Interview Questions

Network Security

Q1. What is a symmetric key? **(Hicube Infosec Pvt. Ltd)**
Answer: Symmetric encryption is a type of encryption that uses only one key (a secret key) to encrypt and decrypt electronic information. Entities that communicate using symmetric encryption must exchange the key before it can be used in the decryption process. This encryption method differs from asymmetric encryption, in which a key pair, one public and one private, is used to encrypt and decrypt messages.

Q2. How is Asymmetric encryption different? **(K7 Computing Pvt. Ltd)**
Answer: Symmetric encryption consists of one key for encryption and decryption, while asymmetric encryption consists of two cryptographic keys known as a public key and a private key. Asymmetric cryptography is a technique that uses a related key pair, a public key and a personal key, to encrypt and decrypt a message and reserve it to guard against unauthorized access or unauthorized use. A public key's a cryptographic key that anyone can use to encrypt a message so that only the intended recipient can decrypt using their private key.

Q3. How does the Diffie Hellman exchange works? **(Wi-Jungle)**
Answer: DH is usually explained by two sample groups, Alice and Bob, who start a dialogue. Everyone has information they want to share while keeping it a secret. To do this, they agree to some benign public information that is mistaken for their privileged information by being transmitted through an insecure channel. Their secrets are mixed with the public information or public key, and while the secrets are being exchanged, the information they want to share is mixed with the shared secret. When they decipher the other's message, they can extract the public information and, knowing their own secret, infer the new information that they took with them. While this method may seem straightforward to describe, decryption by an outside party trying to spy using

long strings of numbers for public and private keys is mathematically impractical, even with significant resources.

Q4. What are RSA algorithms? **(eSec Forte Technologies)**

Answer: The RSA is a series of cryptographic algorithms used for specific security purposes or services that enable public-key encryption and universally defend sensitive data, especially when dispatched to through an insecure network cognate as the Internet. Public critical cryptography, also known as asymmetric cryptography, uses two different but mathematically related keys, one public and one private.

Q5. What are digital certificates? **(Quick Heal Technologies Ltd.)**

Answer: A digital certificate, also known as a public key certificate, is used to cryptographically link the ownership of a public key to the entity that owns it. Digital certificates are used to share public keys for encryption and authentication. Digital certificates include the public key to be certified, identifying information about the entity that owns the public key, metadata related to the digital certificate, and a digital signature of the public key created by the certifier.