Home Assignment -1

1. Define cryptography, explain symmetric key cryptography and asymmetric key cryptography
2. Explain types of attack can be possible in cryptosystem
3. Explain RSA encryption, Decryption algorithm and its advantages
4. Demonstrate the characteristics of Elliptic Curve Cryptography (ECC), Encryption and Decryption and it can be used as a digital signature
5. Explain Hashing and write short notes on SHA-256
6. Explain Message Authentication Code (MAC) for both cases Authentication and Confidentiality obtained.

1. Cryptography: Definition and Key Types

Cryptography is the science of securing information by transforming it into an unreadable format, which can 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 cryptography, the same key is used for both encryption and decryption. This means that both the sender and the receiver must share the same secret key.

Asymmetric Key Cryptography:

- Asymmetric key cryptography, also known as public-key cryptography, uses a pair of keys: a public key (for encryption) and a private key (for decryption). 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 encrypted data to find patterns or weaknesses in the encryption algorithm to break it.
    - **Defense:** Use strong encryption algorithms with proven resistance to cryptanalysis.
3. **Man-in-the-Middle Attack (MITM):**
    - The attacker intercepts the communication between two parties and may alter the communication without the knowledge of either party.
    - **Defense:** Use public key infrastructure (PKI) and digital certificates to authenticate communication.

4. **Replay Attack:**
    - An attacker captures and retransmits a valid data transmission 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 Encryption:

1. Choose two large prime numbers ppp and qqq.
2. Compute n=p×qn = p \times qn=p×q, 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≡1mod ϕ(n)d \times e \equiv 1 \mod \phi(n)d×e≡1modϕ(n).
6. The public key is (e,n)(e, n)(e,n), and the private key is (d,n)(d, n)(d,n).

RSA Encryption Process:

- To encrypt a message MMM, convert MMM into an integer mmm such that 0≤m<n0 \leq m < n0≤m<n.
- The ciphertext CCC is computed as C≡memod nC \equiv m^e \mod nC≡memodn.

RSA Decryption Process:

- To decrypt the ciphertext CCC, compute the original message as m≡Cdmod nm \equiv C^d \mod nm≡Cdmodn.

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.
- **Example:** A 256-bit key in ECC offers comparable security to a 3072-bit key in RSA.

ECC 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.

ECC Decryption Process:

- 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 (or "message") into a fixed-size string of bytes. The output, known as the hash value, is 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.
- Hash functions play a crucial role in various security applications, including digital signatures, message integrity checks, and password storage.

SHA-256 (Secure Hash Algorithm 256-bit):

- SHA-256 is part of the SHA-2 family of cryptographic hash functions, designed by the NSA.
- It produces a 256-bit (32-byte) hash value, usually rendered as a hexadecimal number.
- **Characteristics:**
    - **Deterministic:** The same input will always produce the same hash.
    - **Quick computation:** SHA-256 can compute a hash efficiently, even for large amounts of data.
    - **Collision-resistant:** It is computationally infeasible to find two different inputs that produce the same hash value.
    - **Pre-image resistance:** It is infeasible to determine the original input given its hash.
    - **Applications:** Digital signatures, SSL certificates, blockchain, and more.

6. Message Authentication Code (MAC)

Message Authentication Code (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 (since it doesn't encrypt the message), it can be combined with encryption algorithms to ensure both confidentiality and authentication. For example, encrypt the message first and then generate a MAC for the ciphertext.