

## Cryptography & Network Security

### 1) What is Cryptography?

➔ Cryptography is the science of securing information by converting it into an unreadable format so that only authorized people can access it.

#### 💡 Example:

- When you send a WhatsApp message, it is encrypted (scrambled into a secret code) so that no one except the recipient can read it.
- Main Purpose of Cryptography:
  - ✓ Confidentiality – Keeps information secret.
  - ✓ Integrity – Ensures data is not altered.
  - ✓ Authentication – Verifies sender and receiver identities.
  - ✓ Non-Repudiation – Prevents denial of actions (digital signatures).

### 2) What is Network Security?

➔ Network Security protects data, devices, and communication in a network from cyber threats like hacking, viruses, and unauthorized access.

#### 💡 Example:

- When you shop online, websites use SSL/TLS encryption (HTTPS) to protect your credit card details from hackers.
- Firewalls block unauthorized access to a company's internal network.
- Main Goals of Network Security:
  - ✓ Prevent Attacks – Protects networks from hackers and malware.
  - ✓ Secure Communication – Ensures safe data transfer between devices.
  - ✓ Control Access – Restricts unauthorized users from accessing sensitive data.

### 3) Difference Between Cryptography & Network Security.

Feature	Cryptography	Network Security
Definition	Encrypts data to keep it secret.	Protects the entire network from threats.
Focus	Securing data (files, messages).	Securing data transmission (network traffic).
Example	WhatsApp encryption, Password hashing.	Firewalls, Antivirus, VPNs.
Main Threats	Brute force, Cryptanalysis attacks.	Hacking, DDoS, Phishing.

#### 4) Real-World Example of Cryptography & Network Security.

##### Online Banking Transaction.

- Cryptography encrypts your password and transaction details.
- Network Security ensures your data is safely transmitted over the internet and prevents hackers from intercepting it.


#### 5) Types of cryptography in detail.

- 1) Symmetric Key Cryptography
- 2) Asymmetric Key Cryptography

##### ✓ Symmetric Key Cryptography

- **Definition:** In symmetric key cryptography, the same key is used for both encryption and decryption.
- Symmetric Key Cryptography, also known as secret-key cryptography, is a cryptographic system that uses a single key for both encryption and decryption. It is one of the oldest and simplest forms of cryptography.

##### ❖ How It Works:

- **Encryption:** The sender uses a secret key to convert plaintext (original message) into ciphertext (encrypted message).
- **Decryption:** The receiver uses the same secret key to convert the ciphertext back into plaintext.
-  **Note:** -The same key must be securely shared between the sender and receiver before communication begins.

##### ❖ Key Features:

- **Single Key:** One key is used for both encryption and decryption.
- **Efficiency:** Symmetric encryption algorithms are faster than asymmetric ones, making them suitable for encrypting large amounts of data.
- **Security Dependency:** The system's security relies heavily on keeping the secret key confidential. If the key is exposed, the system is compromised.
- **Suitable for Bulk Data:** Ideal for encrypting large files, databases, and real-time communication.

### ❖ Advantages:

- **Speed:**
  - Symmetric key algorithms are computationally faster than asymmetric cryptography.
- **Simplicity:**
  - Simple mathematical operations make it easier to implement.

### ❖ Disadvantages:

- **Key Distribution Problem:**
  - The secret key must be securely shared between the sender and receiver, which can be challenging in large-scale systems.
- **Scalability Issues:**
  - In a network with  $n$  users,  $n(n-1)/2$  keys are needed for secure communication between all pairs.
- **Lack of non-repudiation:**
  - Since the same key is used by both parties, it's impossible to prove who encrypted or decrypted the message.

### ❖ Applications:

- File Encryption.
- Database Encryption.
- Network Security.
- Wireless Security.

### ✓ Asymmetric Key Cryptography

- Asymmetric Key Cryptography, also known as public-key cryptography, is a cryptographic system that uses two mathematically related keys: a public key and a private key.
- These keys work in pairs, where:
  - The public key is used for encryption and can be freely shared.
  - The private key is used for decryption and must be kept secret.

### ❖ How It Works:

- **Encryption:**

- The sender encrypts the plaintext using the recipient's public key.
- The encrypted message (ciphertext) can only be decrypted using the recipient's private key.

- **Decryption:**

- The recipient uses their private key to decrypt the ciphertext back into plaintext.

- **Digital Signatures:**

- A sender can sign a message using their private key.
- The recipient can verify the signature using the sender's public key, ensuring the authenticity and integrity of the message.

### ❖ Key Features:

- **Two Keys:** One public key (freely shared) and one private key (kept secret).
- **No Key Distribution Problem:** Public keys can be openly distributed, eliminating the risk of exposure during key exchange.
- **Security:** Based on computationally hard mathematical problems (e.g., factoring large numbers, discrete logarithms, or elliptic curve problems).
- **Slower Performance:** Computationally slower compared to symmetric key cryptography due to complex mathematical operations.
- **Scalability:** Ideal for large-scale systems since only public keys need to be exchanged.

### ❖ Advantages:

- **No Shared Secret:**

- Public keys can be shared openly, eliminating the risk of key compromise during exchange.

- **Scalability:**

- Easier to manage in large-scale systems, as each user only needs one key pair.

- **Enables Digital Signatures:**

- Provides authentication, non-repudiation, and integrity verification.

❖ **Disadvantages:**

- **Slower than Symmetric Cryptography:**

- Asymmetric algorithms require more computational power, making them less suitable for bulk data encryption.

- **Key Management Complexity:**

- While public keys can be shared freely, private keys require secure storage.

❖ **Applications:**

- Secure Communication.
- Digital Signatures.
- Email Encryption.
- Key Exchange.
- Blockchain and Cryptocurrencies.
- Authentication Systems.

Tanay Mahale