18/8

HA-1

A. Saketh Ram
2200080049

1. Crytograph is the science of securing information by transforming it into an unreadable format, which only be converted back to its original form by someone who possesses the proper key. This process helps in ensuring the confidentiality, integrity and authenticity of data.

Symmetric key cryptography:

In symmetric key cryptograph, the same key is used for both encryption and decrytion. This means that both the sender and the receiver most share the same secret key.

Asymmetric key cryptograph:

Asymmetric key cryptograph, also known as public-key cryptograph, uses a pair of keys: a public key and a private key. The public key is shared openly while the private key remains confidential.

2. Types of Attacks on Cryptosystems:

1. **Brute Force Attack:**

- An attacker tries every possible key combination until the correct one is found.

- Defense: Use large key sizes to make brute force attacks computationally infeasible.

2. **Cryptanalysis:**

- The attacker analyzes the encryted data to find patterns or weaknesses in the encryption algorithm to break it.

- Defense: Use strong encryption algorithms with proven resistance to cryptanalysis.

3. **Mean-in-the-Middle Attack (MITM):**

- The attacker intercepts the communication between two parties and may alter the communication without the knowledge o either party.

- Defense: Use public key infrastructure (PK and digital certificates to authenticate communication.

4. Reply Attack:

- An attacker captures and retransmits a valid data transmissions to produce an unauthorized effect.
- Defense: Use timestamps and unique session tokens to prevent the reuse of old data.

5. Side-channel Attacks:

- The attacker exploits physical characteristics of the cryptosystem, such as timing information, power consumption, or electromagnetic leaks.
- Defense: Implement countermeasures like masking and hiding, and ensure proper physical security.

3. RSA Encryption and Decryption algorithm:

RSA Encrytion:

1. Choose two large prime numbers ppp & qqq.
2. Compute n=pxqn=p\times qn=pxq, where nnn is the modulus for both the public and private keys.

3. Calculate the totient ϕ(n) - (p-1) × (q-1)\phi(n) = (p-1) \ times (q-1) ϕ(n) = (p-1) × (q-1).

4. choose a public exponent eee such that 1 < e < ϕ(n)1 < e < \phi(n) 1 < e < ϕ(n) and eee is co-prime with ϕ(n)\phi(n)ϕ(n).

5. compute the private key ddd such that d×e = 1 mod ϕ(n) d \ times e \ equiv 1 \mod \ phi(n) d×e = 1 mod ϕ(n).

6. The public key is (e,n)(e,n)(e,n) and the private key is (d,n)(d,n)(d,n).

RSA Decryption process!

To decrypt the ciphertext ccc, compute th original message as m = cd mod nm\equiv c^d \mod nm = cd modn.

4. Elliptic Curve Cryptography (ECC):-

characteristics of ECC:

- ECC is based on the mathematics of elliptic curves over finite fields
- It provides the same level of security as other public key systems like RSA but with much smaller key sizes.
- Ex:- A 256-bit key in ECC offers comparable security to a 3072-bit key is RSA.

Encryption Process:

1. Both the sender and receiver agree on an elliptic curve EEE and a base point GGG.
2. The receiver generates a private key kprk_{pr} kpr and computes the public key kpu=kpr×GK_{pu}=k_{pr}\times Gkpu=kpr×G
3. The sender uses the receiver's public key kpuk_{pu} kpu and their own private key to generate a shared secret.
4. The shared secret is used to encrypt the message.

- The receiver uses their private key kprk. {pr} kpr and the sender's public key to generate the same shared secret and decrypt the message.

5. Hashing and SHA-256

Hashing:

- Hashing is a process that converts an input into fixed-size string of bytes. The output, known as the hash value, it typically a digest that uniquely represents the input data.
- Hash functions are designed to be fast and irreversible, meaning it should be computationally infeasible to generate the original input from the hash value

SHA-256:

- SHA-256 is part of the SHA-2 family of cryptographic hash functions, designed by the NSA.

- It produces a 256 bit hash value, usuall rendered as a hexadecimal number

Characteristics:

-> Deterministc

-> Quick computation

-> Collision-resistant

-> Pre-image resistant

-> Applications

6. Message Authentication Code (MAC):

MAC:

A MAC is a small piece of information used to authenticate a message. It ensures the message's integrity and authenticity.

For Authentication:

The MAC guarantees that the message was generated by someone who knows the secret key and that the message has not been tampered with.

For Confidentiality:

While a MAC does not inherently provide confidentiality, it can be combined with encryption algorithms to ensure both confidentiality and authentication.