1)What is encryption? Why do we need it?

Cryptography is the practice and study of techniques for securing communication and data in the presence of adversaries.

It take a plaintext message and converts it to a sequence of random characters and numbers illegible to humans.

Encryption is essential for communicating or sharing information over the network because it allows you to detect and flag tampering.

2)Name three features of encryption and why encryption is beneficial to us.

It may secure data security, protect data from unwanted modification, and authenticate data sources.

Confidentiality: It means ensuring that no one can read a message except the intended receiver.

It also means keeping data secret from those without the proper credentials, even if this data passes through an insecure network.

Integrity (Anti-Tampering): It means ensuring the receiver that the received message has not been altered in any way from the original.

Authentication: It is the process of proving one’s identity.

Non-Repudiation: A repudiation is a rejection or denial of something's validity, such as refusing to fulfill a legal contract. Non-repudiation refers to mechanisms that prove that the sender sent the message.

3) Name at least five major applications for cryptography.

Authentication/Digital Signatures

Time Stamping

Electronic Money

Secure Network Communications(SSL,Kerberos)

Anonymous Remailers

Disk Encryption

4) A cypher works in conjunction with a key to encrypt plaintext. Different keys will generate different cyphers for the same plaintext.

There are two types of key cryptography: symmetric and asymmetric. Explain each type of cryptography and the techniques behind it.

* Symmetric
* Asymmetric

Symmetric: The sender and receiver of a message share a single key for encrypting and decrypting the message.

Asymmetric: Asymmetric cryptography, also known as public-key cryptography, is a cryptographic algorithm that requires two separate keys, one private and the other public. The message is encrypted with the public key and decrypted with the private key. As a result, anyone with the public key can encrypt but not decrypt information. The information can only be decrypted by someone who has the corresponding private key.

5) Explain what RSA is and its main uses.

RSA, which stands for Rivest-Shamir-Adleman, is a widely used cryptographic algorithm for public-key encryption and digital signatures.

-Public-Key Encryption: RSA is primarily used for secure communication and data transmission over insecure networks, such as the internet.

-Digital Signatures: RSA is used for creating digital signatures, which provide integrity, authenticity, and non-repudiation of digital documents or messages.

-Key Exchange: RSA can also be used for secure key exchange between two parties. By encrypting a shared symmetric key with the recipient's public key, the sender can securely transmit the key to the recipient, who can then decrypt it using their private key. This allows them to establish a shared secret key for further secure communication using symmetric encryption algorithms.

-SSL/TLS Encryption: RSA is an integral part of the SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocols, which provide secure communication between clients and servers over the internet. RSA is used during the initial handshake process to establish a secure connection and exchange session keys.

6)

11)

There are several threats for a cryptographic system. Explain at least 3 of these threats. You may use the following article: http://www.crypto-it.net/eng/attacks/index.htmlCiphertext-only attack – only the ciphertext is known to the attacker. If the hacker is in statistics, then they can use various statistical techniques to break the ciphertext back into the plaintext. Known-plaintext attack – this occurs when the hacker knows some aspect of either the letter pairings, and then can consequently break the ciphertext back into the plaintext.

Chosen-plaintext attack – the hacker can choose the plaintext and view the encrypted output which is transmitted across the network. Then they can reverse-engineer it back into ciphertext to figure out the encryption.Adaptive chosen-plaintext attack – like a chosen-plaintext attack, except the attacker can choose subsequent plaintexts based on information learned from previous encryptions.Related-key attack – like a chosen-plaintext attack, except the attacker can obtain ciphertexts encrypted under two different keys. The keys are unknown, but the relationship between them is known.

**Choose one of the threats you explained in the previous question and explain how you, as a future cybersecurity expert, can protect your network from it.**