National University

of Computer & Emerging Sciences-Lahore

Course – Section	Information Security (CS3002 - Fall 2024) – (BDS-7A, BDS-7B, BSE-7A)
Assignment Number	01
Total Marks	70 Marks
Assigning Date	September 5, 2024
Due Date	September 9, 2024 (for DS sections); September 10, 2024 (for SE section)
Submission	Submit hand-written hardcopy in class (first ten minutes)
Author	Muhammad Mobeen (l247715@lhr.nu.edu.pk)
Approved By	Dr. Syed M. Irteza (m.irteza@nu.edu.pk)
Submission Guidelines	- *Assignments must be received before the deadline. Submissions after the deadline will face a 25% grade penalty (within 1 day) or a 50% grade penalty (within 2 days).* - *Please do the work by yourself, this is an individual assignment.* - *Plagiarism cases will be dealt with strictly.* - *Read questions and marks distribution carefully and write precise answers, avoiding wordy stories.* - *Make assumptions where needed but state them clearly in your answer.* - *Make sure you clearly identify your name, roll number and section*

Question 1. Caesars's Cipher [10 marks]

Q 1.1 Encrypt your Instructor Name by using Caesars's Cipher. Key should be the default value.

Q 1.2 Perform Cryptanalysis on the following text:

ZHORYHSDNLVWDQ

Question 2. Monoalphabetic [10 Marks]

Decrypt the following text by using Frequency analysis

BNCEPQCBEAQBEBIMQFNIYQAEAEYCPMHVMAYCMP

Note: Clearly state Frequency table and explain how you solved it and what are the challenges you faced while doing cryptanalysis.

Question 3. Vigenère cipher **[10 Marks]**

By using Vigenère cipher, Perform encryption and decryption on the following text:

Plaintext = KTWOISTHEHIGHESTPEAKOFPAKISTAN
Key = FASTNUCES

Question 4. Row Transposition **[20 Marks]**

4.1 By using Row Transposition, Perform encryption and decryption on the following text:
Plaintext = ATTACKPOSTPONEDUNTILTWOAM
Key = IRTEZA

4.2 By using Row Transposition, Perform encryption and decryption on the following text:
Plaintext = SAVEYOURSELFWEAREDISCOVERED
Key = PAKISTAN

Note: Explain how you solved it and what are the challenges you faced while doing cryptanalysis.

Question 5. Rail Fence **[15 Marks]**

By using Rail Fence Cipher, Perform encryption and decryption on the following text:
Depth = 3

Plaintext = THE LAHORE FORT IS LOCATED IN THE NORTHERN PART OF LAHORE’S OLD WALLED CITY.

Question 6. Rail Fence **[5 Marks]**

Perform Only Decryption (try to find out the depth level by yourself):

Cipher text = WWLHVAUZNODYEILAEQIOMNA