1. **What is cryptography and cryptanalysis?**

Encryption, decryption without knowing the keys

1. What was the earliest reason for the use of cryptography?

Concealing military and political secrets while they were transported from place to place.

1. **What is a cryptographic key, and what is it used for? What is a more formal name for a cryptographic key?**

Also known as a crypto variable, is the information used in conjunction with an algorithm to create the ciphertext from the plaintext or derive the plaintext from the ciphertext. The key can be a series of bits used by a computer program, or it can be a passphrase used by people that is then converted into a series of bits for use in the computer program.

1. What are the three basic operations in cryptography?

Encrypting, decrypting, and hashing

1. **What is a hash function, and what can it be used for?**

Mathematical algorithms that generate a message summary or digest to confirm the identity and integrity.

Convert variable-length messages into a single fixed-length value, and different messages have different digests.

1. **What does it mean to be “out of band”? Why is it important to exchange keys out of band in symmetric encryption?**

avoid interception, use a band other than the one carrying the ciphertext.

1. **What is the fundamental difference between symmetric and asymmetric encryption?**

|  |  |  |
| --- | --- | --- |
|  | Symmetric | Asymmetric |
| Also known as | Public key encryption | Private key encryption |
| Types of keys | 1, private | 2, public and private |
| Encryption and decryption | Same key | Different key |
| Problem | Send the key to the receiver | Slower |

1. How does public key infrastructure add value to an organization seeking to use cryptography to protect information assets?

PKI makes the use of cryptographic systems more convenient and cost-effective.

1. **What are the components of PKI?**

RA (Regulation Authority), CA (Certificate Authority), CA (Certificate directories), Protocols, Policies and Procedures.

1. What is the difference between a digital signature and a digital certificate?

Digital signatures are encrypted messages that can be verified with the help of hashing while digital certificates are files that contain public key that are used to identify the ownership of computer applications.

1. What critical issue in symmetric and asymmetric encryption is resolved by using a hybrid method like Diffie-Hellman?

3rd party transfer compromising.

1. **What is steganography, and what can it be used for?**

Hiding messages by secret writing.

Protect confidential info.

1. **Which security protocols are predominantly used in Web-based e-commerce?**

SSL (secure sockets layer), S-HTTP (secure hypertext transfer protocol), SET (secure electronic transactions)

1. **Which security protocols are used to protect e-mail?**

S/MIME (secure multipurpose internet mail extensions), PEM (privacy enhanced mail), PGP (pretty good privacy)

1. IPSec can be implemented using two modes of operation. What are they?

Transport and tunnel

1. Which kind of attack on cryptosystems involves using a collection of pre-identified terms? Which kind of attack involves sequential guessing of all possible key combinations?

Dictionary attack, rainbow cracking

Brute force attack

1. If you were setting up an encryption-based network, what key size would you choose and why?

Choose the largest key size consistent with the tools being used and the overhead performance burden it would impose on the environment. The current "gold standard" is to ensure that all computing devices are capable of AES 256-bit encryption.

1. What is the typical key size of a strong encryption system used on the Web today?

At least 256 bits

1. **What encryption standard is currently recommended by NIST?**

AES (advanced encryption standard)

1. **What are the most popular encryption systems used over the Web?**

Symmetric: AES, asymmetric: RSA, hybrid: PGP