DEPARTMENT OF CSE (IOT & CS INCLUDING BCT)

Introduction to Security:
Security refers to the measures taken to protect systems, networks, and data from unauthorized access, misuse, modification, or destruction. It ensures the confidentiality, integrity, and availability of information.

1. **The Need for Security**:
   The need for security arises from the increased reliance on digital communication and data storage, making systems vulnerable to threats like hacking, data breaches, and unauthorized access. It is necessary to protect sensitive data and maintain trust in systems.
2. **Security Approaches**:
   Security approaches include:
   - **Preventive**: Measures taken to prevent attacks (e.g., firewalls, encryption).
   - **Detective**: Tools to identify attacks as they occur (e.g., intrusion detection systems).
   - **Corrective**: Actions taken to recover from security incidents (e.g., patching vulnerabilities).
3. **Principles of Security**:
   The key principles of security are:
   - **Confidentiality**: Protecting information from unauthorized access.
   - **Integrity**: Ensuring data is accurate and unaltered.
   - **Availability**: Ensuring that data and services are accessible when needed.
   - **Authentication**: Verifying the identity of users and systems.

- **Non-repudiation**: Ensuring that actions or data cannot be denied after they occur.

4. **Types of Security Attacks**:
   - **Passive Attacks**: Involve unauthorized surveillance or eavesdropping (e.g., traffic analysis).
   - **Active Attacks**: Modify data or disrupt systems (e.g., denial of service, man-in-the-middle).
   - **Internal Attacks**: Attacks originating from within the organization.
   - **External Attacks**: Attacks from outside the organization (e.g., hacking).
5. **Security Services**:
   Security services include:
   - **Confidentiality**: Protecting data from unauthorized access.
   - **Integrity**: Ensuring data has not been tampered with.
   - **Authentication**: Verifying the identity of entities.
   - **Non-repudiation**: Ensuring actions cannot be denied.
   - **Availability**: Ensuring systems are accessible when needed.
6. **Security Mechanisms**:
   Security mechanisms are tools to implement security services. Examples:
   - **Encryption**: Converts plaintext to ciphertext to ensure confidentiality.
   - **Hashing**: Ensures data integrity.
   - **Firewalls**: Prevent unauthorized access to networks.
   - **Digital Signatures**: Verify the authenticity of a message.
7. **Cryptography**
   Cryptography is the science of protecting information by transforming it into an unreadable format (ciphertext). It is used to ensure confidentiality, integrity, authentication, and non-repudiation.
8. **Plaintext and Ciphertext**:
   - **Plaintext**: Original readable data that needs protection.
   - **Ciphertext**: The encrypted, unreadable form of the plaintext.
9. **Substitution Techniques**:
   Substitution ciphers replace each character in the plaintext with

another character (e.g., Caesar Cipher, where each letter is shifted by a fixed number).

10. **Transposition Techniques**: Transposition ciphers rearrange the order of characters in the plaintext to hide the original message (e.g., Rail Fence Cipher).
11. **Encryption and Decryption**:
    - **Encryption**: Converting plaintext to ciphertext using an algorithm and key.
    - **Decryption**: Converting ciphertext back to plaintext using the corresponding key.