GC University Lahore

ASSIGNMENT

MARKS = 10

INFORMATION SECURITY (CS-4215)
BSCS (HONS) SEMESTER-VIII 2019-2023 SECTION "CSA1 AND CSE$_1$"

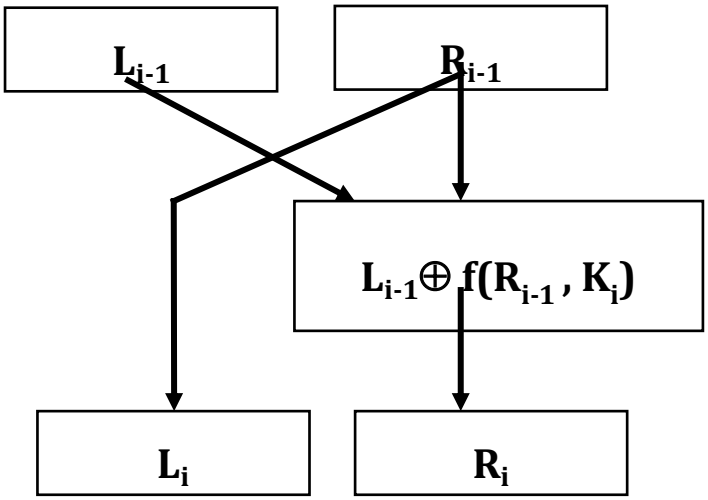
You are given 64-bit Cipher Text message and 64-bit Key given below;

Text [Plain/Cipher] = [0011 0101 0111 0000 1110 0010 1111 0001 1011 1010 0100 0110 1000 0010 1100 0111] 3570E2F1BA4682C7$_{HEX}$

KEY= [0101 1000 0001 1111 1011 1100 1001 0100 1101 0011 1010 0100 0101 0010 1110 1010] 64 bit key (Compute K_1 & K_2 using Key Generation module of standard DES)

This assignment covers a numerical example of **two-round** version of Data Encryption Standard Algorithm (namely myDES). You have to encrypt/decrypt the given Text[Plain/Cipher] using myDES based on your Roll Number. Show the stepwise working of each Round of myDES Encryption/Decryption process.

Note: Students with Odd Roll Numbers will do decryption and Students with Even Roll Numbers will do encryption.



DES i^{th} Round pictorial description

Plagiarism:

All students are expected to be familiar with the regulations on plagiarism and other academic offences. Instances of plagiarism in this course will be dealt according to the University regulations. You may discuss general approaches to assignment problem(s) with classmates. However, these must be general and cannot include things such as detailed steps to follow in a proof. The assignment which you submit must be your own work. Anybody involved in act of plagiarism will be given **grade F.**

Submission Criteria:

You have to submit soft copy (Excel/Word) file at following email address
yahyakhuram@gmail.com (only given email address is valid/accepted)
Do mention your Name and Roll Number in Subject line while submitting Assignment.
Due Date is Tuesday (16-MAY-2023) before 22:00 PST.