NED UNIVERSITY OF ENGINEERING & TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

BS CS, Midterm Examinations Fall 2023

Time: 90 minutes **Network & Information Security (CT-486) - A** **Max Marks: 20**

Date: 27-11-2023

Note: Attempt all questions.

Q-1) ***Modify*** the Playfair encryption scheme by including the numbers (0 to 9) and a special character hyphen (-) in its encryption matrix. ***Compute*** the ciphertext of last four characters of your Roll No. in the format (e.g. **CT-001**) as the plaintext. Use the first six non-repeating letters of your name as the secret keyword. [CLO 6] [4]

Q-2) Consider an encryption key of *Hill Cipher* consisting of the four numbers from your cyphertext of above Q1 and calculate the inverse key matrix. Modify the key if the inverse key is not possible. ***Validate*** the keys by encrypting and decrypting the last four letters of your name. [CLO 6] [4]

Q-3) ***Design*** an attack model to ***explain*** that it is not safe to use the same key repeatedly in a One Time Pad scheme. [CLO 2] [4]

Q-4) ***Describe*** the Meet-in-the-Middle attack model to demonstrate the weakness of 2DES encryption scheme. [CLO 2] [4]

Q-5) In a specific application of secret live data streaming (byte stream) you are required to use 3DES for sending encrypted data. Because of the sensitivity of data, it is required to propagate even a small minor modification or change in data during transmission. ***Design*** an appropriate mode of operation for this scenario. [CLO 6] [4]

NED UNIVERSITY OF ENGINEERING & TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY
BS CS, Midterm Examinations Fall 2023

Time: 90 minutes **Network & Information Security (CT-486) - B** **Max Marks: 20**

Date: 27-11-2023

Note: Attempt all questions.

Q-1) Consider an encryption key of *Hill Cipher* consisting of the first four letters from your name and calculate the inverse key matrix. Modify the key if the inverse key is not possible. ***Validate*** the keys by encrypting and decrypting the first four symbols of your own Roll No. neglecting the hyphen (e.g. **CT001**). [CLO 6] [4]

Q-2) ***Modify*** the Playfair encryption scheme by including the numbers (0 to 9) in its encryption matrix. ***Compute*** the ciphertext of first four letters of your name as the plaintext. Use the last five non-repeating letters of your name as the secret keyword. [CLO 6] [4]

Q-3) ***Explain*** the practical limitations of the One Time Pad scheme. [CLO 2] [4]

Q-4) ***Explain*** how DES scheme was improved after the successful demonstration of a brute force attack on it. [CLO 2] [4]

Q-5) In a specific application of secret live data streaming (byte stream) you are required to use DES for sending encrypted data. The nature of the application is such that it is strictly required to avoid any error propagation in data during transmission. ***Design*** an appropriate mode of operation for this scenario. [CLO 6] [4]