Sample Paper

Question 1: Explain the categories of passive and active security attacks. Provide examples for each.

Answer:  
Passive attacks involve monitoring or eavesdropping on communication channels to gather information without altering the data. Common examples include traffic analysis and signal interception. In contrast, active attacks disrupt or manipulate the data or system. Examples include denial-of-service attacks and data modification during transmission.

Score: 2, 3, 3, 2

Question 2: Encrypt the plaintext 'hello world' using the Vigenère Cipher with the key 'SECURITY'. Provide a step-by-step explanation of the process.

Answer:  
The Vigenère Cipher works by aligning the key with the plaintext and performing character shifts based on the key letters. Aligning 'SECURITY' cyclically with 'HELLO WORLD,' we calculate the ciphertext as follows: 'ZINFFEHPPD'.

Score: 3, 2, 3, 2

Question 3: Explain the encryption and decryption process of the Feistel Cipher. Include a diagram to support your explanation.

Answer:  
The Feistel Cipher divides plaintext into two halves and processes them through multiple rounds of substitution and permutation using keys. Encryption involves transforming the right half based on a function of the key, then swapping. Decryption reverses the process by using the keys in reverse order.

Score: 4, 2, 3, 1

Question 4: Compare and contrast the True Random Number Generator (TRNG) and Pseudorandom Number Generator (PRNG). Include examples of their applications.

Answer:  
TRNG relies on physical phenomena like thermal noise, producing completely random values, ideal for secure key generation. PRNG uses algorithms for reproducible sequences, often used in simulations or gaming. TRNG is slower but more secure; PRNG is faster but less random.

Score: 3, 3, 3, 1

Question 5: Discuss the security requirements for a public-key cryptosystem. Why is RSA considered a secure algorithm, and what potential attacks could compromise it?

Answer:  
Public-key cryptosystems require confidentiality, integrity, and authentication. RSA achieves security using large prime numbers and modular arithmetic. However, side-channel attacks and improper key management can compromise its security.

Score: 4, 3, 2, 1

Question 6: Explain the differences between block ciphers and stream ciphers. Provide examples of each and discuss their appropriate use cases.

Answer:  
Block ciphers encrypt data in fixed-size blocks using padding for smaller data (e.g., AES, DES). Stream ciphers encrypt continuous streams of data (e.g., RC4). Block ciphers are better for file encryption, while stream ciphers suit real-time communication.

Score: 3, 3, 3, 1

Question 7: Describe the purpose and process of the AES SubBytes transformation. Perform the SubBytes transformation on the matrix using the AES S-box.

Answer:  
The AES SubBytes transformation substitutes each byte in the state matrix with a corresponding byte from the AES S-box. For example, applying the S-box transformation to [DB A1 F8 77], we get [8E 1B 3C 4D]. This process improves non-linearity and security.

Score: 4, 4, 2

Question 8: Explain the Hill Cipher encryption technique. Encrypt the plaintext 'ACT' using the given key matrix and show all steps in your calculation.

Answer:  
The Hill Cipher uses a key matrix to encrypt plaintext by matrix multiplication mod 26. For 'ACT', using the given matrix, we compute the ciphertext as 'POH' after performing matrix operations and modulo arithmetic.

Score: 3, 5, 2

Question 9: In the context of public-key cryptography, describe the requirements of a secure algorithm. Explain why modular arithmetic is critical to RSA and provide an example calculation.

Answer:  
Secure algorithms ensure confidentiality, integrity, and non-repudiation. Modular arithmetic underpins RSA, enabling efficient encryption and decryption. For example, modular exponentiation allows operations like (5^3 mod 13) = 8.

Score: 3, 4, 3

Question 10: Discuss the differences between the One-Time Pad and other classical encryption techniques like Caesar Cipher or Vigenère Cipher. Why is the One-Time Pad considered unbreakable under certain conditions?

Answer:  
The One-Time Pad uses a random key of the same length as the plaintext for encryption. Unlike Caesar or Vigenère Ciphers, which rely on repeating keys, the One-Time Pad is unbreakable if keys are random and used only once.

Score: 3, 4, 3

Question 11: Explain the categories of security services. How do they contribute to maintaining a secure system?

Answer:  
Security services like confidentiality, integrity, and authentication protect data and systems. For example, confidentiality uses encryption, integrity employs hash functions, and authentication uses digital signatures.

Score: 2, 5, 3

Question 12: What is the difference between symmetric and asymmetric encryption? Provide examples and explain when each is used.

Answer:  
Symmetric encryption (e.g., AES) uses the same key for encryption and decryption, while asymmetric encryption (e.g., RSA) uses public-private key pairs. Symmetric methods are faster; asymmetric ones suit secure key exchange.

Score: 3, 3, 3, 1

Question 13: Perform encryption and decryption using the Rail Fence Cipher with a depth of 3 on the plaintext: 'HELLOCRYPTO'. Show all steps.

Answer:  
The Rail Fence Cipher encrypts 'HELLOCRYPTO' by writing letters diagonally in three rows, then reading rows sequentially. Encrypted: 'HORELCTLOY'.

Score: 3, 4, 3

Question 14: Discuss the significance of Fermat’s Little Theorem in cryptography. Provide an example calculation to illustrate its application.

Answer:  
Fermat's Little Theorem states that if p is a prime number and a is an integer not divisible by p, then a^(p-1) ≡ 1 (mod p). In RSA, it helps in modular arithmetic operations. For example, 2^6 mod 7 = 1.

Score: 4, 3, 3

Question 15: What are the advantages and challenges of the Double DES encryption method? Explain the 'meet-in-the-middle' attack and its impact on Double DES.

Answer:  
Double DES increases security but is vulnerable to the 'meet-in-the-middle' attack, where an attacker uses intermediate ciphertexts to break the system. This makes it less secure than triple DES or AES.

Score: 3, 3, 4

Question 16: Explain the difference between the output feedback (OFB) mode and cipher block chaining (CBC) mode in block ciphers. Include diagrams for both.

Answer:  
OFB mode turns block ciphers into stream ciphers by applying a key to an initialization vector (IV), while CBC encrypts each block using the previous ciphertext block. OFB suits error-prone channels; CBC works for file encryption.

Score: 4, 4, 2

Question 17: Describe the concept of modular arithmetic and explain its importance in cryptography. Provide an example demonstrating modular exponentiation.

Answer:  
Modular arithmetic involves operations constrained by a modulus. In cryptography, it's critical for algorithms like RSA. Example: Calculating (3^4 mod 5), we get 1.

Score: 3, 3, 4

Question 18: What is the Euclidean algorithm, and how is it used to find the greatest common divisor (GCD)? Use an example to demonstrate the process.

Answer:  
The Euclidean algorithm computes the greatest common divisor (GCD) of two numbers via iterative subtraction or division. For example, GCD(48, 18) is computed as 6.

Score: 3, 5, 2

Question 19: Explain the purpose and process of the AES ShiftRows transformation. Provide an example to illustrate how it works.

Answer:  
The AES ShiftRows transformation cyclically shifts rows in the state matrix left. For example, the second row shifts by one byte, third by two, and fourth by three.

Score: 4, 4, 2

Question 20: Discuss the requirements for a secure public-key cryptosystem. How do these requirements ensure system security?

Answer:  
Secure public-key cryptosystems require robust algorithms, large key sizes, and strong randomness. These prevent brute force and ensure integrity.

Score: 4, 4, 2