Introduction to Cryptography, Cryptosystem, Cryptanalysis, Security Services

1. Cryptography

- **What is Cryptography?**
    - The science of securing communication and data by converting it into a format that only authorized parties can understand.
    - Derived from Greek words:
        - **Kryptos** (hidden) + **Graphein** (to write).
    - Used to ensure **confidentiality, integrity, and authenticity** of data.
- **Key Terms:**
    - **Plaintext:** Original message (readable format).
    - **Ciphertext:** Encrypted message (unreadable format).
    - **Encryption:** Process of converting plaintext to ciphertext.
    - **Decryption:** Process of converting ciphertext back to plaintext.
    - **Key:** A secret value used for encryption and decryption.

---

2. Cryptosystem

- **What is a Cryptosystem?**
    - A system that uses cryptography to secure communication.
    - Includes:
        - Algorithms for encryption and decryption.
        - Keys for securing data.
        - Protocols for secure communication.
- **Components of a Cryptosystem:**
    1. **Plaintext:** The original message.
    2. **Ciphertext:** The encrypted message.
    3. **Encryption Algorithm:** Converts plaintext to ciphertext.

4. **Decryption Algorithm:** Converts ciphertext back to plaintext.
5. **Key:** A secret value used in encryption and decryption.

- **Types of Cryptosystems:**
  1. **Symmetric Key Cryptography:**
     - Uses the **same key** for encryption and decryption.
     - Example: AES (Advanced Encryption Standard).
  2. **Asymmetric Key Cryptography:**
     - Uses a **pair of keys** (public key and private key).
     - Example: RSA (Rivest-Shamir-Adleman).

---

3. Cryptanalysis

- **What is Cryptanalysis?**
  - The study of breaking cryptographic systems to uncover plaintext or keys without authorization.
  - Also known as **code-breaking**.
- **Goals of Cryptanalysis:**
  - Find weaknesses in cryptographic algorithms.
  - Recover plaintext or keys from ciphertext.
  - Improve the security of cryptographic systems.
- **Types of Cryptanalysis Attacks:**
  1. **Brute Force Attack:** Trying all possible keys to decrypt the message.
  2. **Frequency Analysis:** Analyzing patterns in ciphertext to guess the plaintext.
  3. **Man-in-the-Middle Attack:** Intercepting and altering communication between two parties.
  4. **Known Plaintext Attack:** Attacker knows some plaintext-ciphertext pairs to guess the key.

---

4. Security Services

- **What are Security Services?**
    - Services provided by cryptography to ensure secure communication and data protection.
- **Types of Security Services:**
    1. **Confidentiality:**
        - Ensures data is accessible only to authorized users.
        - Achieved through **encryption**.
    2. **Integrity:**
        - Ensures data is not altered or tampered with during transmission.
        - Achieved through **hashing** and **digital signatures**.
    3. **Authentication:**
        - Verifies the identity of users or systems.
        - Achieved through **passwords, biometrics, or digital certificates**.
    4. **Non-Repudiation:**
        - Ensures a sender cannot deny sending a message.
        - Achieved through **digital signatures**.
    5. **Availability:**
        - Ensures data and systems are accessible when needed.
        - Achieved through **backups** and **redundancy**.

---

5. Security Mechanisms

- **What are Security Mechanisms?**
    - Tools and techniques used to implement security services.
- **Types of Security Mechanisms:**

1. **Encryption:**
    - Converts plaintext to ciphertext to ensure confidentiality.
2. **Digital Signatures:**
    - Provides integrity, authentication, and non-repudiation.
3. **Hashing:**
    - Converts data into a fixed-size value (hash) to ensure integrity.
4. **Access Control:**
    - Restricts access to data based on user roles (e.g., passwords, biometrics).
5. **Firewalls:**
    - Blocks unauthorized access to networks.
6. **Intrusion Detection Systems (IDS):**
    - Monitors networks for suspicious activity.

Summary Table

Topic	**Key Points**
Cryptography	Secures communication by converting data into unreadable formats.
Cryptosystem	Includes algorithms, keys, and protocols for encryption and decryption.
Cryptanalysis	The study of breaking cryptographic systems to uncover plaintext or keys.
Security Services	Confidentiality, Integrity, Authentication, Non-Repudiation, Availability.
Security Mechanisms	Encryption, Digital Signatures, Hashing, Access Control, Firewalls, IDS.