Q.1. What are the pros and cons of public-key cryptography? (4 points)

Ans:

Public-key cryptography is a type of encryption that encrypts and decrypts data using two separate keys called public key and private key.

- Pros or Advantages:
- Easy key distribution.
- No longer need to assume that Alice and Bob already share a secret.
- Cons or Disadvantages:
- Much slower than symmetric-key cryptography.
- Number theory calculations are much slower than XORs and bit-shifts.

Q.2. What are the properties of public key encryption? (4 points)

Ans:

- Correctness: Decrypting a ciphertext should result in the message that was originally encrypted.

Dec(SK, Enc(PK, M)) = M for all PK, SK from KeyGen() and M.

- Efficiency: Encryption/decryption should be fast.
- Security: Computationally infeasible to recover M with PK and ciphertext.

Q.3. Describe the steps of public key encryption with example (4 points)

Ans: Steps for Public Key Encryption:

1. Generate a pair of keys.
2. Keep the private key (SK) and distribute the public key (PK).
- Place PK in a public register or other accessible file.
3. Bob encrypts the message with Alice's PK.
4. Upon receiving the ciphertext (CT), Alice decrypts CT with SK.

Q.4. Which categories should be used to classify public key cryptography algorithms? (4 points)

Ans:

There are three categories used to classify public key cryptography algorithms:

1. Encryption/Decryption: Provides secrecy to the key.
2. Digital Signatures: Provides authentication.
3. Key Exchange: Consists of session keys.

Examples of algorithms:

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No
Elliptic Curve	Yes	Yes	Yes

Q.5. Write RSA encryption and decryption algorithms. Suppose the public key {e, n} and private key {d, n} are given. (4 points)

Ans:

RSA Encryption Algorithm:

1. Given a message M and a public key \{e, n\} , create an integer m from the message M such that 0 \leq m < n .
2. Make the ciphertext c as c = m^e \mod n .
3. Return the ciphertext c .

RSA Decryption Algorithm:

1. Compute the plaintext p as p = c^d \mod n .
2. Convert the plaintext p back into the original message M .

Q.6. What are the possible attacks exploiting RSA's properties? (4 points)

Ans:

1. Mathematical Attacks: Several approaches, all equivalent in effort to factoring the product of two primes. Defense: Use a large key size.
2. Timing Attacks: These depend on the running time of the decryption algorithm.

3. Chosen Ciphertext Attacks: Exploits properties of the RSA algorithm by selecting blocks of data. These attacks can be thwarted by suitable padding of the plaintext, such as PKCS1 V1.5 in SSL.

Q.7. What is meant by message authentication? (4 points)

Ans:

Message authentication is concerned with:

1. Protecting the integrity of a message.
2. Validating the identity of the originator.
3. Non-repudiation of origin (dispute resolution).

Q.8. What are the 3 approaches to achieve message authentication? (4 points)

Ans:

Message authentication is the process of verifying the integrity and authenticity of a message. The three approaches are:

1. Message Encryption:

- Provides a measure of authentication.
- If symmetric encryption is used:

1. Receiver knows sender who must have created the message.
2. Only the sender and receiver know the key used.
3. Known content cannot be altered.

- If public-key encryption is used:

1. Encryption provides no confidence of sender.
2. Since anyone potentially knows the public key, recognition of corrupted messages is necessary.

2. Message Authentication Code (MAC):

- Uses a cryptographic technique with a secret key to verify message integrity.

3. Digital Signatures:

- Uses the sender's private key to sign the message and the corresponding public key to verify authenticity.

Q.9. What are the pros and cons of single-key cryptography? (4 points)

Ans:

- Pros:

1. Encryption is fast for large amounts of data.
2. Provides the same level of security with a shorter encryption key.
3. By now, it's unbreakable to quantum computing.

- Cons:

1. Key distribution assumes a secure channel.
2. Does not protect sender from receiver forging a message and claiming it's sent by the sender.
3. Does not scale well for large networks (requires separate keys for each pair).

Q.10. List and explain the requirements for a secure hash function. (4 points)

Ans:

1. Can be applied to any sized message M.
2. Produces fixed-length output h.
3. Easy to compute $h = H(M)$.
4. Preimage Resistance: Infeasible to find x such that $H(x) = h$.
5. Second Preimage Resistance: Given x, infeasible to find $x{\prime}$ such that $H(x) = H(x{\prime})$.
6. Collision Resistance: Infeasible to find any pair $x, x{\prime}$ such that $H(x) = H(x{\prime})$.

Q.11. What is the weakness of hash functions? (4 points)

Ans:

1. Collision: Multiple inputs produce the same hash.
2. Length Extension Attack: Extending the hash for malicious purposes.
3. Man-in-the-Middle Attack: Hash intercepted and altered.

Q.12. How many solutions guarantee the integrity of a hash function? (4 points)

Ans:

1. Message Authentication Code (MAC):

- Created using a secret symmetric key to ensure the integrity of a message.

2. Digital Signature:

- The sender generates a message digest, signs it with their private key, and sends it.
- The recipient decrypts the digest using the sender's public key and compares it with the locally generated digest for verification.

Q.13. Does hashes provide integrity? Explain with scenarios. (4 points)

Ans:

Scenario 1:

- Mozilla publishes a new version of Firefox.
- Alice downloads the program binary.
- Alice checks the hash published by Mozilla against the binary she downloaded.
- If the hashes match, the integrity is verified.

Scenario 2:

- Alice and Bob communicate over an insecure channel.
- David intercepts and modifies the message.
- Using cryptographic hashes, Alice and Bob can detect tampering if the hash values do not match.

Q.14. What is the definition and properties of a Message Authentication Code (MAC)? (4 points)

Ans:

Definition:

A cryptographic scheme using a secret key to verify the integrity and authenticity of a message.

Properties:

1. Correctness: Verifies if the received message matches the original message.
2. Determinism: Consistently produces the same MAC for identical inputs.

3. Efficiency: Fast computation for large-scale use.

Q.15. What are the properties of HMAC? (4 points)

Ans:

1. Collision Resistance: Prevents two different inputs from producing the same output.
2. Determinism: Ensures consistent results for identical inputs.
3. Key Protection: Secure against brute-force attacks.
4. Efficiency: Fast for verification and generation.

Q.16. How many keys are produced by HMAC? What are the keys and how are they generated? (4 points)

Ans:

1. Two Keys: An outer key and an inner key.
2. Outer Key: Derived by XOR-ing the original key with a padded value.
3. Inner Key: Derived by XOR-ing the original key with a different padded value.

Q.17. What is authenticated encryption? Explain two approaches to achieve it. (4 points)

Ans:

Definition:

Authenticated encryption ensures both the confidentiality and authenticity of a message.

Approaches:

1. Encrypt-then-MAC:

- Encrypt the plaintext.
- Generate a MAC for the ciphertext.

2. MAC-then-Encrypt:

- Generate a MAC for the plaintext.
- Encrypt both the plaintext and MAC.

Preferred Approach: Encrypt-then-MAC is considered more secure and robust.

Q.18. What are the characteristics of the output hash function? (4 points)

Ans:

1. Deterministic: Produces the same output for identical inputs.
2. No Randomness: Ensures identical results in deterministic environments.

Q.19. What is a digital signature and describe its properties? (4 points)

Ans:

Definition:

A digital signature is a cryptographic scheme that provides verification of the origin and integrity of a message using private and public keys.

Properties:

1. Correctness: Verifies the message's integrity.
2. Efficiency: Quick generation and verification.
3. Non-repudiation: Prevents sender from denying their signature.

Q.20. Describe the steps of RSA digital signature algorithm. (4 points)

Ans:

1. Generate a hash value or message digest from the message.
2. Sign the hash value with the private key.
3. Send the message and signature to the recipient.
4. The recipient verifies the signature using the sender's public key.

Q.21. What method has been used to guarantee RSA Digital Signature? (4 points)

Ans:

Necessary Hardness Assumptions:

1. Factoring Hardness: Difficult to factorize large primes.

2. Discrete Logarithm Hardness: Difficult to compute discrete logarithms in large fields.
3. Salt Usage: Ensures additional randomness for uniqueness.

Q.22. What are the issues with public-key encryption? What method is used for large data encryption? (4 points)

Ans:

Issues:

1. Inefficient for large data due to computational overhead.
2. Limited to small messages due to modulo operator restrictions.

Solution:

Hybrid Encryption:

1. Encrypt the data using symmetric encryption with a randomly generated key .
2. Encrypt with public-key encryption.