Question Bank

Two-Mark Questions

1. **What is the Caesar Cipher?**
   - **Answer:** The Caesar Cipher is a substitution cipher where each letter in the plaintext is shifted a certain number of places down or up the alphabet. For example, with a shift of 3, 'A' becomes 'D', 'B' becomes 'E', and so on.
2. **Describe the Playfair Cipher briefly.**
   - **Answer:** The Playfair Cipher is a digraph substitution cipher where pairs of letters are encrypted together. It uses a 5x5 matrix of letters as the key to encrypt and decrypt pairs of letters in the plaintext.
3. **Explain the Hill Cipher.**
   - **Answer:** The Hill Cipher is a polygraphic substitution cipher that uses linear algebra. It encrypts blocks of text by multiplying vectors representing the plaintext by an invertible matrix (the key matrix) modulo 26.
4. **What is modulo arithmetic in cryptography?**
   - **Answer:** Modulo arithmetic involves division of integers and taking the remainder. It is often used in cryptography for operations like modular exponentiation and hashing, ensuring results stay within a fixed range.
5. **Define the Greatest Common Divisor (GCD).**
   - **Answer:** The Greatest Common Divisor of two integers is the largest positive integer that divides both numbers without leaving a remainder.
6. **What is the Chinese Remainder Theorem?**

- **Answer:** The Chinese Remainder Theorem states that if one knows the remainders of the division of an integer by several pairwise coprime integers, one can determine the unique integer modulo the product of these integers.

7. **What is a digital certificate?**
    - **Answer:** A digital certificate is an electronic document used to prove the ownership of a public key. It includes information about the key, identity of its owner, and the digital signature of an entity that has verified the certificate's contents.
8. **What is the Diffie-Hellman Key Exchange?**
    - **Answer:** The Diffie-Hellman Key Exchange is a method allowing two parties to securely share a secret key over a public channel by using mathematical operations involving modular arithmetic and prime numbers.
9. **What is a public key infrastructure (PKI)?**
    - **Answer:** A Public Key Infrastructure is a framework for managing digital certificates and public-key encryption. It includes hardware, software, policies, and procedures to ensure secure communication and identity verification.
10. **What is a cryptographic hash function?**
    - **Answer:** A cryptographic hash function takes an input and produces a fixed-size string of bytes that appears random. It is designed to be a one-way function that is infeasible to invert.
11. **What does HMAC stand for, and what is its purpose?**
    - **Answer:** HMAC stands for Hash-based Message Authentication Code. It uses a cryptographic hash function combined with a secret key to ensure both data integrity and authenticity.

12. **What is the main advantage of asymmetric encryption?**

    - **Answer:** The main advantage of asymmetric encryption is that it uses a pair of keys (public and private), enabling secure data exchange without sharing the secret key. It also facilitates digital signatures.

13. **What is DES and why is it considered weak?**

    - **Answer:** DES (Data Encryption Standard) is a symmetric-key block cipher that encrypts data in 64-bit blocks using a 56-bit key. It is considered weak due to its short key length, making it vulnerable to brute-force attacks.

14. **What is AES?**

    - **Answer:** AES (Advanced Encryption Standard) is a symmetric-key block cipher that encrypts data in blocks of 128 bits using key sizes of 128, 192, or 256 bits. It is widely used due to its security and efficiency.

15. **What is a digital signature?**

    - **Answer:** A digital signature is a mathematical scheme for verifying the authenticity and integrity of digital messages or documents. It provides non-repudiation, ensuring that the message was created by a known sender.

16. **What is the purpose of the Needham-Schroeder Protocol?**

    - **Answer:** The Needham-Schroeder Protocol is used for mutual authentication and key exchange between two parties to ensure that both are legitimate and establish a secure session key.

17. **What is Kerberos?**

- **Answer:** Kerberos is a network authentication protocol designed to provide strong authentication for client-server applications by using secret-key cryptography and a trusted third party (the Key Distribution Center).

18. **What does SSL stand for, and what is its purpose?**
    - **Answer:** SSL stands for Secure Sockets Layer. It is a protocol for securing communications over a computer network by encrypting data transmitted between clients and servers.
19. **What is the main difference between symmetric and asymmetric encryption?**
    - **Answer:** Symmetric encryption uses the same key for both encryption and decryption, while asymmetric encryption uses a pair of keys: a public key for encryption and a private key for decryption.
20. **What is the Birthday Attack in cryptography?**
    - **Answer:** The Birthday Attack is a type of cryptographic attack that exploits the mathematics of the birthday problem to find collisions in hash functions, making it easier to break them.
21. **What does PKCS stand for in public key cryptography?**
    - **Answer:** PKCS stands for Public Key Cryptography Standards. It is a set of standards for public-key cryptography developed by RSA Laboratories.
22. **What is the purpose of the SHA family of hash functions?**
    - **Answer:** The SHA (Secure Hash Algorithm) family provides cryptographic hash functions designed to produce fixed-size hash values that are unique to the input data, ensuring data integrity and security.
23. **What is the main feature of the ElGamal cryptosystem?**

- **Answer:** The ElGamal cryptosystem provides asymmetric encryption based on the Diffie-Hellman key exchange. It relies on the difficulty of solving the discrete logarithm problem.

24. **What is the role of a challenge-response protocol in authentication?**
    - **Answer:** A challenge-response protocol involves the server sending a challenge to the client, which then generates a response using a secret key. This helps verify the client’s identity securely.
25. **What are the common tools and methods used in cybercrime?**
    - **Answer:** Common tools and methods in cybercrime include password cracking tools, keyloggers, spyware, and SQL injection techniques. These tools are used to gain unauthorized access, steal data, or compromise systems.

Long Answer Questions

1. **Explain the working of the Caesar Cipher with an example.**
    - **Answer:** The Caesar Cipher shifts each letter in the plaintext by a fixed number of places. For instance, with a shift of 3, the letter 'A' becomes 'D', 'B' becomes 'E', and so forth. To encrypt the plaintext "HELLO" with a shift of 3, you replace each letter: H → K, E → H, L → O, L → O, O → R, resulting in "KHOOR". Decryption involves shifting in the opposite direction.
2. **Describe the Playfair Cipher in detail and provide an example encryption.**
    - **Answer:** The Playfair Cipher uses a 5x5 matrix constructed from a keyword. To encrypt, plaintext is split into digraphs (pairs of letters). Each pair is then substituted

based on their positions in the matrix. For example, with the keyword "KEYWORD" and plaintext "HELLO WORLD", the matrix might look like this:

K E Y W O

R D A B C

F G H I J

L M N P Q

S T U V X

Encrypting "HE" involves locating 'H' and 'E' in the matrix, which are in different rows and columns. Substitute 'H' with the letter in the same row but the column of 'E' (i.e., 'I'), and 'E' with the letter in the same column but the row of 'H' (i.e., 'G'), resulting in "IG".

3. **Discuss the Hill Cipher and provide a sample encryption.**

- **Answer:** The Hill Cipher encrypts blocks of text using linear algebra. A key matrix is used to transform plaintext vectors. For instance, with a 2x2 key matrix:

  [2 3]

  [1 4]

  and plaintext "HI", convert to numerical vectors (H=7, I=8). Multiply the key matrix by the plaintext vector:

  [2 3]   [7]

  [1 4] * [8]

[2 3]   [7]

[1 4] * [8]

The resulting vector is (2*7 + 3*8, 1*7 + 4*8) = (34, 39). Convert back to letters for ciphertext.

4) Implement a program for Caesar Cipher encryption and decryption.

- **Answer:** Here’s a sample Python code for Caesar Cipher:

```
def caesar_encrypt(plaintext, shift):

  encrypted = ""

  for char in plaintext:

    if char.isalpha():

      shift_amount = shift % 26

      start = ord('A') if char.isupper() else ord('a')

      encrypted += chr(start + (ord(char) - start + shift_amount) % 26)

    else:

      encrypted += char

  return encrypted

def caesar_decrypt(ciphertext, shift):

  return caesar_encrypt(ciphertext, -shift
```