18. What is the difference between a digital signature and a message authentication code (MAC)?

19. How can a digital signature be verified?

20. What is the difference between a one-time pad and a stream cipher?

Answer:

1. The main difference between symmetric and asymmetric encryption is using a single secret key versus a pair of public and private keys in asymmetric encryption. In symmetric encryption, the same key is used for encryption and decryption. In contrast, in asymmetric encryption, a public key is used for encryption, and a private key is used for decryption.

Symmetric encryption and asymmetric encryption are two different methods of encrypting data. The main difference between the two is using a single secret key in symmetric encryption versus a pair of public and private keys in asymmetric encryption.

In symmetric encryption, the same key is used for encryption and decryption. This means that the message's sender and receiver must share the same secret key to encrypt and decrypt the message. This can be a problem if the key is intercepted or lost, as anyone who has the key will be able to read the news. Additionally, if the key is compromised, it must be changed for all users, making it a hassle.

On the other hand, asymmetric encryption uses a pair of keys, a public key, and a private key. The public key encrypts the message, while the private key decrypts it. The public key can be freely distributed to anyone, while the private key is kept secret. This means that a message can be encrypted by anyone with the public key but can only be decrypted by the person with the corresponding private key. This makes it much more secure than symmetric encryption, as the private key does not need to be shared and can be kept safe.

In summary, symmetric encryption uses a single key for encryption and decryption. In contrast, asymmetric encryption uses a pair of keys, a public key for encryption, and a private key for

encrypting it with the sender's private key. Once the signature is generated, the recipient can use the sender's public key to decrypt it and compare it to a hash of the received data. If the two hashes match, the signature is valid, meaning that the data has not been modified and is from the claimed sender.

Digital signatures are used in secure communication, such as in electronic commerce, email, and software distribution. It provides a way to authenticate the sender's identity and ensure that the information received has not been tampered with. It also ensures non-repudiation, meaning the sender can not deny sending the message later.

In summary, A digital signature verifies the authenticity and integrity of digital information, such as electronic documents. It is created by applying a mathematical algorithm to the data to be signed, along with a private key. The resulting digital signature can then be verified using the corresponding public key. Digital signatures are used in secure communication to ensure that the information received has not been tampered with and that it is from the claimed sender, providing a way to authenticate the sender's identity and ensure that the information received has not been tampered with.

7. A digital certificate contains information about an entity, such as an individual or organization, and its public key. A trusted third party issues it a certificate authority (CA) to verify the entity's identity. On the other hand, a digital signature verifies the authenticity and integrity of digital information, such as an electronic document. It is created by applying a mathematical algorithm to the data to be signed, along with a private key.

A digital certificate, also known as a public key certificate, is a digital document that contains information about an entity, such as an individual or organization, and its public key. A trusted third party issues it, called a certificate authority (CA), and is used to verify the entity's identity. The information in the certificate includes the entity's name, the public key, and other identifying information, which the CA digitally signs.

A digital certificate is an electronic form of identification, similar to a passport or driver's license. It establishes trust and ensures secure communication in e-commerce and online banking transactions. When a user connects to a website, for example, their browser will check the website's digital certificate to ensure that it is valid and issued by a trusted CA.

The resulting ciphertext and the symmetric key are combined and encrypted using an asymmetric encryption algorithm, such as RSA. This ensures that only the intended recipient, who holds the corresponding private key, can decrypt the data and read the message.

The digital envelope method provides an additional layer of security compared to symmetric encryption. It ensures that only the intended recipient can read the message. Because the symmetric key is encrypted using the recipient's public key, it eliminates the need for a secure key distribution mechanism. Additionally, it provides integrity as the digital signature can be used to verify that the data has not been tampered with while in transit.

In summary, A digital envelope is a method of encrypting data, such as a message, using a combination of symmetric and asymmetric encryption algorithms. It ensures both confidentiality and integrity of the data; the symmetric encryption algorithm is used to encrypt the data, and the symmetric key used to encrypt the data is typically encrypted using the recipient's public key; this process is called vital wrapping; the resulting ciphertext and the symmetric key are then combined and encrypted using an asymmetric encryption algorithm. This ensures that only the intended recipient, who holds the corresponding private key, can decrypt the data and read the message.

17. The Elliptic Curve Digital Signature Algorithm (ECDSA) is a widely used digital signature algorithm based on elliptic curves' mathematical properties. It uses a pair of public and private keys, similar to RSA, to create a digital signature. The private key is used to create the digital signature, which can then be verified using the corresponding public key. The security of the ECDSA algorithm is based on the difficulty of solving the discrete logarithm problem in the group of points on an elliptic curve.

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a widely used digital signature algorithm based on elliptic curves' mathematical properties. It is used to provide authentication and integrity for electronic communications and transactions.

Like RSA, ECDSA uses public and private keys to create a digital signature. The private key is used to create the digital signature, and the corresponding public key is used to verify the