ASSIGNMENT I

CS549: Computer & Network Security   Total Marks: 10

DES is a block cipher and encrypts data in blocks of size of **64 bits** each, which means 64 bits of plain text is used as input to DES, which produces 64 bits ciphertext. The same algorithm and key are used for encryption and decryption, with minor differences.

This is group assignment. Maximum 4 students can participate in a group.

Requirement in this Assignment is to **implement the DES algorithm**, where the 64-bits plain text should be formed using two students' last eight digits of their roll numbers. Please note that each digit is represented as hexadecimal. So, ((8+8) *4 = 64-bit). Similarly, the 64-bits key should be created using the roll number of other two students in the group.

For example:

Roll numbers of students S1 and S2: 2**14101003**, 2**14101004**

Selected digits- 14101003, 14101004

So, the input plain text (in decimal): 1410 1003 1410 1004

and the same in binary: 0001 0100 0001 0000 0001 0000 0000 0011 0001 0100 0001 0000 0001 0000 0000 0100

Do the similar operation using the roll numbers of student S3 and S4 to get the 64-bits key.

If any group has less number of students, then they can use any other roll number which is not same with any member of the group.

Results to be Produced:

In the submitted documentation file, you must **write output after following operations** in the DES algorithm:

1. Initial permutation (mention LPT and RPT) [Marks: 2]
2. For all 16 rounds: [Marks: 2+2+2]
    a. Expansion permutation
    b. Subkey used in the round
    c. LPT and RPT after the round
3. Final permutation (mention Ciphertext) [Marks:2]

Report Submission Strategy:

- ✓ Each group will have 4 members.

- ✓ Any one member of the group should submit the report. In case of multiple submission, only one (randomly chosen) report will be evaluated.
- ✓ Naming convention of the document: GrpNo_<Group number>_CNS_Assignment1.pdf
- ✓ In each report, you should provide the results corresponding to the following set of combinations:
    - For student S1:
        - Plain Text from: S1 S2
        - Key from S3 S4
    - For student S2:
        - Plain Text from: S2 S3
        - Key from S4 S1
    - For student S3:
        - Plain Text from: S3 S4
        - Key from S2 S1
    - For student S4:
        - Plain Text from: S4 S1
        - Key from S3 S2