**Question 1:**

**Explain the categories of passive and active security attacks. Provide examples for each.**

**Grading Rubric**:

* Clear distinction between passive and active attacks: **2 marks**
* Explanation of passive attacks with examples (e.g., eavesdropping, traffic analysis): **3 marks**
* Explanation of active attacks with examples (e.g., spoofing, denial of service): **3 marks**
* Language clarity and coherence: **2 marks**

**Question 2:**

**Encrypt the plaintext “hello world” using the Vigenère Cipher with the key "SECURITY". Provide a step-by-step explanation of the process.**

**Grading Rubric**:

* Correct description of the Vigenère Cipher process: **3 marks**
* Accurate alignment of the plaintext with the key: **2 marks**
* Correct encryption with explanation of each step: **3 marks**
* Neat presentation and clarity of the solution: **2 marks**

**Question 3:**

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

**Grading Rubric**:

* Clear explanation of the Feistel Cipher's structure (e.g., rounds, key schedule): **4 marks**
* Inclusion of a well-labelled diagram: **2 marks**
* Description of the encryption and decryption process: **3 marks**
* Conciseness and readability: **1 mark**

**Question 4:**

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

**Grading Rubric**:

* Explanation of TRNG with examples (e.g., hardware-based randomness): **3 marks**
* Explanation of PRNG with examples (e.g., algorithm-based randomness): **3 marks**
* Key differences outlined clearly: **3 marks**
* Language quality and coherence: **1 mark**

**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?**

**Grading Rubric**:

* Identification and explanation of public-key cryptosystem requirements: **4 marks**
* Discussion of RSA’s security features (e.g., large prime numbers, key size): **3 marks**
* Explanation of potential attacks (e.g., brute force, side-channel attacks): **2 marks**
* Clarity and logical structure of the response: **1 mark**

**Question 6:**

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

**Grading Rubric**:

* Definition of block ciphers with an example (e.g., AES, DES): **3 marks**
* Definition of stream ciphers with an example (e.g., RC4): **3 marks**
* Comparison of their strengths and weaknesses: **3 marks**
* Clarity of the response: **1 mark**

**Question 7:**

**Describe the purpose and process of the AES SubBytes transformation. Perform the SubBytes transformation on the matrix below using the AES S-box.**

**Matrix**:

[DBA1F877186D8BBAA830084EFFD5D7AA]\begin{bmatrix} DB & A1 & F8 & 77 \\ 18 & 6D & 8B & BA \\ A8 & 30 & 08 & 4E \\ FF & D5 & D7 & AA \end{bmatrix}​DB18A8FF​A16D30D5​F88B08D7​77BA4EAA​​

**Grading Rubric**:

* Explanation of the AES SubBytes process: **4 marks**
* Correct use of the AES S-box for transformation: **4 marks**
* Clear presentation of results: **2 marks**

**Question 8:**

**Explain the Hill Cipher encryption technique. Encrypt the plaintext "ACT" using the key matrix below and show all steps in your calculation.**

**Key Matrix**:

[6241131610201715]\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}​61320​241617​11015​​

**Grading Rubric**:

* Explanation of the Hill Cipher and how the key matrix is used: **3 marks**
* Step-by-step calculation of ciphertext: **5 marks**
* Correct final ciphertext: **2 marks**

**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.**

**Grading Rubric**:

* Explanation of secure algorithm requirements (e.g., confidentiality, non-repudiation): **3 marks**
* Discussion of modular arithmetic’s role in RSA: **4 marks**
* Example calculation demonstrating modular arithmetic (e.g., modular exponentiation): **3 marks**

**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?**

**Grading Rubric**:

* Explanation of the One-Time Pad and its key properties: **3 marks**
* Comparison with classical techniques like Caesar Cipher or Vigenère Cipher: **4 marks**
* Explanation of the conditions under which the One-Time Pad is unbreakable (e.g., truly random key, single use): **3 marks**

**Question 11:**

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

**Grading Rubric**:

* Definition of security services: **2 marks**
* Explanation of key categories (e.g., confidentiality, integrity, authentication): **5 marks**
* Examples of how each service is implemented: **3 marks**

**Question 12:**

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

**Grading Rubric**:

* Definition of symmetric encryption with example (e.g., AES, DES): **3 marks**
* Definition of asymmetric encryption with example (e.g., RSA, ECC): **3 marks**
* Explanation of use cases for each: **3 marks**
* Clarity and correctness: **1 mark**

**Question 13:**

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

**Grading Rubric**:

* Correct explanation of the Rail Fence Cipher process: **3 marks**
* Accurate encryption: **4 marks**
* Accurate decryption: **3 marks**

**Question 14:**

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

**Grading Rubric**:

* Explanation of Fermat’s Little Theorem: **4 marks**
* Discussion of its significance in cryptography (e.g., RSA key generation): **3 marks**
* Example calculation with explanation: **3 marks**

**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.**

**Grading Rubric**:

* Advantages of Double DES: **3 marks**
* Challenges and weaknesses: **3 marks**
* Explanation of the "meet-in-the-middle" attack: **4 marks**

**Question 16:**

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

**Grading Rubric**:

* Description of OFB mode with diagram: **4 marks**
* Description of CBC mode with diagram: **4 marks**
* Comparison of the two modes: **2 marks**

**Question 17:**

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

**Grading Rubric**:

* Definition and explanation of modular arithmetic: **3 marks**
* Discussion of its importance in cryptography: **3 marks**
* Example with correct calculations: **4 marks**

**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.**

**Grading Rubric**:

* Explanation of the Euclidean algorithm: **3 marks**
* Step-by-step example of finding the GCD: **5 marks**
* Clarity and correctness of steps: **2 marks**

**Question 19:**

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

**Grading Rubric**:

* Explanation of the ShiftRows transformation: **4 marks**
* Example showing the row shifting process: **4 marks**
* Clarity and correctness: **2 marks**

**Question 20:**

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

**Grading Rubric**:

* Identification of public-key cryptosystem requirements: **4 marks**
* Explanation of how each requirement ensures security: **4 marks**
* Clarity and completeness: **2 marks**