Applied Cryptography.

Mod 1

- Security goals.

1] Confidentiality.

↳ It refers to the principle of keeping sensitive information secure and only accessible to authorized individual or entities.
For example
A software company develops a new application and shares confidential details with employees. If an employee leaks the code to a competitor, it would violate the confidentiality.

2] Intigrity

↳ It means that changes need to be done only by authorized entities and through authorized mechanism.
For example.
when you transfer money online, the Banking system ensures that the correct amount is debited from your account and Credited to recipient. If a hacker tries to modify the transaction amount during transfer, integrity checks (such as cryptographic hash function) prevents unauthorized changes.

3] Availability.

↳ It refers to ensuring that systems, data, and services are accessible and operational when needed, without unexpected downtime and failuare.

For example:

Google drive ensures availability by mainkaing multiple server worldwide. even if one server fails, user can still access their files from another backup server.

→ Vulnerability

- A weakness in a system, network or Software that can be exploited
- e.g. An Outdated operating System with unpatched security flaws.

→ Threat

- A potential danger that can exploit a vulnerability.

eg. Hackers, malware, phishing.

→ Attack

- The actual act of exploiting a Velnerability to Compromise a System.

e.g A DDoS attack floods a website.

Attack Threatening Confidentiality.

- Snooping :- Snooping refers to a unauthorized access to or interception of data. For example. A File transfered through the Internet may contain Confidential information An unauthorized entity may intercept the transmission and use the content for her own benifits.

- Traffic Analysis :- Although encipherment of data may make it non intelligible for the interceptor, she can obtain some other type information by monitoring online traffic For example she can find the email address for both sender and Receiver. She can called pair Requests and Responses to help her guess the nature of transaction.

Attack Threatening Integrity.

- Modification :- After intercepting or accessing information, the attacker modifies the information to make it beneficial to herself.

- Masquerading :- Masquerading or spoofing happens when attacker ~~impo~~ impersonates somebody else.

- Replaying :- The attacker obtain a copy of a message sent by a user and later tries to replay it.

- Repudiation :- It refers to the act of denying participation in transaction or Communication.

Attacks Threatening Availability.

- Denial of Service :- A DoS attack is a cyberattack that aims to make a system, network, or service unavailable by overwhelming it with excessive traffic.

* Security Services.

1] Data Confidentiality
↳ Data confidentiality services are security measures designed to protect sensitive data from unauthorized access; disclosure, theft.

2] Data Integrity
↳ Data integrity is designed to protect data from modification, insertion, deletion and Replaying by adversary.

3] Authentication
↳ This service provides the authentication of the party at the othe end of line.

4] Nonrepudiation
↳ Nonrepudiation service protects against repudiation by either of the sender or the receiver of the data.

5] Access control
↳ It provides protection against unauthorized access of data.

Security Mechanisms.

- Encipherment.
  - Encipherments hiding or covering data can provide confidentiality. Today two techeniques - Cryptography and Steganography are used for encipherment.

- Digital Signature
  → A digital signature is a means by which the sender can electronically sign the data and Receiver can electronically verify the signature.

- Authentication exchange
  → In Authentication exchange two entities exchange some message to prove their identity to each other.

- Traffic padding
  → Traffic padding means inserting some bogus data into the data traffic.

- Routing Control
  → It means continuously changing different available Routes between Sender and Receiver.

- Notarization
  → It means selecting third ~~party~~ trusted party to control communication between two entities.

Encryption.

↳ It is the process of converting plain text into ciphertext using an encryption algorithm and key.

This ensures that only authorised parties can access the original information.

example Converting "Hello" into "xqz#@!" using an encryption algorithm.

Decryption

↳ It is the reverse process of encryption where the ciphertext is converted bg back into plain text using decryption algorithm.

Only users with the correct decryption key can access the orignal Message

example Converting "xqz#@!" bac to "Hello".

Types of Encryption

1) Symmetric Encryption

2) Asymmetric Encryption.

Symmetric Encryption	Asymmetric encryption
→ Single key for encryption and decryption	Public key for encryption and private key for decryption.
→ It is faster	It is slower due to complex computation.
→ Less secure	More secure
→ Used to encrypt large amount of data.	Used for secure communication, digital signature.
→ Key must be securely shared.	No need to share private key.
→ e.g. AES DES 3DES	RSA ECC Diffie Hellman.

Types of key.

1] Symmetric key

→ Same key for encryption & Decryption
→ Used in Secure file storage, VPN.
→ AES, DES, BlowFish.

2] Asymmetric key

→ Public key for encryption, private key for decryption.
→ Secure Communication, Digital signature.
→ RSA, ECC.

3] Session key

→ Temporary key used for a single session.
→ Online Banking, HTTPS
→ AES

4] Pre-Shared key

→ A shared secret key exchange before communication
→ WiFi Security
→ WPA2, IPsec.

5] Private Key.

→ Used for decryption and digital signature
→ Digital signature, blockchain.
→ RSA, ECC.

6] Public key.

→ Used for encryption and verifying digital signature
→ HTTPS security, email encryption
→ RSA, ECC, PGP.

7] Master key

→ Used to generate other key in key management.
→ Database encryption, cloud security
→ Key Management System (KMS).

Cryptanalysis Method.

1] Brute Force Attack.

→ Tries all possible key
→ Cracking weak passwords.

2] Ciphertext - Only Attack.

→ Analyze Ciphertext pattern
→ Frequency analysis on classical cipher.

3] Known - Plaintext Attack

→ Uses known plaintext and corresponding Ciphertext.
→ WWII Enigma machine attack.

4] Chosen - Plaintext Attack

→ Encrypts controlled plaintext and observe Ciphertext.
→ Attacks on RSA encryption.

5] Chosen - Ciphertext attack

→ Decrypts controlled Ciphertext and observe plaintext.
→ Bleichenbacher's attack on RSA.

6] Side - Channel Attack.

→ Analyzes power, timing, or electromagnetic leaks.
→ Timing attacks on RSA.

7] Differential Cryptanalysis.

→ Studies input-output differences in a cipher.
→ Breaking DES.

8] Linear Cryptanalysis.

→ Uses linear approximations to analyze encryption
→ Breaking weak block ciphers.

9] Man in the middle Attacks.

→ Intercepts and modifies communication.
→ Attacking weak HTTPS sessions.

10] Birthday Attack

→ Exploits hash function collision.
→ Breaking MD5, SHA-1 hashes.

Classical cryptography.

1) Substitution Encryption.
   ↳ In Substitution Ciphers, each letter or symbol in the plain text is replaced with another letter, ~~with~~ numbers or symbol.

Types of Substitution Cipher.

- Ceasar Cipher - Each letter is shifted by a fixed number of position in the alphabet
- Monoalphabetic Cipher - Each letter is replaced with a fixed different letter, forming a one-to-one mapping.
- Playfair Cipher - Uses 5x5 grid of letters to encrypt digraph (pair of letter) instead of single letters.

Strengths	weakness
• Simple and easy to implement	Vulnerable to frequency analysis.
• More secure than plaintext communication	Can be broken with pattern recognition or Brute Force attack.

2] Transposition Encryption.

↳ In transposition encryption the letter of plaintext Remain same but their positions are rearranged according to fix Rule.

Types of Transposition Encryption.

- Rail Fence Cipher - Text is written in a zig zag pattern across multiple lines then read Row by Row.
- Columnar Cipher - The plaintext is written in a grid and columns are Rearranged based on a Keyword.

Strengths

- No chance in letter frequency, making it resistant to frequency analysis.
- Can be combined with substitution for stronger encryption.

Weakness

Still vulnerable to pattern analysis and anagram-solving techniques.

Block Cipher	Stream Cipher.
Encrypts data in fixed size blocks (e.g. 64-bit 128 bit).	Encrypts data bit by bit or byte by byte.
works on block of plaintext at a time	Encrypts data in a continuous stream.
Uses same key for the entire block	Generates a key stream dynamically.
Slower due to processing entire block at once.	Faster since encryption is done on small units of da
Suitable for file encryption and database Security	Preffered for Real-time Communication like Vido streaming etc.
AES, DES, Blowfish	RC4, Salsa20, Chacha20.

MOM [Method, Opportunity, Motive].

1] Method - The technique or tools used to carry out an attack.

2] Opportunity - The vulnerability or weakness in a system that can attacker can exploit.

3] Motive - The Reason behind the attack.

Why MOM is Important?

- Helps in identifying potential threats before they occur.
- Assist in Risk assessment and mitigation strategies.
- Enable security teams to prioritize defenses based on attacker's possible method and motives.