1> Explain Security Mechanisms in Information & Cyber security.

Security Mechanisms in information & cyber security are methods, technologies or processes designed to protect data, systems & networks from authorized access, attacks, tampering, or other security threats. These mechanisms work to detect, prevent or recover from security attacks & help maintain the confidentiality, integrity, authentication, access control, non-repudiation & availability of information.

Main Security Mechanisms

- Encryption: This involves using mathematical algorithms to transform data into an unreadable format for unauthorized users. Encryption ensures data confidentially during transmission or storage by converting data into ciphertext which can only be decrypted with the correct key.
- Access Control: Mechanisms such as passwords, firewalls, or PINs are used to restrict unauthorized access to resources. Access control enforces policies determining who can access or modify data.
- Digital Signature: A cryptographic means of verifying the authenticity & integrity of a message or document. It acts as an electronic signature to verify the sender's identity and confirm that the data has not been altered.
- Data Integrity: Techniques like appending values derived from the data itself ensure that data has

not been tampered with during transmission or storage.

- Authentication Exchange: Processes for verifying the identities of communicating parties often by protocols like two-way handshaking, to confirm legitimacy before granting access.
- Notarization: The involvement of a trusted of third party that acts as a mediator in communications to keep a record and reduce conflicts or disputes about message exchanges
- Bit stuffing: A method to add extra bits into data being transmitted allowing error detection at the receiving end by parity checks.
- Traffic padding & Routing control: Adds extra data to obscure true traffic content and controls routing paths to select secure routes for data transmission.

Security services supported by Mechanisms

- Authentication: verifying user or device identities.
- Access control: Regulating access to resources
- Data confidentiality: protecting data from unauthorized disclosure.
- Data Integrity: Ensuring data is not altered improperly.
- Non-repudiation: Preventing denial of actions like sending a message.
- Availability: Ensuring resources and data are accessible to authorized users when needed.

2) Discuss various Risks and attacks types in Information & Cyber Security.

The risks and attack Types in information & cyber security are diverse and constantly evolving posing threats to organizations data, systems, and reputation.

Common Information & cyber Security Risks:

- Data Breaches: Unauthorized access to sensitive data can result in financial & reputational damage
- Insider threats: Attacks arising from within an organization such as disgruntled employees or contra-ctors with access rights.
- Third-party Risks: Vulnerabilities originating from vendors, suppliers or partners that connect to organ-izational systems.
- Compliance Risks: Failure to comply with laws and regulations, potentially leading to legal penalties.
- Reputational Risks: Harm to organizational image following a security incident.
- Technology Risks: Vulnerabilities in hardware, softwa-re & networks such as unpatched systems or misconfigured infrastructure.

Major Types of Cyber Attacks:

- Malware: Malicious software (viruses, trojans, worms, ransomware) used to damage or gain unauth-orized access to systems.

- Ransomware:
Attackers lock or encrypt data, demanding ransom for restoration.
- phishing & Social Engineering:
Manipulating people into revealing confidential information or installing malicious software (includes spear phishing & baiting).
- Password Attacks:
Attempts to steal or guess login credentials to gain access
- Denial of service (DOS/DDOS):
Overloading services or networks to disrupt availability.
- SQL Injection:
Exploiting vulnerable web applications to steal or manipulate data.
- Man-in-the-Middle (MitM):
Intercepting & possibly altering communications b/w parties without their knowledge
- Zero-Day Exploits:
Attacks targetting previously unknown vulnerabilities before they are patched.
- API Attacks: Exploiting vulnerabilities in APIs for unauthorized access or data leakage.
- IOT & BYOD Risks: Poorly secured devices (like smart gadgets & employee-owned devices) can become entry points for attackers.

3) What is cryptography? Discuss the private key cryptography with neat diagram.

Cryptography is the art & science of securing information by converting it into an unreadable form to prevent unauthorized access, ensuring confidentiality, integrity, authentication, & non-repudiation of data. It uses mathematical concepts & algorithms for key generation, encryption & decryption to protect data in communication, web browsing, digital transactions & more

Features of Cryptography:

- Confidentiality: only intended recipients can access the information.
- Integrity: Data cannot be modified unnoticed.
- Authentication: confirms the identity of sender & receiver.
- Non-repudiation: The sender cannot deny sending the message.

Types of Cryptography

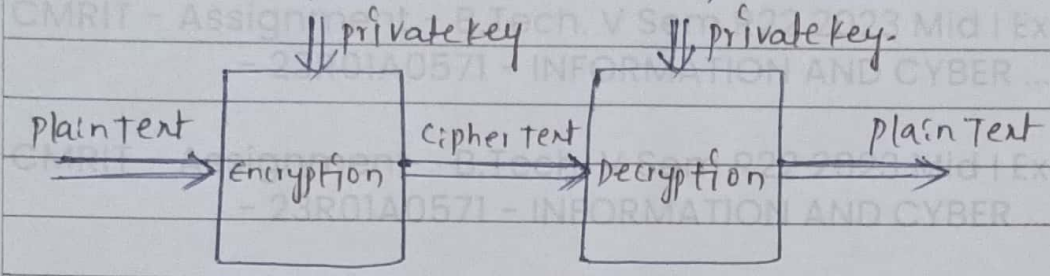
1. Private key Cryptography (Symmetric)
2. Public key Cryptography (Assymmetric)

Private key Cryptography:

Private key cryptography also called symmetric key cryptography uses the same secret key for both encryption & decryption. Both the sender & the receiver must posses this key, which must be kept strictly confidential.

How private key Cryptography Works:

1. Key Generation: A single secret key is generated & securely shared b/w sender & receiver.
2. Encryption: The sender uses the secret key to convert plaintext into cipher text.
3. Decryption: The receiver uses the same secret key to convert ciphertext back to plaintext.



Example Algorithms:

- DES (Data Encryption Standard).
- AES (Advanced Encryption Standard.

Advantages:

- Fast & efficient for large data volumes.
- simple design & implementation.

Applications:

- securing emails, files & VPNs
- Digital signatures.
- SSL/TLS for secure web browsing.
- IoT security & two-factor authentication.
- Key Distribution: securely sharing the key is difficult, especially with many users.
- Key Management: If the key is compromised, all messages are vulnerable.

4. Explain the purpose of PGP (Pretty Good Privacy). How does it ensure secure email communication.

Pretty Good Privacy (PGP) is a robust encryption standard used primarily to secure email communications and ensure data privacy, confidentiality & authenticity in digital correspondence.

Purpose of PGP:

PGP was developed to protect sensitive electronic communications especially emails from unauthorized access, eavesdropping, alteration or impersonation. By doing so, it empowers individuals, organizations, journalists & activists to communicate confidentially over inherently insecure networks like the Internet. PGP also enables users to verify the identity of correspondents & check that messages were not tampered with in transit.

How PGP Ensures Secure Email Communication:

PGP secures email through a combination of symmetric & asymmetric encryption mechanisms:

- Confidentiality: The sender uses the recipient's public key to encrypt a randomly generated session key, which is then used to encrypt the actual email content. Only the recipient in possession of the matching private key, can decrypt the session key & thus the message.

• Authentication & Integrity:
The sender can digitally sign the email using their private key. The recipient can verify the signature with the sender's public key, ensuring the message truly originated from the claimed sender & was not altered in transit.

• End-to-End Encryption:

Unlike standard email, which may be stored encrypted on servers, PGP ensures that only those with the proper private key can read the message - even the email service provider cannot decrypt or access the content.

Core security properties provided by PGP

• Encryption: Prevents all unauthorized parties from reading the message.
• Digital Signatures (Authentication & Non-repudiation): Allows the recipient to verify the sender's identity & assure the message's origin.
• Integrity checks:
Ensures that the contents of the message have not been tampered with or altered during transmission.
• Web of Trust Model: Rather than relying solely on certificate authorities, PGP users can vouch for one another's public keys, increasing resilience.

5> Discuss about implementation of cryptographic techniques - OpenSSL.

- OpenSSL is an open source toolkit that provides implementations of Secure Sockets Layer (SSL), Transport Layer Security (TLS) protocols & a robust library for cryptographic functions.
- It supports symmetric key encryption, asymmetric encryption (public/private keys), hashing & digital certificates.
- It is widely used in securing communications over the internet. (e.g. HTTPS, VPNs, email security).

Q. Major Cryptographic Techniques in OpenSSL.

a) Symmetric Key Encryption (private key)

- Same key used in enayption & decryption.
- Ex algorithms: AES, DES, 3DES, chacha20.
- Implementation with OpenSSL (AES-256 encryption)

```
#Encrypt a file
openssl enc -aes-256-cbc -in input.txt -out encrypted.txt
                                        -k secretkey.
#Decrypt a file
openssl enc -d -aes-256-cbc -in encrypted.txt -out
                                    decrypted.txt -k secretkey
```

b> Public key Cryptography (Asymmetric)

- Uses a public key for encryption & private key for decryption.
- Ex: RSA
- Implementation with OpenSSL (RSA):

```
# generate private key
openssl genrsa -out private.pem 2048
# Extract public key
openssl rsa -in private.pem -pubout -out public.pem
# Encrypt using public key
openssl rsautl -encrypt -pubin -inkey public.pem -in
                    input.txt -out encrypted.bin
# Decrypt using private key
openssl rsautl -decrypt -inkey private.pem -in encrypted
                    .bin -out decrypted.txt.
```

c) Hashing

- Hash functions convert data into a fixed-length string, ensuring integrity.
- Ex algorithms: MD5, SHA-256, SHA-512
- Implementation with OpenSSL:

```
# Generate SHA-256 hash
openssl dgst -sha256 file.txt.
```

d) Digital Signatures

- provide authentication & integrity verification using asymmetric cryptography.
- Implementation with OpenSSL:

```
# Create a signature (private key)
openssl dgst -sha256 -sign private.pem -out sign.bin file.txt
# Verify the signature (public key)
openssl dgst -sha256 -verify public.pem -signature sign.bin
                    file.txt.
```

e) Digital certificates

- Used in SSL/TLS for secure communication
- Implementation with OpenSSL:

Generate a self-signed certificate

```
openssl req -x509 -newkey rsa:2048 -keyout key.pem
            -out cert.pem -days 365
```

3. Applications:

- Securing web servers with HTTPS
- Encrypting files for confidentiality
- Generating & verifying digital signatures.
- Creating & managing digital certificates.