📘 UNIT-1: Attacks on Computers & Computer Security (Short Notes)

Introduction

Computer security protects data, devices, and networks from unauthorized access, misuse, modification, or destruction.

Need for Security

- Protect confidentiality, integrity, and availability (CIA).
- Prevent financial loss, reputation damage, cyber-attacks.

Security Approaches

1. **Layered Security** – multiple defenses.
2. **Security by Design** – integrate security during system design.
3. **Security by Obscurity** – hiding system details.
4. **Proactive and Reactive Approaches**.

Principles of Security

- **Confidentiality** – no unauthorized access.
- **Integrity** – no unauthorized modification.
- **Availability** – system accessible when needed.
- **Authentication**
- **Authorization**
- **Non-repudiation**

Types of Security Attacks

- **Passive**: Eavesdropping, traffic analysis.
- **Active**: Modification, replay, masquerading, DoS.
- **Insider Attacks**
- **Malware-based attacks**

Security Services

- Confidentiality

- Integrity
- Availability
- Authentication
- Non-Repudiation
- Access Control
- Auditing/Monitoring

Security Mechanisms

- Encryption
- Digital Signatures
- Authentication protocols
- Access control mechanisms
- Firewalls, IDS, IPS

A Model for Network Security

Sender → Encryption → Secure Channel → Decryption → Receiver
Uses **algorithm + key + secure services**.

📘 Cryptography Concepts & Techniques

Plain Text & Cipher Text

- **Plain Text** – original message.
- **Cipher Text** – encrypted unreadable form.

Substitution Techniques

Replace characters with other characters.
Examples: Caesar Cipher, Monoalphabetic Cipher.

Transposition Techniques

Rearrange characters without altering them.
Examples: Rail Fence, Columnar Transposition.

Encryption

Convert plaintext → ciphertext using a key.

Decryption

Convert ciphertext → plaintext using the same or another key.

Symmetric Key Cryptography

- Same key for encryption and decryption.
- Fast.
- Examples: DES, AES.

Asymmetric Key Cryptography

- Two keys: Public + Private.
- Slower but more secure.
- Examples: RSA, Diffie-Hellman.

Steganography

Hiding data inside other media (image/audio/text).

Key Range and Key Size

- Larger key size → stronger security.
- Keyspace = total possible keys.

Types of Attacks

- Brute force
- Cryptanalysis
- Dictionary attack
- Man-in-the-middle
- Replay attack

📘 UNIT-2: Symmetric Key Ciphers (Short Notes)

Block Cipher Principles

- Encrypts data in fixed-size blocks (e.g., 64-bit, 128-bit).

DES (Data Encryption Standard)

- 64-bit block size, 56-bit key.
- Uses Feistel structure.

AES (Advanced Encryption Standard)

- 128-bit block size.
- Key sizes: 128, 192, 256 bits.
- Uses SubBytes, ShiftRows, MixColumns, AddRoundKey.

Block Cipher Modes

- **ECB** – simple, less secure.
- **CBC** – uses IV, more secure.
- **CFB** – stream-like mode.
- **OFB** – error-resistant.
- **CTR** – parallel encryption.

Stream Ciphers

Encrypt data bit-by-bit/byte-by-byte. (Fast)
Example: **RC4**

RC4

- Simple stream cipher.
- Uses variable key length (40–256 bits).

Location & Encryption Placement

- Link layer, network layer, application layer encryption depending on need.

Key Distribution

- Sharing symmetric keys securely.
- Techniques: KDC, Diffie-Hellman, public key encryption.

📘 UNIT-3: Asymmetric Key Ciphers (Short Notes)

Principles of Public Key Cryptosystems

- Uses **public–private key pairs**.
- Public key for encryption, private for decryption.
- Provides confidentiality & authentication.

RSA Algorithm

- Based on factoring large prime numbers.
- Public key (n, e), Private key (d).
- Encryption: $C = M^e \bmod n$
- Decryption: $M = C^d \bmod n$

Diffie-Hellman Key Exchange

- Exchanges secret keys over insecure channels.
- Based on discrete logarithm problem.

Key Distribution

- Certificates, PKI, trusted authorities.

📘 UNIT-4: Message Authentication & Hash Functions

Authentication Requirements

- Validate identity.
- Ensure message integrity.
- Prevent modification or impersonation.

Message Authentication Code (MAC)

- Uses secret key + message.
- Provides integrity & authenticity.

Hash Functions

- One-way functions.
- Fixed output size.

- Examples: SHA, Whirlpool.

Secure Hash Algorithm (SHA)

- SHA-1 (160-bit), SHA-256, SHA-512 (modern).

Whirlpool

- 512-bit hash function, highly secure.

HMAC

- MAC based on hashing + secret key.

Digital Signatures

- Sender signs with private key.
- Receiver verifies with public key.
- Provides authentication & non-repudiation.

Authentication Applications

- **Kerberos** – ticket-based authentication.
- **X.509 Certificates** – used in SSL.
- **Public Key Infrastructure (PKI)** – certificate management.
- **Biometric Authentication** – fingerprints, iris, face.

📘 UNIT-5: E-Mail Security

Pretty Good Privacy (PGP)

- Uses hybrid encryption (symmetric + asymmetric).
- Ensures confidentiality, integrity, authentication.

S/MIME

- Secure Multipurpose Internet Mail Extensions.
- Provides encrypted & signed emails.

IP Security (IPSec) Overview

Secures IP packets in network communication.

IPSec Architecture

- AH (Authentication Header)
- ESP (Encapsulating Security Payload)
- IKE (Key management)

Authentication Header (AH)

- Provides integrity, authentication.

Encapsulating Security Payload (ESP)

- Provides confidentiality + integrity.

Security Associations

- Defines encryption/authentication parameters.

📘 UNIT-6: Web Security & Intruders, Viruses, Firewalls

Web Security Considerations

- Protect data transmitted over web.
- Defend against XSS, CSRF, SQL injection.

SSL/TLS

- Provides secure communication using certificates.
- Uses asymmetric + symmetric encryption.

Secure Electronic Transaction (SET)

- Designed for secure credit card payments.

Intruders

- Hackers attempting unauthorized access.
- Types: Masquerader, Misfeasor, Clandestine user.

Intrusion Detection

- **Signature-based IDS**
- **Anomaly-based IDS**

Password Management

- Strong password policies.
- Password hashing.

Virus & Related Threats

- Worms, Trojans, spyware, ransomware.

Countermeasures

- Anti-virus, patching, backups, IDS/IPS.

Firewall Design Principles

- Enforces access control.
- Packet filtering, proxy, stateful inspection.

Types of Firewalls

- Packet filter firewall
- Stateful firewall
- Application-level gateway
- Circuit-level gateway

📘 **Case Studies on Cryptography & Security**

Secure Inter-Branch Payment Transactions

- Uses encryption + digital signatures.
- Ensures authenticity between bank branches.

Cross-Site Scripting (XSS) Vulnerability

- Injecting malicious scripts into web pages.
- Prevent using input validation & sanitization.

Virtual Elections

- Use of cryptography for secure electronic voting.
- Ensures voter privacy, integrity, and authentication.