B.Sc. Eng. CSE 7th Semester **08 March 2019 (Afternoon)**

ISLAMIC UNIVERSITY OF TECHNOLOGY (IUT)
ORGANISATION OF ISLAMIC COOPERATION (OIC)
Department of Computer Science and Engineering (CSE)

MID SEMESTER EXAMINATION **WINTER SEMESTER, 2018-2019**
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.

There are **4 (four)** questions. Answer any **3 (three)** of them.

Figures in the right margin indicate marks.

1. a) What do you understand by the terms *Authentication, Data Confidentiality and Data Integrity*? 8

   b) Write short notes on the following, 7
      i. Digital Signature.
      ii. Public Key Cryptography.

   c) Distinguish between *Cryptography* and *Steganography*. Mention few historical uses and few modern uses of Steganography. 10

2. a) Name some passive attacks and active attacks. Define the type of security attacks in each of the following cases: 6
      i. A student breaks into a professor's office to obtain a copy of the next day's test.
      ii. A student gives a check for $10 to buy a used book. Later she finds that the check was cashed for $100.

   b) Use the *Playfair cipher* to encipher the message "The Key Is Hidden". The secret key can be made by filling the first and part of the second row with the word "GUIDANCE" and filling the rest of the matrix with the rest of the alphabets sequentially. 9

   c) The encryption key in a *Transposition cipher* is (3, 2, 6, 1, 5, 4). Find the decryption key. 5

   d) "The *One-Time Pad* can be proven unbreakable" – justify the statement. 5

3. a) Draw the general structure of *DES (Data Encryption Standard)*. 5

   b) Draw a single *Feistel Round* of *DES*. How the Feistel design helps DES to run the Encryption and Decryption algorithm in same direction? 10

   c) What is the *block size*, *key size* and the *number of rounds* in *AES (Advanced Encryption Standard)*? Why AES is not a Feistel algorithm? 5

   d) The following ciphertext is encrypted by using *Caesar cipher* with the shift parameter value 3. Decrypt it. 5

      "fdhvdu flskhu lv hdvb"

4. a) Are all block ciphers polyalphabetic? 3

b) What is called the heart of *DES?* Briefly explain the working principle of *S-box* in each round of *DES.* 10

c) What do you understand by *Diffusion* and *Confusion*? 5

d) Figure 1 demonstrates a simple product cipher with two rounds. How does this product cipher guarantee the *diffusion* and *confusion* properties? Clarify your statement with appropriate figure. 7

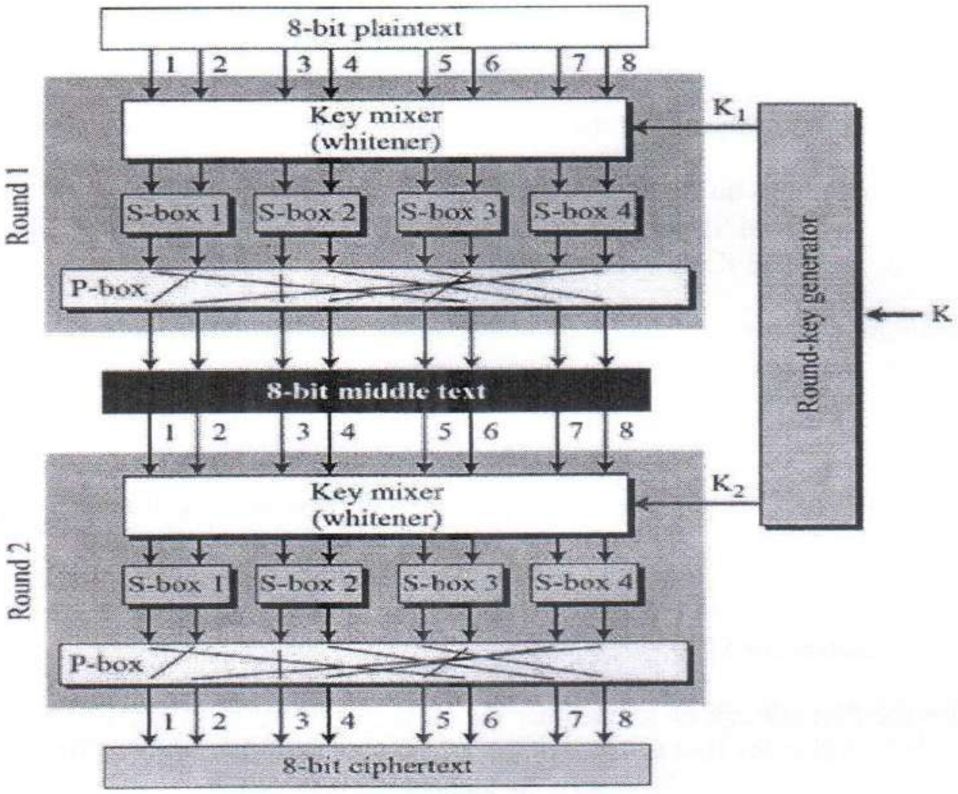

Figure 1