CRYPTOGRAPHY INTERVIEW QUESTIONS

1.What is cryptography?

Answer: Cryptography is the practice and study of techniques for securing communication and data from adversaries by transforming information into secure formats that only intended recipients can read and process.

2.What is the difference between symmetric and asymmetric cryptography?

Answer: Symmetric cryptography uses the same key for both encryption and decryption, whereas asymmetric cryptography uses a pair of keys – a public key for encryption and a private key for decryption.

3.Explain the concept of public key infrastructure (PKI).

Answer: PKI is a framework for managing digital keys and certificates. It uses asymmetric cryptography to secure communications and authenticate identities through a hierarchy of trusted certificate authorities (CAs).

4.What is the Advanced Encryption Standard (AES)?

Answer: AES is a symmetric encryption algorithm established by NIST that supports key sizes of 128, 192, and 256 bits. It is widely used due to its efficiency and strong security.

5.What are the main differences between RSA and ECC encryption?

Answer: RSA is based on the difficulty of factoring large integers, while ECC (Elliptic Curve Cryptography) is based on the algebraic structure of elliptic curves over finite fields. ECC offers similar security to RSA but with smaller key sizes, making it more efficient.

6.What is a digital signature and how does it work?

Answer: A digital signature is a cryptographic technique that verifies the authenticity and integrity of a message or document. It uses the sender's private key to sign a hash of the message, which can be verified by the recipient using the sender's public key.

7.What is a hash function, and what are its properties?

Answer: A hash function takes an input and produces a fixed-size string of bytes. Its properties include determinism, preimage resistance, second preimage resistance, collision resistance, and quick computation time.

8.What is the purpose of a cryptographic nonce?

Answer: A nonce is a number that is used only once in cryptographic communication to ensure that old communications cannot be reused in replay attacks. It ensures that each encryption operation produces a unique ciphertext.

9.Explain the concept of key exchange and mention a commonly used protocol.

Answer: Key exchange is the process of securely exchanging cryptographic keys between parties. A commonly used protocol for key exchange is the Diffie-Hellman key exchange, which allows two parties to establish a shared secret over an insecure channel.

10.What is a certificate authority (CA)?

Answer: A CA is a trusted entity that issues digital certificates to verify the identity of entities and their public keys. It plays a central role in PKI by validating and vouching for the authenticity of public keys.

11.What is the purpose of a digital certificate?

Answer: A digital certificate binds a public key to an entity's identity, providing proof that the public key belongs to that entity. It is used to establish trust in online communications and authenticate users, devices, and websites.

12.What is a man-in-the-middle (MITM) attack and how can cryptography prevent it?

Answer: A MITM attack occurs when an attacker intercepts and potentially alters the communication between two parties without their knowledge. Cryptography prevents it by using encryption and digital signatures to ensure confidentiality, integrity, and authenticity of the communication.

13.What is Perfect Forward Secrecy (PFS) in cryptographic communications?

Answer: PFS is a property that ensures that the compromise of long-term keys does not compromise past session keys. It is achieved by generating unique session keys for each communication session, which are not derived from the server's private key.

14.Explain the role of a hashing algorithm in digital signatures.

Answer: In digital signatures, a hashing algorithm creates a hash of the message to be signed. The hash is then encrypted with the sender's private key to create the digital signature. The recipient can decrypt the signature using the sender's public key and compare the hash with the hash of the received message to verify integrity and authenticity.

15.What are some common hashing algorithms and their typical use cases?

Answer: Common hashing algorithms include MD5 (although now considered insecure), SHA-1 (also considered insecure for many applications), and SHA-256 (part of the SHA-2 family, widely used for secure hashing). They are typically used in digital signatures, integrity verification, and password hashing.

16.What is a cryptographic salt and why is it used?

Answer: A cryptographic salt is a random value added to data before hashing to ensure that the same input does not always produce the same hash output. It is used to protect against rainbow table attacks and ensure that identical passwords result in different hashes.

17.Describe the concept of a block cipher and give an example.

Answer: A block cipher encrypts data in fixed-size blocks (e.g., 128 bits) using a symmetric key. An example of a block cipher is AES. Block ciphers can operate in different modes such as ECB, CBC, and CTR to encrypt larger data.

18.What is the difference between a block cipher and a stream cipher?

Answer: A block cipher encrypts data in fixed-size blocks, while a stream cipher encrypts data one bit or byte at a time in a continuous stream. Stream ciphers are typically faster and more suitable for real-time applications.

19.What is Elliptic Curve Digital Signature Algorithm (ECDSA)?

Answer: ECDSA is a variant of the Digital Signature Algorithm (DSA) that uses elliptic curve cryptography. It provides the same level of security as DSA but with smaller key sizes, making it more efficient.

20.What is the role of TLS (Transport Layer Security) in cryptography?

Answer: TLS is a cryptographic protocol designed to provide secure communication over a computer network. It ensures confidentiality, integrity, and authentication of data exchanged between clients and servers, commonly used in securing web traffic (HTTPS).