# Sample Paper

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

Answer:  
Explain the categories of passive and active security attacks. Provide examples for each. This response provides a moderate explanation with examples, addressing most of the rubric components.

Score: 1, 2, 3, 4

## 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:  
Encrypt the plaintext 'hello world' using the Vigenère Cipher with the key 'SECURITY'. Provide a step-by-step explanation of the process. This response provides a moderate explanation with examples, addressing most of the rubric components.

Score: 1, 2, 3, 4

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

Answer:  
Explain the encryption and decryption process of the Feistel Cipher. Include a diagram to support your explanation. This response provides a moderate explanation with examples, addressing most of the rubric components.

Score: 1, 2, 3, 4

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

Answer:  
Compare and contrast the True Random Number Generator (TRNG) and Pseudorandom Number Generator (PRNG). Include examples of their applications. This response provides a moderate explanation with examples, addressing most of the rubric components.

Score: 1, 2, 3, 4

## 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:  
Discuss the security requirements for a public-key cryptosystem. Why is RSA considered a secure algorithm, and what potential attacks could compromise it? This response provides a moderate explanation with examples, addressing most of the rubric components.

Score: 1, 2, 3, 4

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

Answer:  
Explain the differences between block ciphers and stream ciphers. Provide examples of each and discuss their appropriate use cases. This response provides a moderate explanation with examples, addressing most of the rubric components.

Score: 1, 2, 3, 4

## 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:  
Describe the purpose and process of the AES SubBytes transformation. Perform the SubBytes transformation on the matrix using the AES S-box. This response provides a moderate explanation with examples, addressing most of the rubric components.

Score: 1, 2, 3, 4

## 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:  
Explain the Hill Cipher encryption technique. Encrypt the plaintext 'ACT' using the given key matrix and show all steps in your calculation. This response provides a moderate explanation with examples, addressing most of the rubric components.

Score: 1, 2, 3, 4

## 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:  
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. This response provides a moderate explanation with examples, addressing most of the rubric components.

Score: 1, 2, 3, 4

## 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:  
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? This response provides a moderate explanation with examples, addressing most of the rubric components.

Score: 1, 2, 3, 4

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

Answer:  
Explain the categories of security services. How do they contribute to maintaining a secure system? This response provides a moderate explanation with examples, addressing most of the rubric components.

Score: 1, 2, 3, 4

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

Answer:  
What is the difference between symmetric and asymmetric encryption? Provide examples and explain when each is used. This response provides a moderate explanation with examples, addressing most of the rubric components.

Score: 1, 2, 3, 4

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

Answer:  
Perform encryption and decryption using the Rail Fence Cipher with a depth of 3 on the plaintext: 'HELLOCRYPTO'. Show all steps. This response provides a moderate explanation with examples, addressing most of the rubric components.

Score: 1, 2, 3, 4

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

Answer:  
Discuss the significance of Fermat’s Little Theorem in cryptography. Provide an example calculation to illustrate its application. This response provides a moderate explanation with examples, addressing most of the rubric components.

Score: 1, 2, 3, 4

## 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:  
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. This response provides a moderate explanation with examples, addressing most of the rubric components.

Score: 1, 2, 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:  
Explain the difference between the output feedback (OFB) mode and cipher block chaining (CBC) mode in block ciphers. Include diagrams for both. This response provides a moderate explanation with examples, addressing most of the rubric components.

Score: 1, 2, 3, 4

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

Answer:  
Describe the concept of modular arithmetic and explain its importance in cryptography. Provide an example demonstrating modular exponentiation. This response provides a moderate explanation with examples, addressing most of the rubric components.

Score: 1, 2, 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:  
What is the Euclidean algorithm, and how is it used to find the greatest common divisor (GCD)? Use an example to demonstrate the process. This response provides a moderate explanation with examples, addressing most of the rubric components.

Score: 1, 2, 3, 4

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

Answer:  
Explain the purpose and process of the AES ShiftRows transformation. Provide an example to illustrate how it works. This response provides a moderate explanation with examples, addressing most of the rubric components.

Score: 1, 2, 3, 4

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

Answer:  
Discuss the requirements for a secure public-key cryptosystem. How do these requirements ensure system security? This response provides a moderate explanation with examples, addressing most of the rubric components.

Score: 1, 2, 3, 4