ENCRYPTION INTERVIEW QUESTIONS

1.What is symmetric encryption?

Answer: Symmetric encryption is a type of encryption where the same key is used for both encryption and decryption of data. Common symmetric algorithms include AES, DES, and 3DES.

2.What is asymmetric encryption and how does it work?

Answer: Asymmetric encryption uses a pair of keys – a public key for encryption and a private key for decryption. Examples include RSA and ECC. This method is often used for secure key exchange and digital signatures.

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

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

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

Answer: PKI is a framework that manages digital keys and certificates. It uses a combination of asymmetric encryption and digital signatures to provide secure communication and authentication.

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

Answer: RSA (Rivest-Shamir-Adleman) is an older asymmetric encryption algorithm based on the difficulty of factoring large integers. ECC (Elliptic Curve Cryptography) is a newer, more efficient algorithm that uses the mathematics of elliptic curves to provide similar security with smaller key sizes.

6.What is BitLocker and how does it work?

Answer: BitLocker is a full-disk encryption feature available in Windows. It uses AES encryption to protect data on the entire drive and can utilize TPM (Trusted Platform Module) for secure key management.

7.What is LUKS and what is its role in Linux encryption?

Answer: LUKS (Linux Unified Key Setup) is a standard for disk encryption in Linux. It provides a secure way to encrypt entire partitions and manage multiple encryption keys.

8.How does the Encrypting File System (EFS) in Windows differ from BitLocker?

Answer: EFS is a file-level encryption feature in Windows, allowing individual files and directories to be encrypted. BitLocker, on the other hand, provides full-disk encryption.

9.What are some common tools for encrypting files on Linux?

Answer: Common tools include GnuPG for file encryption, dm-crypt combined with LUKS for disk encryption, and eCryptfs for file system-level encryption.

10.Can you explain the process of setting up full disk encryption on a Linux system using LUKS?

Answer: Setting up full disk encryption with LUKS involves creating a LUKS partition, initializing it with a passphrase, and then formatting the encrypted partition with a file system. The partition can then be mounted and used like any other file system, but all data is encrypted on disk.

11.What is a cryptographic hash function?

Answer: A cryptographic hash function takes an input (or 'message') and returns a fixed-size string of bytes. The output, often called the hash value, should be unique to the given input. Common examples include SHA-256, SHA-3, and MD5.

12.What are the properties of a good cryptographic hash function?

Answer: A good cryptographic hash function should have properties like determinism, preimage resistance, second preimage resistance, collision resistance, and a quick computation time.

13.Explain the concept of a hash collision.

Answer: A hash collision occurs when two different inputs produce the same hash output. A good cryptographic hash function minimizes the likelihood of collisions.

14.What is the difference between SHA-1 and SHA-256?

Answer: SHA-1 produces a 160-bit hash value and is considered weak due to vulnerability to collisions. SHA-256 is part of the SHA-2 family and produces a 256-bit hash value, offering stronger security against collisions.

15.How is hashing used in digital signatures?

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

16.What is a VPN and how does it enhance security?

Answer: A VPN (Virtual Private Network) creates a secure, encrypted connection over a less secure network, such as the internet. It enhances security by protecting data in transit from eavesdropping, tampering, and other attacks.

17.What is the difference between SSL/TLS VPNs and IPsec VPNs?

Answer: SSL/TLS VPNs use the SSL/TLS protocol to secure the VPN connection, typically through a web browser. IPsec VPNs use the IPsec protocol suite to provide secure communication at the IP layer, often requiring specialized client software.

18.How does the OpenVPN protocol work?

Answer: OpenVPN is an open-source VPN protocol that uses SSL/TLS for key exchange and encryption. It can use either TCP or UDP for data transfer and is highly configurable for different network environments.

19.What is the purpose of a VPN kill switch?

Answer: A VPN kill switch is a security feature that automatically disconnects the user's internet access if the VPN connection drops, preventing data from being transmitted over an unsecured connection.

20.Explain the concept of split tunneling in VPNs.

Answer: Split tunneling allows a VPN user to route some of their traffic through the encrypted VPN tunnel while sending other traffic directly to the internet without encryption. This can optimize network performance and reduce load on the VPN server.