CNS-2025-May-PYQ

Q1. [20 Marks]

a. Explain the CIA triad.

b. Explain the structure and purpose of an X.509 digital certificate.

c. What is the purpose of Trojan horse and backdoor?

d. Explain the working of a Virtual Private Network (VPN) and its security benefits.

Q2. [10 Marks]

a. Given a 5×5 grid and the keyword "PLAYFAIR", encrypt the message "HIDE" using the Playfair cipher. Demonstrate the steps and the final ciphertext.

b. Explain the working of SHA-256 using suitable example.

Q3. [10 Marks]

a. What is a SPAM? Explain different types of SPAMs.

b. What is the significance of IPSec? Explain the different modes of operation in IPSec?

Q4. [10 Marks]

a. Explain the various use cases of NAC.

b. Explain the different types of IDS.

Q5. [10 Marks]

a. What are the characteristics of a firewall?

b. What are the steps involved in implementing NAC solutions?

Q6. [20 Marks]

a. Write short notes on:

i. HMAC and CMAC

ii. S/MIME

iii. RSA Algorithm

v. OSI Security Architecture

vi. HTTPS

Q1. [20 Marks] - Answers

a. Explain the CIA triad.

CIA Triad (Confidentiality, Integrity, Availability)

The **CIA Triad** is the fundamental model of information security that defines three key principles used to protect data and systems.

1. **Confidentiality**
   - Ensures that information is accessible **only to authorized users**.
   - Protects data from **unauthorized access or disclosure**.
   - Techniques: Encryption, authentication, and access control mechanisms.

2. **Integrity**
   - Ensures that data is **accurate, consistent, and unaltered** during storage or transmission.
   - Prevents **unauthorized modification** of data.
   - Techniques: Hashing, digital signatures, and checksums.

3. **Availability**

- Ensures that data and systems are **accessible to authorized users whenever needed**.
- Protects against **downtime, hardware failure, or denial-of-service (DoS) attacks**.
- Techniques: Redundancy, backups, and fault-tolerant systems.

4. **Goal of CIA Triad**
    - Maintain a balanced approach between all three principles to ensure **overall security** of information systems.

Example:

Online banking systems must ensure user data confidentiality (encryption), transaction integrity (hashing), and service availability (backup servers).

b. Explain the structure and purpose of an X.509 digital certificate.

X.509 Digital Certificate

An **X.509 digital certificate** is a standard format used to verify the **identity of entities** (like websites, users, or organizations) and establish **secure communication** over networks.

Purpose

- Authenticates the **identity** of an entity.
- Enables **secure communication** using **public key cryptography**.
- Helps establish **trust** in **SSL/TLS** connections (e.g., HTTPS websites).
- Prevents **man-in-the-middle** and **spoofing** attacks.

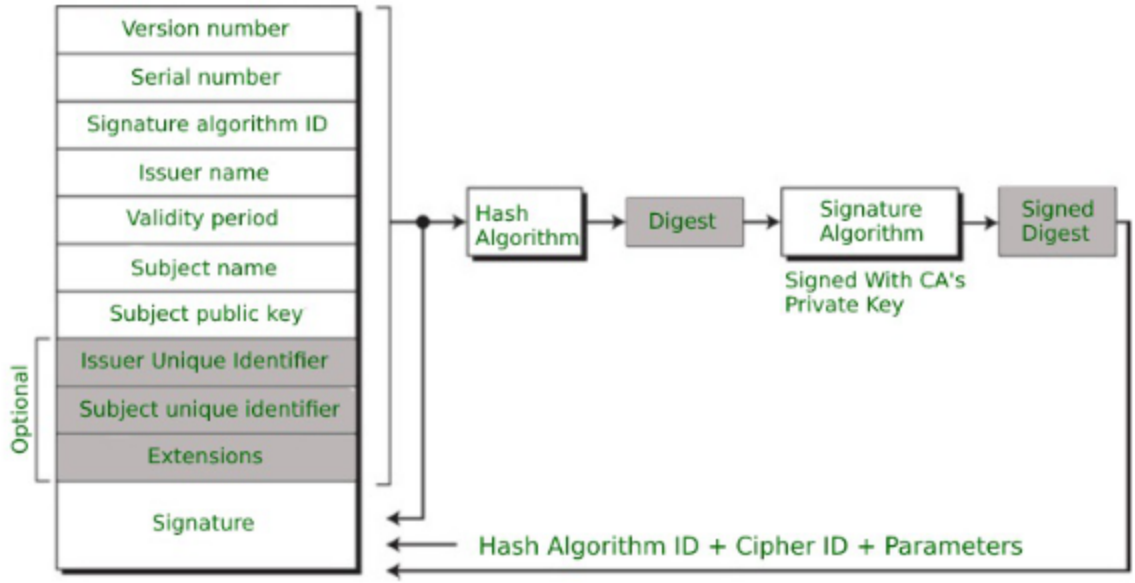
Structure of X.509 Certificate

1. **Version**
    - Indicates the certificate format version (v1, v2, or v3).
2. **Serial Number**
    - Unique identifier assigned by the Certificate Authority (CA).
3. **Signature Algorithm**
    - Specifies the algorithm (e.g., SHA256 with RSA) used for signing the certificate.
4. **Issuer Name**
    - The trusted **Certificate Authority (CA)** that issued the certificate.
5. **Validity Period**
    - Defines the **start and expiry date** of the certificate.
6. **Subject Name**
    - The **owner's identity** (person, organization, or domain name).
7. **Subject Public Key Info**
    - Contains the **public key** and the algorithm associated with it.
8. **Extensions (v3)**
    - Additional information like **key usage**, **certificate policies**, and **subject alternative names**.
9. **Digital Signature**
    - Signature by the CA to ensure **authenticity and integrity**.

Example:

When you visit `https://www.google.com`, your browser verifies Google's **X.509 certificate** issued by a trusted CA to ensure that the site is genuine and the connection is encrypted.

Structure of X.509 Certificate diagram:



c. What is the purpose of Trojan horse and backdoor?

1. Trojan Horse

- A **malicious program disguised as legitimate software**.
- Tricks users into installing it, giving attackers access to their systems.
- Purpose:
  - **Steal sensitive data** (passwords, banking info).
  - **Install additional malware** or create a backdoor.
  - **Control or monitor** the victim's computer remotely.
  - **Damage or modify files** without the user's knowledge.
- Example: A fake game or utility that secretly installs malware in the background.

---

2. Backdoor

- A **hidden entry point** in a system or application that allows bypassing normal authentication.
- Often created by attackers (or sometimes developers for maintenance).
- Purpose:
  - **Gain unauthorized remote access** to the system.
  - **Control the infected machine** without detection.
  - **Steal or manipulate data** anytime after the initial compromise.
- Example: After a Trojan infection, a backdoor may be installed to allow continued access even after antivirus removal.

d. Explain the working of a Virtual Private Network (VPN) and its security benefits.

Virtual Private Network (VPN)

A **VPN** creates a **secure, encrypted connection (tunnel)** between a user's device and a remote network over the internet, ensuring **privacy and security** of data transmission.

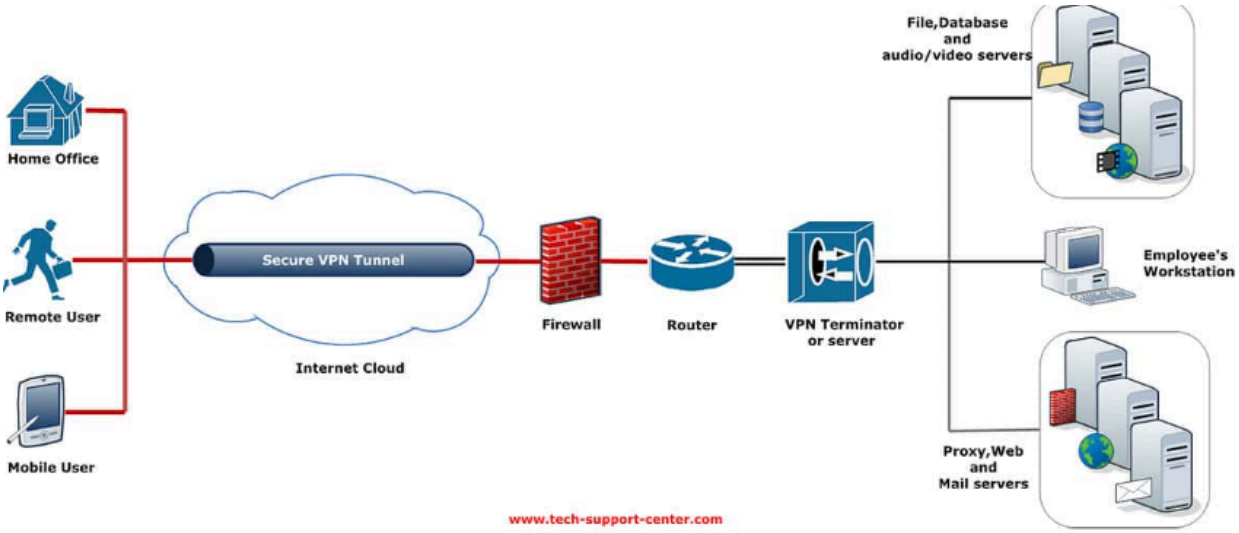
Working of VPN

1. **Connection Establishment**
   - The user connects to a **VPN server** using VPN client software.
2. **Authentication**
   - User credentials and certificates are verified to **authenticate** the connection.
3. **Data Encryption**
   - All data sent between the device and VPN server is **encrypted** using protocols like **IPsec** or **SSL/TLS**.
4. **Tunneling**

- The encrypted data travels through a **secure tunnel** over the public internet, preventing eavesdropping.

5. **Decryption and Forwarding**
    - The VPN server **decrypts the data** and forwards it to the target destination (e.g., a website or corporate server).
    - Responses are encrypted again and sent back through the same tunnel.

Working of VPN diagram:



Security Benefits

- **Data Confidentiality:** Encryption protects sensitive data from hackers or ISPs.
- **Data Integrity:** Prevents tampering or alteration during transmission.
- **User Anonymity:** Masks the user's **IP address** and location.
- **Secure Remote Access:** Enables employees to safely connect to corporate networks from anywhere.
- **Bypass Restrictions:** Allows access to geo-restricted or censored content securely.

Q2. [10 Marks] - Answers

a. Given a 5x5 grid and the keyword "PLAYFAIR", encrypt the message "HIDE" using the Playfair cipher. Demonstrate the steps and the final ciphertext.

CNS-2025-May-PYQ

Q.2]

Ans-a Given:

Message / Plain Text = HIDE

Keyword = PLAYFAIR

Step-1] Building the 5×5 matrix.

P	L	A	Y	F
I/J	R	B	C	D
E	G	H	K	L
M	N	O	Q	S
T	U	V	W	X

P	L	A	Y	F
I/J	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

Step-2: Preparing the Plain text and splitting them into digraphs

HI DE

↓ ↓ ↓ ↓

E B I M

Step-3 Encrypting each digraph

Final Cipher Text = EBIM

b. Explain the working of SHA-256 using suitable example.

Introduction to SHA-256

- SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function from the SHA-2 family.
- It takes an input message and produces a fixed 256-bit (32-byte) hash value.
- Commonly used in digital signatures, blockchain (e.g., Bitcoin), and data integrity verification.

Working of SHA-256

1. **Message Preprocessing**
    - **Padding**: The input message is padded so its length becomes a multiple of 512 bits.
    - **Length Appending**: The original message length (in bits) is appended as a 64-bit value.

2. **Message Parsing**
    - The padded message is divided into 512-bit blocks.

3. **Initialization**
    - SHA-256 uses **eight 32-bit initial hash values** (H0 to H7), defined by the standard.

4. **Compression Function**
    - Each 512-bit block undergoes 64 rounds of processing using:
        - Logical functions (AND, OR, XOR, NOT)

- Bitwise operations (shifts and rotations)
- Constants (K0 to K63)
- Working variables (a to h)

5. **Hash Value Update**
   - After processing each block, the intermediate hash values are updated.

6. **Final Output**
   - After all blocks are processed, the final 256-bit hash is produced by concatenating H0 to H7.

Example:

Input: `"hello"`

Steps:

- Convert to binary → Pad → Process through 64 rounds
- Final SHA-256 hash:

```
2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824
```

Q3. [10 Marks] - Answers

a. What is a SPAM? Explain different types of SPAMs.

What is SPAM?

- **SPAM** refers to **unsolicited or irrelevant messages** sent over the internet, typically in bulk.

- Commonly seen in **emails**, **social media**, **forums**, and **messaging platforms**.
- Purpose: advertising, phishing, spreading malware, or wasting bandwidth.

Types of SPAM

1. **Email Spam**
    - Bulk emails sent to random or purchased addresses.
    - Often includes ads, scams, or malicious links.

2. **Phishing Spam**
    - Fraudulent messages pretending to be from trusted sources.
    - Aim: steal sensitive data like passwords or credit card info.

3. **Comment Spam**
    - Irrelevant or promotional comments posted on blogs, forums, or social media.
    - Usually includes links to external sites.

4. **SMS Spam**
    - Unwanted promotional or scam messages sent via text.
    - May include fake offers or phishing links.

5. **Search Engine Spam (Spamdexing)**
    - Manipulating search engine rankings using keyword stuffing or link farms.
    - Goal: drive traffic to low-quality or malicious sites.

6. **Social Media Spam**

- Fake accounts or bots posting promotional content, scams, or misleading links.
- Can also include mass tagging or fake giveaways.

7. **Instant Messaging Spam**
    - Spam sent via platforms like WhatsApp, Telegram, or Messenger.
    - Often includes chain messages or malicious attachments.

b. What is the significance of IPSec? Explain the different modes of operation in IPSec?

Significance of IPSec (Internet Protocol Security)

- **IPSec** is a suite of protocols used to secure IP communications by authenticating and encrypting each IP packet.
- It operates at the **network layer**, making it transparent to applications.
- Ensures **confidentiality, integrity, and authenticity** of data over untrusted networks like the Internet.

Key Benefits:

- **Data Confidentiality**: Encrypts data to prevent unauthorized access.
- **Data Integrity**: Ensures data is not altered in transit.
- **Authentication**: Verifies the identity of the sender.

Modes of Operation in IPSec

IPSec operates in two modes:

1. **Transport Mode**

- **Encrypts only the payload** (data) of the IP packet, not the header.
- Original IP header is retained.
- Used for **end-to-end communication** (e.g., host-to-host).
- Suitable for **internal secure communication** within a trusted network.

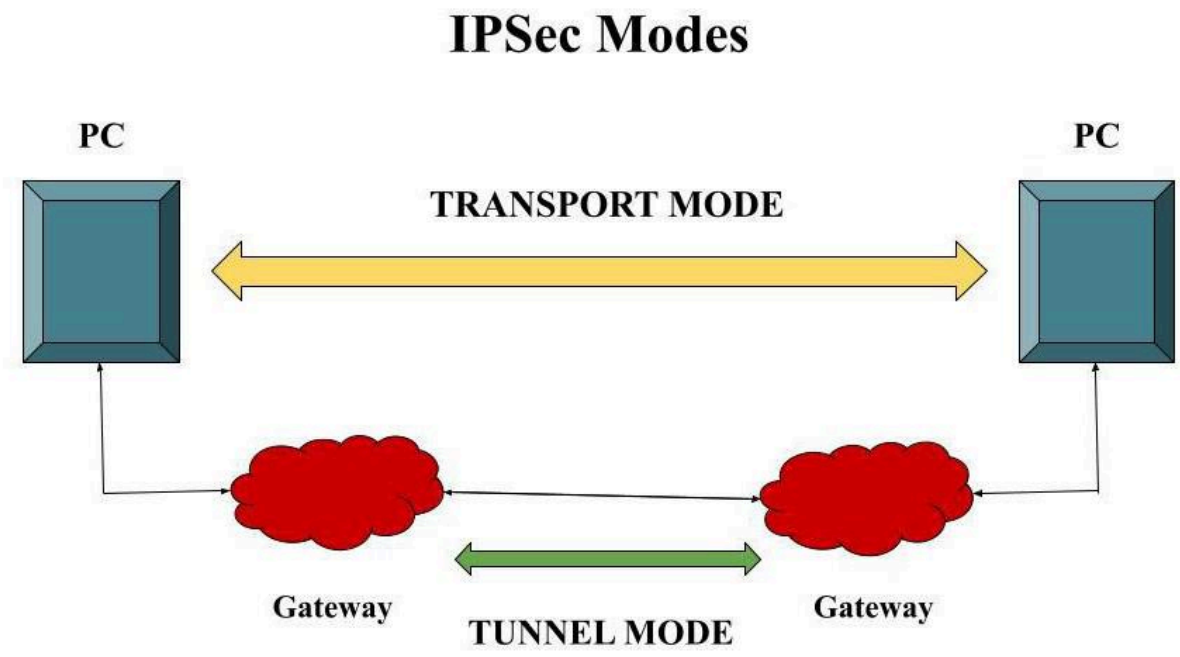
Example: Secure communication between two servers in the same organization.

2. **Tunnel Mode**

- **Encrypts the entire IP packet** (header + payload).
- A new IP header is added for routing.
- Used for **network-to-network** or **host-to-network** communication via VPNs.
- Common in **site-to-site VPNs** and **remote access VPNs**.

Example: Secure communication between two branch offices over the Internet.

IPSec Modes diagram:

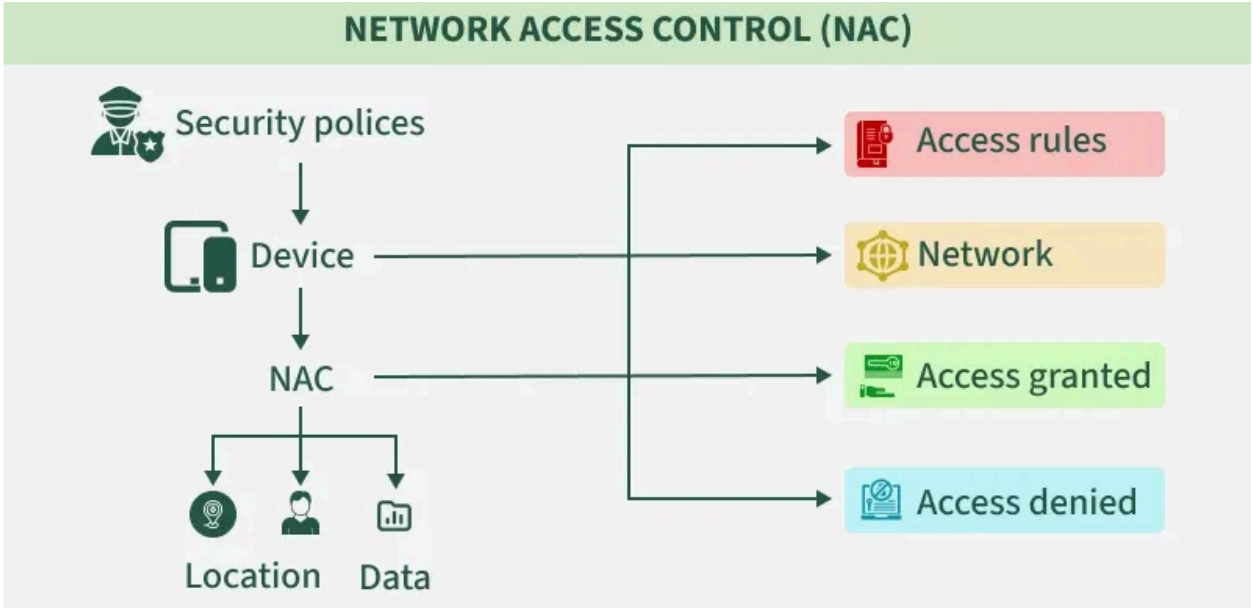


Q4. [10 Marks] - Answers

a. Explain the various use cases of NAC.

What is NAC?

- **Network Access Control (NAC)** is a security solution that manages and enforces policies for device access to a network.
- It ensures that only **authorized, compliant, and secure devices** can connect to the network.



Use Cases of NAC

1. **Endpoint Compliance Enforcement**
    - Verifies if devices meet security standards (e.g., antivirus, OS updates) before granting access.

- Prevents vulnerable or infected devices from entering the network.

2. **Guest Network Access**
    - Provides **segmented access** to guests or contractors.
    - Limits access to internal resources while allowing internet or specific services.

3. **BYOD (Bring Your Own Device) Management**
    - Controls access for personal devices like smartphones or laptops.
    - Applies different policies based on device type, user role, or location.

4. **Role-Based Access Control**
    - Grants network access based on user identity or department.
    - Example: HR staff can access payroll systems, but not engineering servers.

5. **Threat Containment and Quarantine**
    - Automatically isolates suspicious or compromised devices.
    - Prevents lateral movement of malware within the network.

6. **Visibility and Inventory**
    - Tracks all connected devices in real-time.
    - Helps in auditing and identifying unauthorized or rogue devices.

7. **Integration with Security Systems**
    - Works with firewalls, SIEM, and antivirus tools for coordinated response.

- Enhances overall network security posture.

b. Explain the different types of IDS.

What is IDS?

- **Intrusion Detection System (IDS)** monitors network or system activities for malicious actions or policy violations.
- It helps detect unauthorized access, attacks, or abnormal behavior in real-time.

Types of IDS

1. **Network-based IDS (NIDS)**

- Monitors traffic across the entire network.
- Placed at strategic points like routers or firewalls.
- Detects attacks like DoS, port scans, or malware propagation.

Example: Snort, Suricata

2. **Host-based IDS (HIDS)**

- Installed on individual devices (servers, PCs).
- Monitors system logs, file integrity, and user activity.
- Detects insider threats, unauthorized file changes, or privilege escalation.

Example: OSSEC, Tripwire

3. **Signature-based IDS**

- Uses predefined attack patterns (signatures) to detect threats.
- Effective against known attacks but **cannot detect zero-day threats**.

Example: Detecting a known SQL injection pattern.

4. **Anomaly-based IDS**

- Learns normal behavior and flags deviations.
- Can detect **unknown or novel attacks**, but may produce **false positives**.

Example: Unusual login time or data transfer volume.

5. **Hybrid IDS**

- Combines features of multiple IDS types (e.g., NIDS + HIDS or Signature + Anomaly).
- Offers broader coverage and improved accuracy.

Q5. [10 Marks] - Answers

a. What are the characteristics of a firewall?

What is a Firewall?

- A **firewall** is a security device (hardware or software) that monitors and controls incoming and outgoing network traffic.
- It acts as a **barrier between trusted internal networks and untrusted external networks** (like the Internet).

Key Characteristics of a Firewall

1. **Packet Filtering**
    - Inspects packets based on IP address, port number, and protocol.
    - Allows or blocks traffic based on predefined rules.

2. **Stateful Inspection**
    - Tracks the state of active connections.
    - Makes decisions based on the context of traffic (e.g., part of an established session).

3. **Access Control**
    - Enforces policies to permit or deny traffic.
    - Can be based on user identity, device type, or application.

4. **Network Address Translation (NAT)**
    - Masks internal IP addresses from external networks.
    - Enhances privacy and security.

5. **Application Layer Filtering**
    - Inspects traffic at the application level (e.g., HTTP, FTP).
    - Detects and blocks malicious content or unauthorized applications.

6. **Logging and Monitoring**
    - Records traffic events for analysis and auditing.
    - Helps in detecting suspicious activity or breaches.

7. **VPN Support**
    - Facilitates secure remote access via Virtual Private Networks.
    - Encrypts traffic between remote users and internal network.

8. **Intrusion Prevention Integration**

- Some firewalls include IDS/IPS features to detect and block threats in real-time.

b. What are the steps involved in implementing NAC solutions?

Introduction

Network Access Control (NAC) ensures that only **authorized and compliant devices** can access network resources. Implementing NAC involves strategic planning, integration, and enforcement of security policies.

Key Steps in NAC Implementation

1. **Define Security Policies**
   - Establish rules for device authentication, compliance checks, and access levels.
   - Example: Devices must have updated antivirus and OS patches.

2. **Assess Network Infrastructure**
   - Identify existing hardware (switches, routers) and software compatibility.
   - Ensure support for NAC protocols like 802.1X.

3. **Select a NAC Solution**
   - Choose based on organization size, device diversity, and integration needs.
   - Examples: Cisco ISE, Aruba ClearPass, FortiNAC.

4. **Deploy Authentication Mechanisms**
   - Implement methods like 802.1X, MAC filtering, or captive portals.

- Integrate with identity systems (e.g., Active Directory, RADIUS).

5. **Device Profiling and Classification**
    - Automatically detect and categorize devices (e.g., laptop, smartphone, printer).
    - Apply role-based access policies accordingly.

6. **Policy Enforcement**
    - Allow, deny, or quarantine devices based on compliance status.
    - Use VLAN assignment or access control lists (ACLs) to segment traffic.

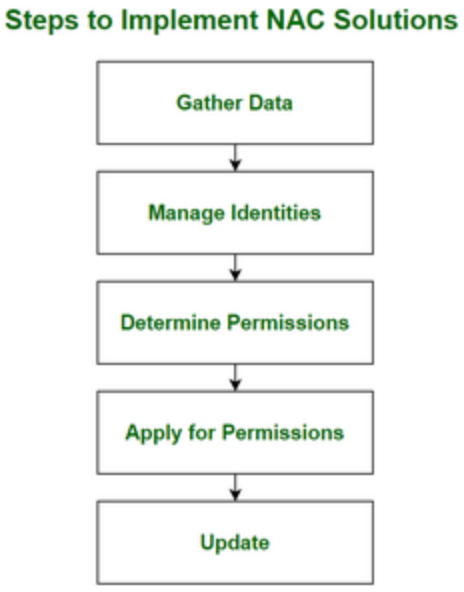
7. **Monitoring and Reporting**
    - Continuously track device behavior and access patterns.
    - Generate alerts and compliance reports for auditing.

8. **Incident Response Integration**
    - Link NAC with SIEM or endpoint protection tools for threat containment.
    - Automatically isolate compromised devices.

9. **User Education and Rollout**
    - Inform users about NAC policies and onboarding procedures.
    - Gradually roll out NAC to minimize disruption.

10. **Review and Update Policies**

- Regularly refine rules based on new threats, device types, or business needs.



Implement NAC Solutions

Q6. [10 Marks] - Answers

a. Write short notes on: HMAC and CMAC

Feature	HMAC (Hash-Based Message Authentication Code)	CMAC (Cipher-Based Message Authentication Code)
Full Form	Hash-Based Message Authentication Code	Cipher-Based Message Authentication Code
Underlying Algorithm	Uses a **hash function** (e.g., SHA-256, MD5)	Uses a **block cipher** (e.g., AES, 3DES)
Key Type	Symmetric key (shared secret)	Symmetric key (shared secret)
Purpose	Ensures **data integrity** and **authenticity**	Ensures **data integrity** and **authenticity**
Computation Process	Combines **message** and **key** using hashing operations (inner and outer hash)	Encrypts data blocks using **cipher-based operations**
Use Cases	Common in **SSL/TLS, IPSec, APIs, and VPNs**	Used in **IEEE 802.11i (Wi-Fi), IPSec, and AES-based systems**

Feature	HMAC (Hash-Based Message Authentication Code)	CMAC (Cipher-Based Message Authentication Code)
Performance	Generally **faster** on systems optimized for hashing	**More secure** when encryption hardware is available

b. Write short notes on: S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions)

- **Definition:**

  S/MIME is a standard for **secure email communication** that provides **encryption**, **authentication**, and **message integrity**.

- **Purpose:**

  It ensures that emails are **confidential**, **tamper-proof**, and sent by **verified users**.

- **Key Features:**
  1. **Encryption:** Protects email content so only intended recipients can read it.
  2. **Digital Signature:** Verifies the sender's identity and ensures message integrity.
  3. **Certificate-Based Security:** Uses **X.509 digital certificates** for sender authentication.
  4. **Interoperability:** Works with standard email formats (MIME).
  5. **Data Integrity:** Detects any unauthorized modification of the message.

- **Working:**
  - The sender signs the message using their **private key** and encrypts it with the recipient's **public key**.
  - The recipient decrypts it using their **private key** and verifies the signature using the sender's **public key**.

- **Applications:**

  Widely used in **corporate**, **government**, and **financial organizations** for secure email exchange.

c. Write short notes on: RSA Algorithm

RSA Algorithm

- **Definition:**
  RSA (Rivest–Shamir–Adleman) is a **public key cryptographic algorithm** used for **secure data transmission** and **digital signatures**.
- **Principle:**
  Based on the mathematical difficulty of **factoring large prime numbers** — making it secure against brute-force attacks.
- **Key Generation:**
  1. Choose two large prime numbers p and q.
  2. Compute $n = p \times q$ and $\phi(n) = (p-1)(q-1)$.
  3. Select public key e (coprime with $\phi(n)$).
  4. Compute private key d such that $(d \times e) \mod \phi(n) = 1$.
- **Encryption and Decryption:**
  - **Encryption:** $C = (M^e) \mod n$
  - **Decryption:** $M = (C^d) \mod n$
    (Where M = message, C = ciphertext)
- **Uses:**
  - **Data encryption and decryption**
  - **Digital signatures** for authentication and integrity
  - **Secure key exchange** in protocols like **SSL/TLS**
- **Example:**
  Used in **HTTPS** to securely transmit encryption keys between a browser and a web server.

e. Write short notes on: OSI Security Architecture

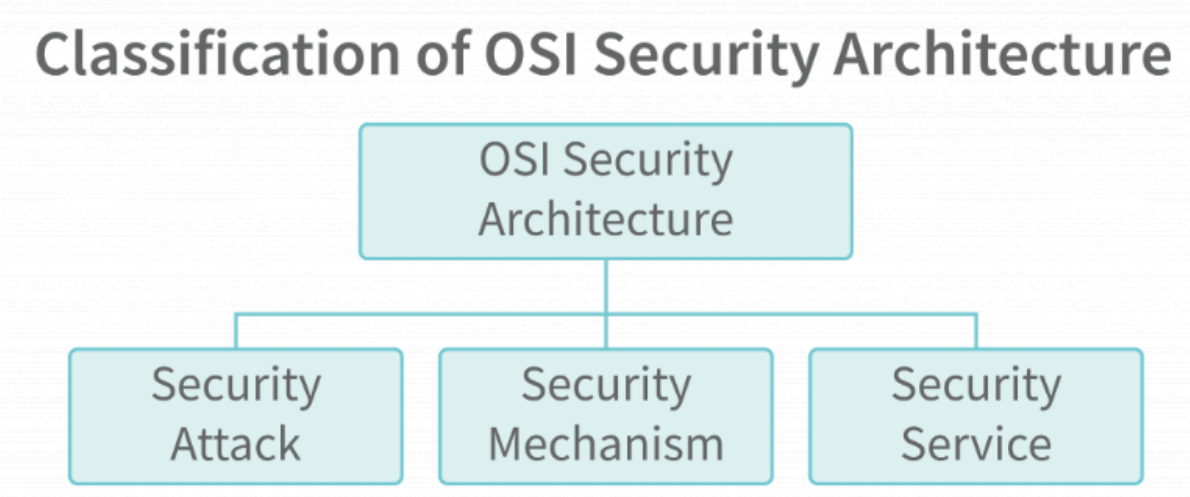
OSI Security Architecture

- **Definition:**

  The **OSI Security Architecture** is a framework defined by ISO to provide a **systematic approach to network security**, identifying what is needed to protect data during communication.

- **Purpose:**

  Helps in designing **secure communication systems** by defining **security services**, **mechanisms**, and **attacks**.



- **Main Elements:**
  1. **Security Attack:**

     Any action that compromises the security of information (e.g., interception, modification, fabrication).
  2. **Security Mechanism:**

     Tools or methods used to detect, prevent, or recover from attacks.

     Examples – Encryption, Digital Signatures, Firewalls, Authentication.
  3. **Security Service:**

     Services that enhance the security of data processing and transfer.

     Examples – Confidentiality, Integrity, Authentication, Non-repudiation.

- **Security Services (as defined by OSI):**
  - **Authentication** – Verifies identity of entities.
  - **Access Control** – Prevents unauthorized use.
  - **Data Confidentiality** – Protects data from unauthorized disclosure.

- **Data Integrity** – Ensures data isn't altered.
- **Non-repudiation** – Prevents denial of actions.

- **Significance:**

  Provides a **structured and layered model** to implement and manage network security consistently across systems.

f. Write short notes on: HTTPS

HTTPS (Hypertext Transfer Protocol Secure)

- **Definition:**

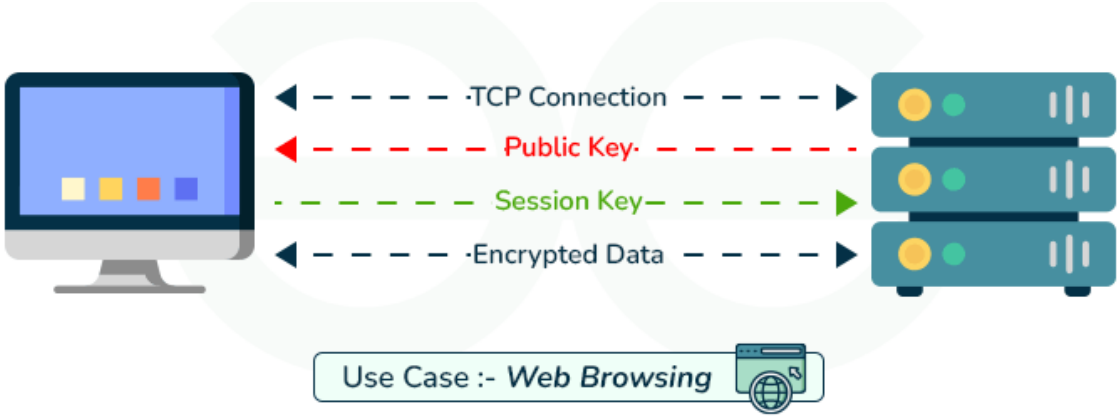
  HTTPS is the **secure version of HTTP**, used for safe communication between a **web browser and web server** over the internet.

- **Purpose:**

  Ensures **data confidentiality, integrity, and authentication** during web communication.

- **How It Works:**

  1. Uses **SSL/TLS (Secure Sockets Layer / Transport Layer Security)** to encrypt data.
  2. The web server presents an **X.509 digital certificate** to verify its identity.
  3. Data exchanged between browser and server is **encrypted**, preventing eavesdropping and tampering.



- **Key Features:**
  - **Encryption:** Protects data from interception (e.g., login credentials, payment info).
  - **Authentication:** Confirms that users are communicating with the **legitimate website**.
  - **Integrity:** Prevents data modification during transfer.

- **Benefits:**
  - Builds **user trust** and prevents **phishing attacks**.
  - Mandatory for secure websites (e.g., banking, e-commerce).
  - Indicated by a **lock icon (🔒)** and “https://” in the browser address bar.

- **Example:**

  Websites like **https://www.amazon.com** use HTTPS to secure online transactions and protect user data.