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)

16 Marks Questions

1. **Introduction to Security, The Need for Security, and Security Approaches**

   Introduction to Security:
   Security encompasses a range of measures to protect data, systems, and networks from threats such as unauthorized access, manipulation, and destruction. It includes confidentiality, integrity, and availability of information.

   The Need for Security:
   The reliance on digital systems for communication, commerce, and data storage has made information security crucial. Data breaches, cyber-attacks, and privacy violations threaten the integrity of information and systems. Hence, security measures are needed to protect sensitive data from malicious threats and unauthorized access, ensuring confidentiality, integrity, and availability.

   Security Approaches:
   There are three primary approaches to implementing security:

   1. **Preventive Measures**: Aimed at preventing attacks and minimizing risks (e.g., using encryption, firewalls, access control).
   2. **Detective Measures**: Tools used to detect and alert on security breaches (e.g., intrusion detection systems, activity logs).

3. **Corrective Measures**: Actions taken to recover from security breaches or incidents (e.g., restoring from backups, patching vulnerabilities).

2. **Principles of Security and Types of Security Attacks**

   Principles of Security:
   The basic principles of security include:

   - **Confidentiality**: Ensures that data is only accessible to those authorized to view it.
   - **Integrity**: Ensures that data remains accurate and unaltered during transmission or storage.
   - **Availability**: Ensures that systems and data are accessible and functional when required by authorized users.
   - **Authentication**: Verifies the identity of users, systems, or entities.
   - **Non-repudiation**: Ensures that an entity cannot deny the validity of its actions or data.

   Types of Security Attacks:

   - **Passive Attacks**: Involve unauthorized monitoring or interception of data without modifying it (e.g., eavesdropping).
   - **Active Attacks**: Involve altering or disrupting data or systems (e.g., man-in-the-middle, denial of service attacks).
   - **Internal Attacks**: Attacks originating from within an organization, such as employees misusing access.
   - **External Attacks**: Attacks from outside the organization, often by hackers or cybercriminals.

3. **Security Services, Security Mechanisms, and Cryptography**

   Security Services:
   Security services provide protection to ensure secure communications and operations. These include:

- **Confidentiality**: Ensuring data is kept secret from unauthorized users.
- **Integrity**: Ensuring data is not altered during transmission.
- **Authentication**: Verifying the identities of users or systems.
- **Non-repudiation**: Preventing denial of actions taken.
- **Access Control**: Restricting access to sensitive information or systems.

Security Mechanisms:
Security mechanisms are the tools or techniques used to implement security services:

- **Encryption**: Converts data to an unreadable form, protecting confidentiality.
- **Hashing**: Provides data integrity by generating a unique hash for data.
- **Firewalls**: Control network access to prevent unauthorized connections.
- **Digital Signatures**: Ensure authenticity and integrity of messages.

Cryptography:
Cryptography protects information through techniques such as encryption and decryption. There are two main types of cryptography:

- **Symmetric Key Cryptography**: The same key is used for both encryption and decryption.
- **Asymmetric Key Cryptography**: Different keys are used for encryption (public key) and decryption (private key).

4. **Plaintext and Ciphertext, Substitution and Transposition Techniques**

Plaintext and Ciphertext:

- **Plaintext**: The original, unencrypted message or data.
- **Ciphertext**: The encrypted version of plaintext, which is unreadable without the correct decryption key.

Substitution Techniques:
Substitution ciphers replace each letter in the plaintext with another letter or symbol. Common examples include:

- **Caesar Cipher**: Shifts the letters in the plaintext by a certain number of positions in the alphabet.

Transposition Techniques:
Transposition ciphers rearrange the order of characters in the plaintext while preserving the original letters. Examples include:

- **Rail Fence Cipher**: The plaintext is written in a zigzag pattern, and then read off row by row to create the ciphertext.

Encryption and Decryption:

- **Encryption**: The process of converting plaintext into ciphertext using a cryptographic algorithm and key.
- **Decryption**: The process of converting ciphertext back into plaintext using the decryption key.