**Answer\_Set\_4.docx**

**Q1 (a): Encrypt the plaintext "meet me after the toga party" using Rail Fence Cipher and the key depth is 2.**

**A:** The Rail Fence Cipher writes the message in a zigzag pattern along 2 rails. For the plaintext "meet me after the toga party", the encryption process is as follows:

Copy

m e m a t r h t g a a t

e t e f e t e o p r y

The ciphertext is obtained by reading the rows sequentially: **memathrhtgaatetefeteopry**.

**Score: 3, 2, 3, 2, 5**

**Q1 (b): Consider an online banking system in which users provide an account number and password to access the bank account and transfer money online. Mention example of CIA (confidentiality, integrity, and availability) requirements associated with the system. Also discuss the level of importance (low, medium, high) of each requirement on the system.**

**A:**

* **Confidentiality:** Ensuring that only authorized users can access the account information. Example: Encrypting sensitive data like account numbers and passwords. **Importance: High**.
* **Integrity:** Ensuring that the data is not altered during transmission. Example: Using hash functions to verify data integrity. **Importance: High**.
* **Availability:** Ensuring that the banking system is accessible when needed. Example: Implementing redundant servers to prevent downtime. **Importance: High**.

**Score: 3, 2, 3, 2, 5**

**Q1 (c): In relation to classical encryption techniques, explain the following:**

**(i) One Time Pad**

**A:** A One Time Pad (OTP) is an encryption technique that uses a random key that is as long as the message itself. The key is used only once, making it theoretically unbreakable if the key is truly random and kept secret. For example, if the message is "HELLO" and the key is "XMCKL", the ciphertext would be generated by XORing each corresponding character.

**Score: 3, 2, 3, 2, 5**

**(ii) Brute force Attack**

**A:** A brute force attack involves trying every possible key or password until the correct one is found. For example, if a password is 4 digits long, a brute force attack would try all combinations from 0000 to 9999.

**Score: 3, 2, 3, 2, 5**

**(iii) Row Transposition Cipher**

**A:** A Row Transposition Cipher rearranges the plaintext by writing it in rows and then reading the columns in a specific order. For example, if the plaintext is "HELLOWORLD" and the key is 3, the ciphertext would be written in 3 rows and then read column-wise.

**Score: 3, 2, 3, 2, 5**

**Q2 (a): Describe the encryption and decryption process of Feistel Cipher. Use diagram to illustrate your answer.**

**A:** The Feistel Cipher divides the plaintext into two halves, left (L) and right (R). In each round, the right half is combined with a subkey using a round function, and then XORed with the left half. The halves are then swapped. This process is repeated for multiple rounds. Decryption is the same process but with the subkeys applied in reverse order.

**Score: 3, 2, 3, 2, 5**

**Q2 (b): Explain the Fermat’s Theorem and Euler’s Theorem. Use example to illustrate your answer.**

**A:**

* **Fermat’s Theorem:** States that if p is a prime number, then for any integer a, ap≡amod  p*ap*≡*a*mod*p*. For example, if p = 5 and a = 2, then 25=32≡2mod  525=32≡2mod5.
* **Euler’s Theorem:** States that if a and n are coprime, then aϕ(n)≡1mod  n*aϕ*(*n*)≡1mod*n*, where ϕ(n)*ϕ*(*n*) is Euler's totient function. For example, if n = 10 and a = 3, then ϕ(10)=4*ϕ*(10)=4 and 34=81≡1mod  1034=81≡1mod10.

**Score: 3, 2, 3, 2, 5**

**Q2 (c): In relation to number theory, explain the following:**

**(i) Divisibility**

**A:** Divisibility refers to the ability of one integer to be divided by another without leaving a remainder. For example, 10 is divisible by 2 because 10÷2=510÷2=5 with no remainder.

**Score: 3, 2, 3, 2, 5**

**(ii) Modular Arithmetic**

**A:** Modular arithmetic is a system of arithmetic for integers where numbers "wrap around" upon reaching a certain value, the modulus. For example, 7mod  3=17mod3=1 because 7 divided by 3 leaves a remainder of 1.

**Score: 3, 2, 3, 2, 5**

**(iii) Euclidean Algorithm**

**A:** The Euclidean Algorithm is a method for finding the greatest common divisor (GCD) of two integers. For example, the GCD of 48 and 18 is found by repeatedly applying the algorithm: 48÷18=248÷18=2 with remainder 12, then 18÷12=118÷12=1 with remainder 6, and finally 12÷6=212÷6=2 with remainder 0. The GCD is 6.

**Score: 3, 2, 3, 2, 5**

**Q3 (a): In relation to public key cryptography, explain what Bob achieves in terms of confidentiality and authentication in the following scenarios:**

**(i) Bob encrypts a message with Alice's public key and sends it to Alice.**

**A:** Confidentiality is achieved because only Alice, with her private key, can decrypt the message. Authentication is not achieved because anyone could have sent the message.

**Score: 3, 2, 3, 2, 5**

**(ii) Bob encrypts a message with his private key and sends it to Alice.**

**A:** Authentication is achieved because only Bob could have encrypted the message with his private key. Confidentiality is not achieved because anyone with Bob's public key can decrypt the message.

**Score: 3, 2, 3, 2, 5**

**(iii) Bob first encrypts with his private key and then with Alice's public key and sends it to Alice.**

**A:** Both confidentiality and authentication are achieved. Authentication is achieved because only Bob could have encrypted the message with his private key. Confidentiality is achieved because only Alice, with her private key, can decrypt the message.

**Score: 3, 2, 3, 2, 5**

**Q3 (b): Briefly discuss the ShiftRows and AddRoundKey function of AES algorithm. Use example to illustrate your answer.**

**A:**

* **ShiftRows:** In this step, each row of the state matrix is shifted cyclically to the left. The first row is not shifted, the second row is shifted by one byte, the third row by two bytes, and the fourth row by three bytes. For example, if the state matrix is:

Copy

[a b c d]

[e f g h]

[i j k l]

[m n o p]

After ShiftRows, it becomes:

Copy

[a b c d]

[f g h e]

[k l i j]

[p m n o]

* **AddRoundKey:** In this step, each byte of the state matrix is XORed with the corresponding byte of the round key. For example, if the state matrix is [a b c d] and the round key is [k l m n], the result is [a XOR k, b XOR l, c XOR m, d XOR n].

**Score: 3, 2, 3, 2, 5**

**Q3 (c): What requirements must a public-key cryptosystem fulfill to be a secure algorithm?**

**A:** A public-key cryptosystem must fulfill the following requirements:

1. **Key Generation:** It should be computationally infeasible to derive the private key from the public key.
2. **Encryption and Decryption:** The encryption and decryption processes should be computationally efficient.
3. **Security:** It should be resistant to known cryptographic attacks, such as brute force and chosen-plaintext attacks.

**Score: 3, 2, 3, 2, 5**

**Q4 (a): Explain in your own words what you have learned in relation to the True Random Number Generator (TRNG) and Pseudorandom Number Generator (PRNG). Do not write more than 400 words.**

**A:**

* **TRNG:** A True Random Number Generator generates random numbers from physical processes, such as electronic noise or radioactive decay. These numbers are truly random and unpredictable. For example, a TRNG might use the timing of keystrokes to generate random numbers.
* **PRNG:** A Pseudorandom Number Generator generates numbers that appear random but are actually determined by an initial seed value. These numbers are predictable if the seed is known. For example, a PRNG might use a mathematical algorithm to generate a sequence of numbers based on a seed.

**Score: 3, 2, 3, 2, 5**

**Q4 (b): Discuss the Double DES and explain the meet-in-the-middle attack.**

**A:**

* **Double DES:** Double DES uses two keys and applies the DES algorithm twice. The ciphertext is generated by encrypting the plaintext with the first key and then encrypting the result with the second key.
* **Meet-in-the-Middle Attack:** This attack exploits the fact that Double DES can be broken with a time complexity of 256256 instead of 21122112. The attacker encrypts the plaintext with all possible first keys and decrypts the ciphertext with all possible second keys, looking for a match in the middle.

**Score: 3, 2, 3, 2, 5**

**Q4 (c): Perform the DES initial permutation on the Plaintext: 02468aceeca86420. You can use the table 1 (Plaintext in Binary) and table 2 (Initial Permutation (IP)).**

**A:** The initial permutation (IP) rearranges the bits of the plaintext according to a fixed table. For example, if the plaintext in binary is 0000 0010 0100 0110 1000 1010 1100 1110 1110 1100 1010 1000 0110 0100 0010 0000, the IP table will rearrange these bits to produce the permuted plaintext.

**Score: 3, 2, 3, 2, 5**