CNS-2024-December-PYQ

Q1. [20 Marks]

a. Enlist security goals. Discuss their significance.

b. Compare and contrast DES and AES.

c. SHA provides better security than MD5 Justify.

d. Explain the purpose of keylogger and rootkit.

Q2. [10 Marks]

a. Encrypt “This is the final exam” with Play fair cipher, the key is ‘Guidance’

b. What is the significance of a digital signature on a certificate?

Q3. [10 Marks]

a. What is PKI. Explain PKI architecture in detail

Q4. [10 Marks]

a. What is network access control? Discuss the elements present in this context.

Q5. [10 Marks]

a. Explain network management security with respect to SNMP protocol.

Q6. [10 Marks]

a. Explain different methods of IDS? State capabilities and challenges in IDS.

Q1. [20 Marks] - Answers

a. Enlist security goals. Discuss their significance.

Security Goals and Their Significance

Main Security Goals:

1. **Confidentiality**
    - Ensures that information is accessible **only to authorized users**.
    - Prevents **unauthorized disclosure** of sensitive data.
    - **Example:** Encrypting emails to prevent interception.

2. **Integrity**
    - Ensures that data remains **accurate and unaltered** during storage or transmission.
    - Protects against **unauthorized modification or deletion**.
    - **Example:** Using hashing or digital signatures to verify data integrity.

3. **Availability**
    - Ensures that **authorized users can access** information and resources **when needed**.
    - Protects against **DoS attacks, hardware failures, or outages**.
    - **Example:** Backup systems and redundant servers.

4. **Authentication**
    - Confirms the **identity** of users or systems before granting access.
    - **Example:** Login credentials, digital certificates, or biometrics.

5. **Non-repudiation**

- Ensures that the sender **cannot deny** sending a message or performing an action.
- **Example:** Digital signatures in online transactions.

Significance:

- Forms the **foundation of information security policies**.
- Ensures **trust, reliability, and accountability** in digital communication.
- Protects organizations from **data breaches, fraud, and service disruptions**.
- Supports **legal compliance** and **user confidence** in digital systems.

b. Compare and contrast DES and AES.

Aspect	DES (Data Encryption Standard)	AES (Advanced Encryption Standard)
Full Form	Data Encryption Standard	Advanced Encryption Standard
Key Length	56 bits	128, 192, or 256 bits
Block Size	64 bits	128 bits
Algorithm Type	Symmetric block cipher using **Feistel structure**	Symmetric block cipher using **Substitution–Permutation Network (SPN)**
Rounds	16 rounds	10, 12, or 14 rounds (depending on key size)
Security Level	**Less secure**, vulnerable to brute-force attacks	**Highly secure**, resistant to known attacks
Performance	**Slower** and less efficient on modern hardware	**Faster**, more efficient, widely adopted standard
Usage	Older encryption standard (now obsolete)	Current **U.S. encryption standard (FIPS-197)**

c. SHA provides better security than MD5 Justify.

SHA Provides Better Security than MD5 – Justification

1. **Hash Length:**
    - **MD5** produces a **128-bit hash value**, while **SHA-1** and **SHA-256** produce **160-bit** and **256-bit** hashes respectively.
    - Longer hash values make **SHA** more resistant to brute-force and collision attacks.

2. **Collision Resistance:**
    - MD5 is **vulnerable to collision attacks** (two different inputs producing the same hash).
    - **SHA algorithms** (especially **SHA-256** and above) offer **stronger collision resistance**, making them more secure for integrity verification.

3. **Cryptographic Strength:**
    - MD5 has **known vulnerabilities** exploited in digital signatures and certificates.
    - SHA provides **stronger mathematical design** and **better resistance** against cryptanalysis.

4. **Data Integrity:**
    - SHA ensures **reliable integrity checks**, preventing data tampering in transit.
    - MD5's weaknesses make it **unsuitable for modern cryptographic use**.

5. **Current Usage:**
    - MD5 is now considered **deprecated** for security purposes.
    - **SHA-256 and SHA-3** are widely used in **SSL/TLS**, **digital signatures**, and **blockchain technology** for their robustness.

d. Explain the purpose of keylogger and rootkit

1. Keylogger

- **Definition:**

  A **keylogger** is a type of **spyware** that secretly records every **keystroke** made by a user on a keyboard.

- **Purpose:**
  - To **capture sensitive information** such as passwords, credit card numbers, and messages.
  - Used by attackers for **identity theft**, **financial fraud**, or **monitoring user activity**.
  - Can be **software-based** (installed on OS) or **hardware-based** (plugged into the keyboard port).
- **Prevention:**
  - Use **antivirus and anti-spyware** tools.
  - Keep the system updated and avoid installing untrusted software.
  - Use **virtual keyboards** for sensitive input.

---

2. Rootkit

- **Definition:**

  A **rootkit** is a collection of malicious tools designed to **gain unauthorized root (administrator) access** and **hide malicious activities** on a system.

- **Purpose:**
  - To **maintain persistent, hidden access** for attackers.
  - Used to **hide malware**, modify system files, and **disable security software**.
  - Often installed after exploiting a system vulnerability.

- **Prevention:**
  - Use **trusted operating systems** and **regular system scans**.
  - Apply **security patches** and monitor for unusual system behavior.

e. Explain about software Re-engineering and reverse engineering?

1. Software Re-engineering:

Definition:

Software Re-engineering is the **process of analyzing and modifying existing software** to improve its **quality, performance, or maintainability** without changing its core functionality.

Key Points:

- Involves **restructuring, cleaning, and updating** old code.
- Helps **extend the life** of legacy systems.
- May include activities like **code refactoring, documentation update, and migration** to new platforms.
- Goal: **Enhance software quality and reduce future maintenance costs.**

Example:

Converting an old **C-based desktop application** into a **modern Java web application**.

2. Reverse Engineering:

Definition:

Reverse Engineering is the process of **analyzing existing software to understand its design, structure, and functionality** when documentation is missing or outdated.

Key Points:

- Used to **recover design details** or **generate documentation** from source code.
- Helps in **understanding legacy systems** or integrating with new systems.
- Often a **first step in re-engineering**.

Example:

Extracting UML diagrams from source code to understand system flow.

Q2. [10 Marks] - Answers

a. Encrypt “This is the final exam” with Play fair cipher, the key is ‘Guidance’

CNS - 2024 - December - PYQ

Q.2

Ans-a Given:

Message / Plain text = "THIS IS THE FINAL EXAM"

Keyword = "GUIDANCE"

Step-1: Building the 5×5 matrix.

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

Step-2: Preparing the plain text & splitting them into diagraphs.

TH IS IS TH EF IN AL EX AM

↓↓ ↓↓ ↓↓ ↓↓ ↓↓ ↓↓ ↓↓ ↓↓ ↓↓ ↓↓

PO RD RD PO BN GE IG LI OD

Step-3 → Encrypting each diagram according to the rules of Playfair cipher.

∴ Final Cipher text = PORD RD POB NGEIO LIOD

b. What is the significance of a digital signature on a certificate?

Significance of a Digital Signature on a Certificate

A **digital signature** on a digital certificate is a cryptographic mechanism used to ensure the **authenticity, integrity, and trustworthiness** of the certificate.

Key Roles:

1. **Authenticity**
    - Confirms that the certificate was issued by a trusted **Certificate Authority (CA)**.
    - Prevents impersonation or fake certificates.

2. **Integrity**
    - Ensures the certificate has **not been tampered with** after issuance.
    - Any modification invalidates the signature.

3. **Trust Establishment**
    - Allows users and systems to **trust the public key** contained in the certificate.
    - Forms the basis of **SSL/TLS**, **email encryption**, and **code signing**.

4. **Verification**
    - Recipients can use the CA's **public key** to verify the signature.
    - If valid, the certificate is considered genuine.

Example:

When you visit `https://example.com`, your browser checks the website's certificate. If the digital signature is valid, it confirms the site is secure and issued by a trusted authority.

Q3. [10 Marks] - Answers

a. What is PKI. Explain PKI architecture in detail

What is PKI?

Public Key Infrastructure (PKI) is a framework of **policies, technologies, and procedures** used to create, manage, distribute, use, store, and revoke **digital certificates** and **public-private key pairs**.

It enables **secure communication**, **authentication**, **data integrity**, and **digital signatures** in networks and over the internet.

PKI Architecture Components

1. **Certificate Authority (CA)**
    - A trusted entity that **issues and signs digital certificates**.
    - Verifies the identity of entities (users, servers, devices).
    - Can be:
        - **Root CA**: Top-level, self-signed.
        - **Intermediate CA**: Issued by Root CA; used for scalability and security.

2. **Registration Authority (RA)**
    - Acts as a **verifier** on behalf of the CA.
    - Authenticates users or devices before certificate issuance.
    - Forwards verified requests to the CA.

3. **Certificate Database**
    - Stores issued certificates and their status.
    - Used for auditing and management.

4. **Certificate Store**
    - A local repository on client devices or servers.
    - Stores trusted root certificates and user certificates.

5. **Certificate Revocation List (CRL) / OCSP**
    - Lists certificates that have been revoked before expiry.
    - **CRL**: Periodically updated list.
    - **OCSP (Online Certificate Status Protocol)**: Real-time certificate status checking.

6. **Public and Private Keys**
    - **Public Key**: Shared openly; used for encryption or signature verification.
    - **Private Key**: Kept secret; used for decryption or signing.

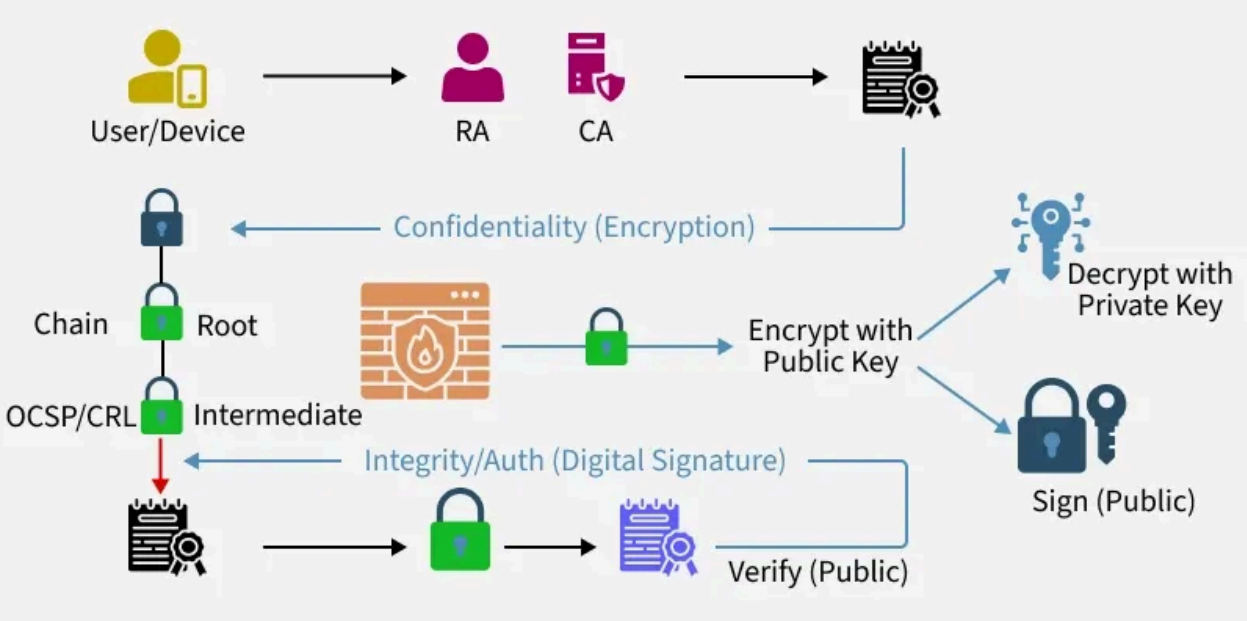
7. **Digital Certificates (X.509)**
    - Bind a public key to an entity's identity.
    - Include fields like Subject, Issuer, Validity, Public Key, and Digital Signature.

PKI Workflow (Simplified)

1. **User requests a certificate** → submits identity proof to RA.

2. **RA verifies identity** → forwards request to CA.
3. **CA issues a digital certificate** → signed with CA's private key.
4. **User installs certificate** → used for secure communication.
5. **Other parties verify certificate** using CA's public key.
6. **If compromised**, certificate is revoked via CRL or OCSP.

Process of creation of certificate:



Q4. [10 Marks] - Answers

a. What is network access control? Discuss the elements present in this context.

What is Network Access Control (NAC)?

Network Access Control (NAC) is a security framework that **regulates and restricts access** to network resources based on predefined policies. It ensures

that only **authorized, authenticated, and compliant devices** can connect to the network.

NAC plays a vital role in **preventing unauthorized access**, **enforcing security policies**, and **protecting sensitive data** in enterprise and distributed environments.

Key Elements of NAC

1. **Authentication**

- Verifies the identity of users and devices before granting access.
- Uses credentials, certificates, or multi-factor authentication.
- Ensures only trusted entities can connect.

2. **Authorization**

- Determines **what level of access** a user or device should have.
- Based on roles, device type, location, or compliance status.
- Example: Admins get full access; guests get internet-only access.

3. **Endpoint Compliance**

- Checks if devices meet security requirements:
  - Antivirus installed
  - OS updated
  - Firewall enabled
- Non-compliant devices may be quarantined or denied access.

4. **Policy Enforcement**

- Applies rules to control access based on authentication and compliance.
- Can redirect, block, or isolate devices using VLANs or ACLs.

5. **Monitoring and Reporting**

- Tracks real-time activity of connected devices.
- Generates logs and alerts for suspicious behavior or policy violations.

6. **Remediation**

- Guides non-compliant devices to fix issues (e.g., update antivirus).
- Allows re-evaluation after remediation for access approval.

7. **Integration with Security Tools**

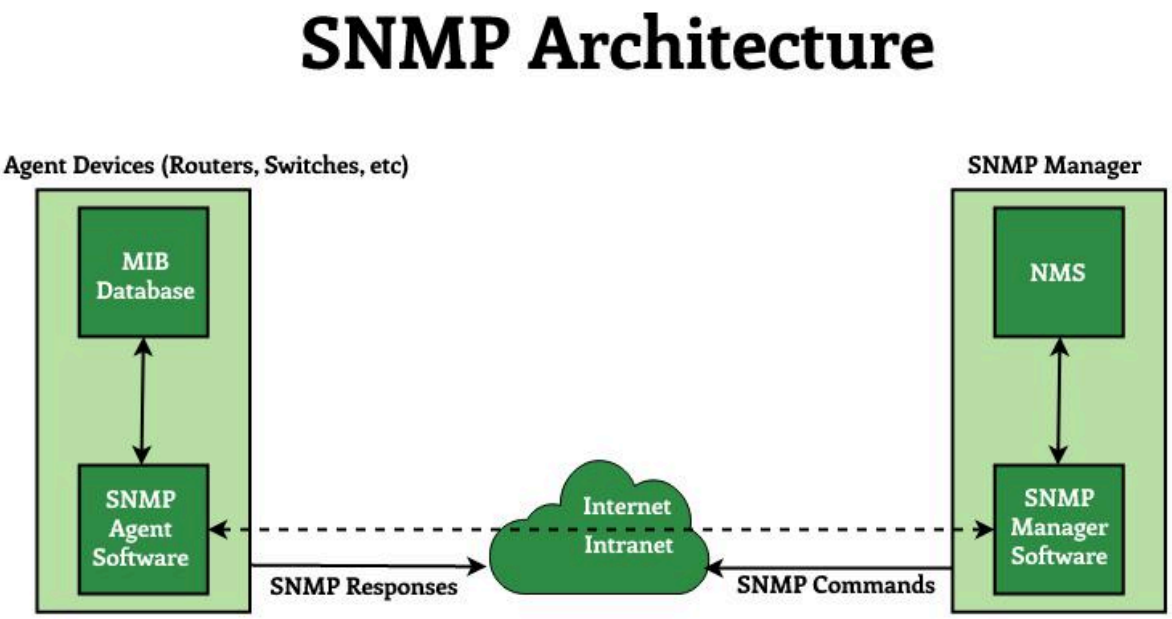
- Works with firewalls, SIEM, antivirus, and identity management systems.
- Enables coordinated threat detection and response.

Q5. [10 Marks] - Answers

a. Explain network management security with respect to SNMP protocol.

What is SNMP?

SNMP (Simple Network Management Protocol) is a widely used protocol for **monitoring and managing network devices** such as routers, switches, servers, and printers. It enables administrators to collect performance data, configure devices, and detect faults remotely.



Network Management Security in SNMP

While SNMP is powerful for network management, it also introduces **security risks** if not properly secured. Here's how SNMP handles security across its versions:

SNMP Versions and Their Security Features

1. **SNMPv1 and SNMPv2c**

- Use **community strings** for authentication (like passwords).
- **No encryption** or strong authentication.
- Vulnerable to:
  - Eavesdropping
  - Unauthorized access
  - Replay attacks

Security Tip: Restrict access using ACLs and change default community strings (e.g., avoid "public").

2. **SNMPv3 (Secure SNMP)**

- Introduces robust security features:
  - **Authentication**: Verifies identity using HMAC with MD5 or SHA.
  - **Privacy (Encryption)**: Encrypts SNMP messages using DES or AES.
  - **Access Control**: Uses user-based security model (USM) and view-based access control model (VACM).

Benefits:

- Prevents unauthorized access and data tampering.
- Protects sensitive configuration and performance data.

Key Security Elements in SNMPv3

Feature	Description
Authentication	Confirms sender identity (e.g., SHA, MD5)
Privacy	Encrypts messages (e.g., AES, DES)
Access Control	Limits access to specific MIB objects
User Management	Assigns roles and permissions to SNMP users

Q6. [10 Marks] - Answers

a. Explain different methods of IDS? State capabilities and challenges in IDS.

Capabilities of IDS

- **Threat Detection**: Identifies malware, DoS attacks, unauthorized access.
- **Real-Time Alerts**: Notifies administrators instantly.
- **Traffic Analysis**: Monitors network packets and logs.
- **Policy Enforcement**: Detects violations of security policies.

- **Forensics Support**: Provides logs for post-attack analysis.

Challenges in IDS

- **False Positives**: Legitimate activity flagged as malicious.
- **False Negatives**: Missed detection of actual threats.
- **Scalability**: Performance may degrade in large networks.
- **Encrypted Traffic**: Hard to inspect without decryption.
- **Maintenance**: Requires regular updates and tuning.
- **Resource Usage**: Can consume CPU and memory during deep inspection.