Q1) Cryptanalytic Attacks: Known Plaintext, Chosen Plaintext, Ciphertext-Only and Chosen Ciphertext

Ans - In cryptography, an attacker attempts to break an encryption system by analyzing the relationship between plaintext and ciphertext. Depending on the amount of information available to the attacker, cryptanalytic attacks are classified into four major types:

- Ciphertext-Only Attack (COA)
- Known Plaintext Attack (KPA)
- Chosen Plaintext Attack (CPA)
- Chosen Ciphertext Attack (CCA)

These attacks differ in the level of power given to the attacker.

1. Ciphertext-Only Attack (COA)

In a Ciphertext-Only Attack, the attacker has access only to the intercepted ciphertext. The corresponding plaintext and encryption key are unknown.

Characteristics:

- Most restrictive attack model.
- Attacker relies on statistical analysis and patterns.
- Applicable to classical ciphers with predictable frequency distributions.

Example:

In classical substitution ciphers, attackers exploit frequency analysis (e.g., letter ‘E’ is most common in English).

Objective:

Recover the plaintext or deduce the encryption key.

Modern encryption algorithms like AES are designed to be secure even if attackers obtain unlimited ciphertext.

---

2. Known Plaintext Attack (KPA)

In a Known Plaintext Attack, the attacker has access to some plaintext and its corresponding ciphertext.

Characteristics:

- Attacker analyzes known plaintext–ciphertext pairs.

- Helps reveal key patterns or weaknesses.
- Stronger than ciphertext-only attack.

Example:

Breaking the **Enigma machine** during World War II involved using predictable message headers as known plaintext.

Objective:

Use known mappings to recover the secret key and decrypt other ciphertexts.

---

3. Chosen Plaintext Attack (CPA)

In a Chosen Plaintext Attack, the attacker can choose arbitrary plaintexts and obtain their corresponding ciphertexts.

Characteristics:

- More powerful than KPA.
- Attacker selects specially crafted inputs.
- Used to test structural weaknesses.

Practical Relevance:

Modern encryption schemes must be secure against CPA. For example, improper implementations of **RSA** without padding are vulnerable.

Objective:

Discover key information or predict ciphertext outputs for other plaintexts.

CPA security is considered a minimum requirement for modern encryption schemes.

---

4. Chosen Ciphertext Attack (CCA)

In a Chosen Ciphertext Attack, the attacker can choose ciphertexts and obtain their decrypted plaintexts.

Characteristics:

- Most powerful attack model.
- Attacker interacts with a decryption oracle.
- Exploits error messages, timing information, or padding validation.

Real-World Example:

Padding oracle vulnerabilities in **Transport Layer Security** are examples of CCA.

Objective:

Recover the secret key or decrypt other ciphertexts without authorization.

Modern secure systems aim to achieve CCA-security (IND-CCA secure).

Comparison of Attack Types

Attack Type	Attacker Access	Strength Level
Ciphertext-Only	Only ciphertext	Weakest
Known Plaintext	Plaintext–ciphertext pairs	Moderate
Chosen Plaintext	Can choose plaintext	Strong
Chosen Ciphertext	Can choose ciphertext	Strongest

Q2) Explain Side channel attacks

A **side channel attack** is a type of cryptographic attack that exploits physical or implementation-related information leaked by a system rather than breaking the mathematical algorithm itself.

Instead of attacking the encryption algorithm directly, the attacker gathers information from **physical characteristics** such as:

- **Execution time**
- **Power consumption**
- **Electromagnetic emissions**
- **Cache behavior**
- **Sound**

Thus, even a mathematically secure algorithm can be compromised due to implementation weaknesses.

Basic Concept

When a cryptographic algorithm runs on a computer or hardware device, it consumes time, power, and memory in ways that may depend on the secret key. These unintended leakages are called **side channels**.

An attacker measures these leakages and uses statistical analysis to recover secret keys.

Types of Side Channel Attacks

---

1. Timing Attacks: Timing attacks measure the time taken by an algorithm to perform encryption or decryption.

2. Power Analysis Attacks: Power attacks analyze the power consumption of a device during cryptographic operations.

3. Cache Attacks: These attacks exploit shared CPU cache behavior.

4. **Electromagnetic (EM) Attacks:** Devices emit electromagnetic radiation during computation.

5. Fault Injection Attacks: Attacker intentionally introduces faults by: Voltage glitching**,** Clock manipulation**,** Laser injection

Q) Explain active and passive attacks

In network security, attacks are broadly classified into **Passive Attacks** and **Active Attacks** based on whether the attacker only monitors communication or actively alters it.

- **Passive attacks** involve unauthorized monitoring of data.
- **Active attacks** involve modification, disruption, or destruction of data.

1. Passive Attacks

A passive attack is an attack in which an unauthorized party monitors or intercepts communication without altering the data.

The primary objective is to obtain information without being detected.

Characteristics

- No modification of data.
- Difficult to detect.
- Focus on breaching confidentiality.
- Prevention is easier than detection.

2. Active Attacks

Definition

An active attack is an attack where the attacker modifies, disrupts, deletes, or injects data into communication channels.

The goal is to compromise integrity, authenticity, or availability.

Characteristics

- Data is altered or system operation is affected.
- Easier to detect than passive attacks.
- More damaging in nature.

Q) Layers of Cryptography: End-to-End Encryption vs Hop-by-Hop Encryption

1. End-to-End Encryption (E2EE)

Definition

End-to-End Encryption is a method in which data is encrypted at the sender's device and decrypted only at the final receiver's device.

Intermediate nodes (routers, servers, ISPs) cannot read or modify the encrypted content.

Working

- Sender encrypts message using a key.
- Encrypted data travels through multiple intermediate nodes.
- Only the receiver has the key to decrypt it.
- Intermediate systems forward encrypted data but cannot access the content.

Examples

- **WhatsApp** messages
- **Signal**
- Secure email systems
- Encrypted messaging apps

Advantages

- High confidentiality
- No trust required in intermediate nodes
- Protects against insider attacks

Disadvantages

- Harder for authorities to inspect traffic
- Key management is complex
- No content-level monitoring by service provider

2. Hop-by-Hop Encryption

Definition

In Hop-by-Hop Encryption, data is encrypted between two consecutive nodes in a communication path.

Each intermediate node decrypts the message and re-encrypts it before sending it to the next node.

Working

- Sender encrypts data for the next node.
- Intermediate node decrypts it.
- Re-encrypts before forwarding.
- Process repeats until it reaches final destination.

Examples

- **Transport Layer Security** between browser and server
- VPN tunnels between endpoints
- Secure links in corporate networks

Advantages

- Easier monitoring and filtering
- Effective for securing network infrastructure
- Simpler key management per link

Disadvantages

- Intermediate nodes can access plaintext
- Requires trust in every node
- Higher risk of data exposure inside network

Q) Covert Channel

A **covert channel** is a communication path that allows two entities to transfer information in a way that violates a system's security policy.

It uses system resources that were **not intended for information transfer**, thereby bypassing normal security controls such as access restrictions and mandatory access control systems.

In simple terms, a covert channel is a *hidden communication method* that breaks security rules.

Q) CIA Triad

1. Confidentiality

Confidentiality ensures that information is accessible only to authorized individuals and is protected from unauthorized disclosure.

It prevents sensitive data from being exposed to attackers or unauthorized users.

How to Achieve Confidentiality

1. **Encryption**
    - Use strong encryption algorithms like **Advanced Encryption Standard**
    - Secure communication protocols such as **Transport Layer Security**
2. **Access Control Mechanisms**
    - Authentication (passwords, biometrics, MFA)
    - Authorization policies
3. **Data Classification**
    - Public, private, confidential levels
4. **Network Security**
    - Firewalls
    - VPNs

2. Integrity

Integrity ensures that data remains accurate, consistent, and unaltered during storage or transmission.

It prevents unauthorized modification or tampering.

How to Achieve Integrity

1. **Hash Functions**
   - Using cryptographic hash algorithms like **SHA-256**
2. **Message Authentication Codes (MAC)**
3. **Digital Signatures**
   - Public-key techniques such as **RSA**
4. **Access Controls**
   - Prevent unauthorized changes
5. **Version Control & Backup Systems**

3. Availability

Availability ensures that systems and data are accessible to authorized users whenever required.

It protects against service disruption.

How to Achieve Availability

1. **Redundancy**
   - Backup servers
   - Load balancing
2. **Regular System Maintenance**
   - Updates and patch management
3. **Protection Against Denial of Service (DoS)**
4. **Disaster Recovery Plans**
   - Data backups
   - Business continuity planning