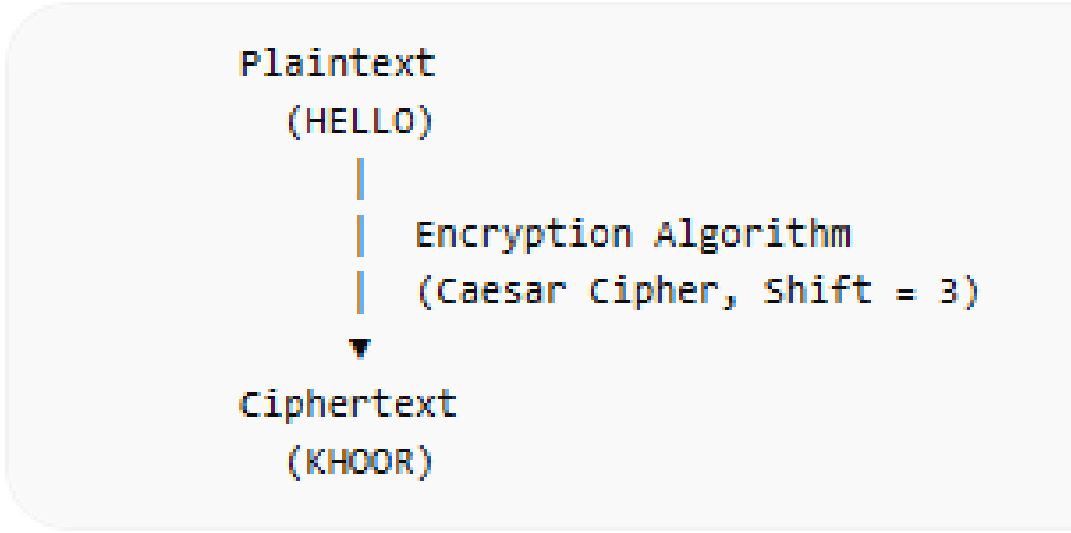
**Example:**

If we encrypt **HELLO** using a simple cipher, it might become:

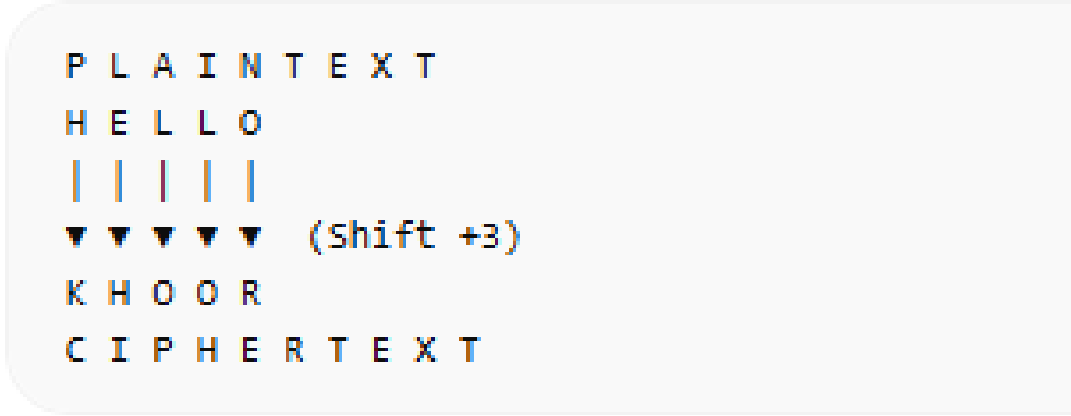
**`KHOOR`**

This encrypted message is **ciphertext**.

## Figure: Plaintext to Ciphertext Process




## Another Simple Visual



## 1. Symmetric Key Cryptography (One Key System)

### Definition

**Symmetric cryptography** is an encryption method where **the same key is used for both encryption and decryption**. Both the **sender and receiver share the same secret key** before communication begins.

### How It Works

1.Sender writes a message (plaintext).
2.The message is encrypted using a **secret key** and an algorithm.
3.The encrypted message becomes **ciphertext**.
4.The receiver uses **the same secret key** to decrypt the ciphertext back into plaintext.

**Plaintext ⟶ Encryption + Secret Key ⟶ Ciphertext**
**Ciphertext ⟶ Decryption + Same Key ⟶ Plaintext**

## Examples of Symmetric Algorithms

- Advanced Encryption Standard (AES)
- Data Encryption Standard (DES)
- Triple DES (3DES)
- Blowfish

## Advantages

✓ Very **fast and efficient**
✓ Suitable for **encrypting large amounts of data**
✓ Requires **less computational power**

## Disadvantages

❌ **Key distribution problem** (sharing the secret key securely)
❌ If the key is **compromised, all communication is exposed**
❌ Not ideal for large networks with many users

## Example Use

- Disk encryption
- Database encryption
- Secure file storage

## Asymmetric Key Cryptography (Two Key System)

### Definition

**Asymmetric cryptography** uses **two different but mathematically related keys**:

1. **Public Key** – shared openly
2. **Private Key** – kept secret by the owner

A message encrypted with one key can **only be decrypted with the other key**.

### How It Works

1. Receiver generates **two keys**: public and private.
2. The **public key is shared** with others.
3. Sender encrypts the message using the **receiver's public key**.
4. Receiver decrypts the message using their **private key**.

**`Plaintext → Encryption + Public Key → Ciphertext`**

**`Ciphertext → Decryption + Private Key → Plaintext`**

**Examples of Asymmetric Algorithms**

- RSA encryption
- Diffie–Hellman key exchange
- Elliptic Curve Cryptography

**Advantages**

✓ **More secure key distribution**

✓ No need to share the private key

✓ Supports **digital signatures and authentication**

**Disadvantages**

❌ **Slower than symmetric encryption**

❌ Requires **more computational resources**

❌ Not efficient for encrypting large data

**Example Use**

- Secure email
- Digital signatures
- SSL/TLS secure websites

| Feature | Symmetric Encryption | Asymmetric Encryption |
| --- | --- | --- |
| Number of Keys | One key | Two keys |
| Key Type | Shared secret key | Public + Private |
| Speed | Fast | Slower |
| Security | Lower for key distribution | Higher |
| Usage | Large data encryption | Key exchange & authentication |


Questions


THANK
YOU