SNS COLLEGE OF ENGINEERING
Kurumbapalayam (Po), Coimbatore – 641 107
AN AUTONOMOUS INSTITUTION
Approved by AICTE, New Delhi and Affiliated to Anna University, Chennai

DEPARTMENT OF CSE (IOT & CS INCLUDING BCT)

Encryption and Decryption

Encryption and **decryption** are the core processes in modern cryptography, used to protect data and ensure secure communication. They are opposite operations, and together they help secure sensitive information, preventing unauthorized access.

1. Encryption:

Encryption is the process of converting **plaintext** (readable data or information) into **ciphertext** (an unreadable format) to protect it from unauthorized access. This is done using an **encryption algorithm** and a **key**. Only someone with the correct key can reverse the process to retrieve the original message.

Purpose of Encryption:

- **Confidentiality**: Ensures that sensitive data is kept private and secure, so only authorized parties can read it.
- **Integrity**: Protects the data from being tampered with during transmission.
- **Authentication**: Verifies that the data comes from a trusted source.

How Encryption Works:

1. **Plaintext**: The original readable message you want to secure.
2. **Encryption Algorithm**: The method used to convert plaintext into ciphertext. The algorithm uses a **key** for the encryption process.
3. **Ciphertext**: The encrypted, unreadable output that results from applying the algorithm to the plaintext.

Example of Encryption:

- Plaintext: **HELLO**
- Key: **3** (for example, shifting each letter by 3 positions in the alphabet)
- Encryption Algorithm: A simple **Caesar Cipher**, where each letter is shifted by 3.

Resulting ciphertext: **KHOOR** (H → K, E → H, L → O, etc.)

2. Decryption:

Decryption is the process of converting **ciphertext** (encrypted data) back into its original **plaintext** form. Decryption requires a specific **decryption key**, which may be the same as the encryption key (in **symmetric encryption**) or different (in **asymmetric encryption**).

Purpose of Decryption:

- **Restoration of Information**: Converts encrypted data back into its readable form so the intended recipient can access and understand the message.
- **Access Control**: Only those who have the correct decryption key can decrypt and view the original message.

How Decryption Works:

1. **Ciphertext**: The encrypted message or data.
2. **Decryption Algorithm**: The method used to reverse the encryption process. The decryption algorithm may use the same key as encryption (in symmetric encryption) or a different key (in asymmetric encryption).
3. **Plaintext**: The decrypted original message.

Example of Decryption:

- Ciphertext: **KHOOR**
- Key: **3** (same as the encryption key)
- Decryption Algorithm: Using the same Caesar Cipher but shifting in the opposite direction (back by 3).

Resulting plaintext: **HELLO** (K → H, H → E, O → L, etc.)

3. Types of Encryption:

Symmetric Encryption (Secret Key Encryption):

In symmetric encryption, the same key is used for both encryption and decryption. Both the sender and the recipient must share the secret key securely.

- **Example Algorithms**: AES (Advanced Encryption Standard), DES (Data Encryption Standard), 3DES (Triple DES).
- **Advantages**: Faster than asymmetric encryption and efficient for large amounts of data.
- **Challenges**: Secure key distribution is a problem, as both parties must have the same key without it being intercepted.

Asymmetric Encryption (Public Key Encryption):

In asymmetric encryption, two different keys are used: a **public key** for encryption and a **private key** for decryption. The public key is freely shared, while the private key is kept secret by the recipient.

- **Example Algorithms**: RSA, ECC (Elliptic Curve Cryptography).
- **Advantages**: Solves the key distribution problem of symmetric encryption. Even if the public key is intercepted, only the private key can decrypt the message.
- **Challenges**: Slower than symmetric encryption and computationally more expensive.