Name of the Program: B.Sc. in Computer Science Engineering **Date: 20 June, 2021**
Semester: Winter 2020-2021 **Time: 2:30 pm – 4:00 pm**

ISLAMIC UNIVERSITY OF TECHNOLOGY (IUT)
ORGANISATION OF ISLAMIC COOPERATION (OIC)
DEPARTMENT OF MECHANICAL ENGINEERING (ME)

Mid Semester Examination **Winter Semester: 2020 – 2021**
Course Number: CSE 4743 **Full Marks: 75**
Course Title: Cryptography and Network Security **Time: 1.5 Hours**

Programmable calculators are not allowed. Do not write anything on the question paper.
There are **3 (three)** sets of questions. Answer all **3 (three)** of them.
Marks of each question and corresponding CO and PO are written in brackets.

---

1. a) What are the different types of security attacks threatening Confidentiality, Integrity and Availability and discuss which security mechanisms can counter them? (8) (CO1) (PO1, PO2, PO6)

   b) Hinata and Kageyama are two volleyball players for their high school team, Karasuno High. In order to communicate discreetly, Hinata sends Kageyama two secret cipher messages with a shared secret key, ***k*** where k = 15 using Caesar cipher and Multiplicative cipher respectively. Decrypt the enciphered messages to get the original plaintext. (12) (CO2) (PO1, PO3)
      i) ***HPLPBJGP SPXRWX XH HRPGN*** *(Caesar Cipher)*
      ii) ***UAVAKONC SQJJ PIAZ KBQVAZCVQLASA*** *(Multiplicative Cipher)*

   c) Calculate the key domain size for Affine Cipher and elucidate why is it vulnerable to brute force attack? (5) (CO2) (PO1, PO3)

2. a) Encrypt the message ***"the question is easy"*** using the following ciphers. Encrypt them to get the cipher text. (12) (CO2) (PO1, PO3)
      i) Autokey Cipher with key = 12.
      ii) Vigenere Cipher with key = "lucky"

   b) Figure 1 demonstrates a simple product cipher with two rounds. How does this product cipher gurantee the diffusion and confusion properties? Clarify your statement with appropraite daiagram. (10) (CO3) (PO1, PO2)

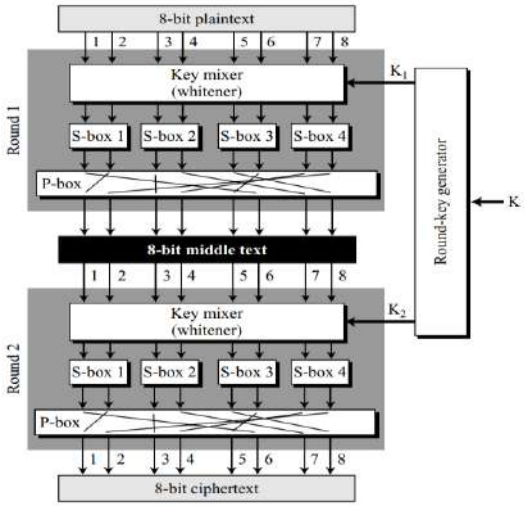

Figure 1: Figure for question no. 2(b)

2. c) "A modern block cipher can be designed to act as a substitution cipher or a transposition cipher" – Justify this statement. (3) (CO3) (PO1, PO2)

3 a) Explain the properties of exclusive-or operation component in modern block ciphers and how it assists in Feistel Ciphers (5) (CO3) (PO1, PO2)

b) The final design of the Feistel Cipher is given in Figure 2. Show appropriate mathematical calculations and reasoning to derive, ***L6 = L1*** and ***R6 = R1.*** Explain how is it different from the previous designs? (12) (CO3) (PO1, PO2)

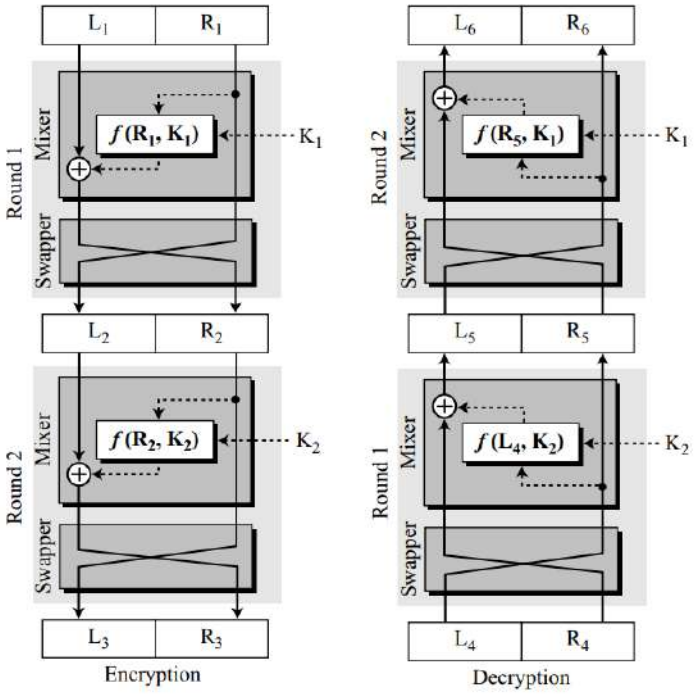

Figure 2: Figure for question no. 3(b)

c) What is called the heart of Data Encryption Standard (DES)? Describe the working principle of *S-Box* in each round of DES. (8) (CO3) (PO1, PO2