National University of Computer and Emerging Sciences

Lahore Campus

Information Security (CS3002)

Assignment-I

Total Marks: 20

Total Questions: 5

____________ Roll No

____________ Section

CLO #: 1

Instructions: Solve each question on paper, showing all steps clearly. Submit a report with your solutions. Ensure clarity and conciseness in your explanations.

Questions

1. **Caesar Cipher**
   - **Q1**: Encrypt the following plaintext message using a Caesar cipher with a key of 3:
     Plaintext: "HELLO WORLD"
     Show your work: Include each shift for the individual characters and explain how the encryption works.
   - **Q2**: Given the ciphertext **"KHOOR ZRUOG"**, decrypt it to reveal the plaintext. Assume the key is 3.
     Explain: Describe the decryption steps and verify the result by explaining the key shift back to the original message.
2. **Monoalphabetic Substitution Cipher**
   - **Q1**: Encrypt the following message using the substitution cipher where each letter is mapped as follows:
     Plaintext: "SECURITY"
     Substitution Key: A → Q, B → W, C → E, D → R, E → T, F → Y, G → U, H → I, I → O, J → P, K → A, L → S, M → D, N → F, O → G, P → H, Q → J, R → K, S → L, T → Z, U → X, V → C, W → V, X → B, Y → N, Z → M.
     Show your work: Demonstrate the substitution process for each letter.
   - **Q2**: You receive a ciphertext message: **"LKKXYLTX"**. Using the above substitution key, decrypt it to find the original plaintext.
3. **Vigenère Cipher**
   - **Q1**: Encrypt the plaintext **"ATTACKATDAWN"** using the Vigenère cipher with the keyword "KEY".
     Process: Show the repeated keyword alignment and the resulting ciphertext.
   - **Q2**: Decrypt the following ciphertext **"LXFOPVEFRNHR"** using the keyword "LEMON" to find the original message.
     Steps: Provide the process of using the keyword shifts for each letter in the ciphertext.
4. **Rail Fence Cipher**
   - **Q1**: Use a rail fence cipher with depth 3 to encrypt the following plaintext: **"DEFENDTHEBASE"**.
     Show the Work: Write out the zigzag pattern and read the encrypted message.
   - **Q2**: Given the ciphertext **"TSNRHSIETEYYIAGMIVESSNSA"**, decrypt it using a rail fence depth of 4 to retrieve the plaintext.
     Explain: Illustrate the reverse process of zigzagging and retrieving each row.

5. **Columnar Transposition Cipher**
   - **Q1**: Encrypt the plaintext **"SAVE THE DATA"** using a columnar transposition with key order [3, 1, 4, 2].
     Steps: Organize the letters in a grid and show the column-wise reading order.
   - **Q2**: Decrypt the ciphertext **"SOC HSSE TIPR ITET"** using the key order [3, 2, 4, 1].
     Explanation: Lay out the ciphertext in the grid, and demonstrate how to read each column in the key's sequence to reveal the plaintext.

Submission: Prepare a report with your answers and explanations for each question. Ensure that each step is presented clearly, with the process fully outlined to demonstrate your understanding of each cipher.