B.Sc. Engg. CSE 7th Semester 03 October 2022 (Morning)

ISLAMIC UNIVERSITY OF TECHNOLOGY (IUT)

ORGANISATION OF ISLAMIC COOPERATION (OIC)

Department of Computer Science and Engineering (CSE)

MID SEMESTER EXAMINATION **WINTER SEMESTER, 2021-2022**

DURATION: 1 HOUR 30 MINUTES **FULL MARKS: 75**

CSE 4743: Cryptography and Network Security

Programmable calculators are not allowed. Do not write anything on the question paper.

Answer all 3 (three) questions. Marks of each question and corresponding CO and PO are written in the right margin with brackets.

---

1. a) Choose the technique (cryptography or steganography) and its subtypes that should be used in each of the following cases for confidentiality: 2×5 (CO1) (PO2)
   i. A student writes the answer to a test on a small piece of paper, rolls up the paper, and inserts it in a ball-point pen, and passes the pen to another student.
   ii. To send a message, a spy replaces each character in the message with a symbol that was agreed upon in advance as the character's replacement.
   iii. A company uses special ink on its checks to prevent forgeries.
   iv. A graduate student uses watermark to protect her thesis, which is posted on her website.
   v. Members of the secret 'Nuvos' family uses a digital lock when entering their meeting room.

   b) Ayai and Irido are two friends studying in the same grade. Ayai sends a secret message, *"DCTE GW TW TVC DKGVTE RCETKXUD"* to Irido using Affine Cipher with keys, $k_1 = 15$ and $k_2 = 20$. Deduce the original message. 10 (CO2) (PO1)

   c) Some archeologists found a new script written in an *unknown language*. The archeologists later found a small *tablet* at the same place that contains a sentence in the same language with the translation in Greek. Using the tablet, they were able to read the original `script`. Identify the type of cryptanalysis attack with proper justification the archeologists used. 5 (CO2) (PO1)

2. a) Alice often needs to encipher plaintext made of both letters (a to z) and digits (0 to 9). For each of the following scenarios, determine the key domain and the modules: 2×3 (CO2) (PO1)
   i. If she uses an additive cipher.
   ii. If she uses a multiplication cipher.
   iii. If she uses an affine cipher.

   b) Determine the ciphertext for the message "cryptography is fun" each of the following ciphers. 6×2 (CO2) (PO1)
   i. Autokey Cipher with key = 12.
   ii. Vigenere Cipher with key = "lucky"

   c) Suppose you have a modem block cipher where the number of input bits, n = 64 and the number of output bits, m = 64. If there are ten 1's in the ciphertext, determine the number of tests you need to conduct to recover the plaintext from the ciphertext for each of the following cases: 3.5×2 (CO3) (PO1, PO2)
   i. The cipher is designed as a *substitution* cipher
   ii. The cipher is designed as a *transposition* cipher

3 a) The input/output relation in a 2 × 2 S-box is shown in Table 1. Show the table for the inverse S-box that is used in decryption. 6 (CO3) (PO1, PO2)

Table 1: Table for Question 3(a)

Input	0	1
0	01	11
1	10	00

b) The final design of the Feistel Cipher is shown in Figure 1. 12 (CO3) (PO1, PO2)

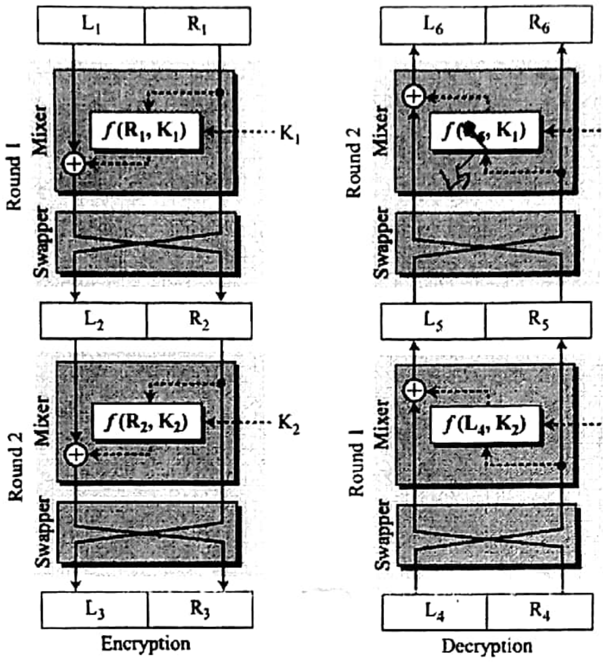

Figure 1: Figure for question 3(b)

Show appropriate mathematical calculations and reasoning to derive, ***L₆*** = ***L₁*** and ***R₆*** = ***R₁***. Assess the differences between this design and its previous iterations.

c) What is called the heart of Data Encryption Standard (DES)? Illustrate the working principle of *S-Box* in each round of DES. 7 (CO3) (PO1, PO2)