REAL TIME WORK ON CRYPTOGRAPHY INTERVIEW QUESTIONS

1.What is cryptography?

Answer: Cryptography is the science of protecting information by transforming it into a secure format. The main goal is to ensure confidentiality, integrity, authenticity, and non-repudiation of data.

2.What are the primary goals of cryptography?

Answer: The primary goals of cryptography are:

Confidentiality: Ensuring that information is accessible only to those authorized to access it.

Integrity: Ensuring that information is not altered during storage or transit.

Authentication: Verifying the identity of users and the origin of messages.

Non-repudiation: Ensuring that a sender cannot deny having sent a message.

3.What is the difference between symmetric and asymmetric encryption?

Answer: Symmetric encryption uses the same key for both encryption and decryption, while asymmetric encryption uses a pair of keys (public and private) for encryption and decryption.

4.Can you name some common symmetric encryption algorithms?

Answer: Common symmetric encryption algorithms include Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES (3DES), and Blowfish.

5.What are some examples of asymmetric encryption algorithms?

Answer: Examples of asymmetric encryption algorithms include RSA (Rivest–Shamir–Adleman), DSA (Digital Signature Algorithm), and ECC (Elliptic Curve Cryptography).

6.How does AES encryption work?

Answer: AES (Advanced Encryption Standard) works by dividing data into blocks of 128 bits and encrypting each block using a symmetric key. It employs a series of transformations, including substitution, permutation, mixing, and key addition over several rounds (10, 12, or 14) depending on the key size (128, 192, or 256 bits).

7.What is a public key and how is it used in encryption?

Answer: A public key is part of an asymmetric key pair used to encrypt data. It can be freely distributed and used by anyone to encrypt a message intended for the holder of the corresponding private key, which is used for decryption.

8.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, document, or software. It works by generating a hash of the message and encrypting it with the sender's private key. The recipient can verify the signature by decrypting the hash with the sender's public key and comparing it to a hash of the received message.

9.What is key management and why is it important in cryptography?

Answer: Key management involves the generation, distribution, storage, rotation, and disposal of cryptographic keys. It is crucial for maintaining the security and effectiveness of encryption systems, as the compromise of keys can lead to unauthorized access and data breaches.

10.How are cryptographic keys securely distributed?

Answer: Cryptographic keys can be securely distributed using methods such as:

Public key infrastructure (PKI), which uses asymmetric encryption for secure key exchange.

Key exchange protocols like Diffie-Hellman, which enable two parties to securely share a symmetric key over an insecure channel.

Encrypted key transfer, where keys are encrypted using a pre-shared key or public key before being transmitted.

11.What role does cryptography play in securing online transactions?

Answer: Cryptography secures online transactions by ensuring the confidentiality and integrity of data, authenticating the identities of the parties involved, and providing non-repudiation. It is used in SSL/TLS for secure web communication, digital signatures for verifying transactions, and encryption for protecting sensitive information like credit card details.

12.How is cryptography used in securing emails?

Answer: Cryptography secures emails through encryption and digital signatures. Email encryption, using protocols like PGP (Pretty Good Privacy) or S/MIME (Secure/Multipurpose Internet Mail Extensions), ensures that only the intended recipient can read the content. Digital signatures verify the sender's identity and ensure that the email has not been tampered with.

13.What is a blockchain and how does cryptography support it?

Answer: A blockchain is a distributed ledger technology that records transactions across multiple computers in a way that ensures security, transparency, and immutability. Cryptography supports blockchain by securing transactions through digital signatures, ensuring data integrity with cryptographic hashing, and protecting participant identities with public-key cryptography.

14.What is homomorphic encryption and its potential use cases?

Answer: Homomorphic encryption allows computations to be performed on encrypted data without decrypting it, producing an encrypted result that, when decrypted, matches the result of the operations as if they were performed on the plaintext. Potential use cases include secure data processing in the cloud, privacy-preserving data analysis, and encrypted search.

15.What is quantum cryptography and how does it differ from classical cryptography?

Answer: Quantum cryptography leverages principles of quantum mechanics to secure communication. Unlike classical cryptography, which relies on mathematical complexity for security, quantum cryptography, such as Quantum Key Distribution (QKD), ensures security based on the fundamental properties of quantum particles, making it theoretically immune to certain types of attacks, including those from quantum computers.

16.What is the significance of cryptographic hashing?

Answer: Cryptographic hashing generates a fixed-size hash value from input data, providing a unique digital fingerprint. It is significant for ensuring data integrity, securing passwords, and supporting digital signatures and blockchain technology.

17.How can password security be enhanced using cryptography?

Answer: Password security can be enhanced by:

Using strong, cryptographic hash functions (e.g., SHA-256) with salting to store password hashes.

Implementing multi-factor authentication (MFA) to add additional layers of security.

Using password managers to generate and store complex, unique passwords for different accounts.

18.What is SSL/TLS and how does it secure communications?

Answer: SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security) are cryptographic protocols that secure internet communications by providing encryption, data integrity, and authentication between web browsers and servers. They use a combination of asymmetric and symmetric encryption to establish a secure connection.

19.What is the role of a Certificate Authority (CA) in public key infrastructure (PKI)?

Answer: A Certificate Authority (CA) issues digital certificates that verify the ownership of public keys in a PKI system. The CA acts as a trusted third party that authenticates the identity of certificate holders, ensuring the trustworthiness of secure communications.

20.How is cryptography used in securing IoT (Internet of Things) devices?

Answer: Cryptography secures IoT devices by:

Encrypting data transmitted between devices to ensure confidentiality and prevent eavesdropping.

Using digital signatures to authenticate firmware updates and prevent tampering.

Implementing secure boot processes to ensure that devices run trusted software.