HTU Course Title: Cryptography

Session 1 and 5: Practical Session on DES
Exam time: 120 minutes
Date: 1/04/2024
Student name:
Student ID:

Lab Objectives:

- ➢ Gain proficiency in bitwise operations and mathematical transformations used in product ciphers.
- ➢ Implement simple encryption and decryption functions in the C programming language.
- ➢ Validate the correctness and efficiency of the implemented algorithm through test cases and performance analysis.

Task:

The encryption algorithm under consideration is tailored for securing sensitive yet non-confidential data. Distinguished by its bit-oriented approach, unlike conventional ciphers, it integrates both transformation and substitution processes, earning it the moniker of a 'product cipher.' Each input and output block spans 8 bits, with a 10-bit key orchestrating the encryption process across two rounds. These rounds are fueled by distinct 8-bit keys, derived from the original key block through a series of operations including parity bit elimination, bit permutation, and subsequent extraction of 8 bits.

1-Based on the following schemes:

- ○ calculate the value of the block cipher mathematically.
    - Let's assume this is your key in binary, which has 10 bits.
      Key: 0x282.
    - Let's assume this is your plain text in binary, which has 8 bits.
      Plain text: 0xF2.

    - Assume the permutation tables is defined as the follow:

P10	
Input	1 2 3 4 5 6 7 8 9 10
Output	3 5 2 7 4 10 1 9 8 6
P8	
Input	1 2 3 4 5 6 7 8 9 10
Output	6 3 7 4 8 5 10 9
P4	
Input	1 2 3 4
Output	2 4 3 1

- Assume that the Initial and Final Permutations are defined as follows:

Initial Permutation							
2	6	3	1	4	8	5	7
Final Permutation							
4	1	3	5	7	2	8	6

- Assume that there are only two s-boxes:

S_0

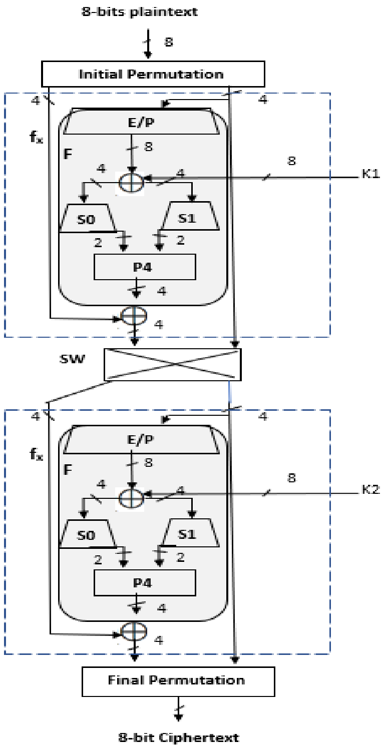
01	**00**	**11**	**10**
11	**10**	**01**	**00**
00	**10**	**01**	**11**
11	**01**	**11**	**10**

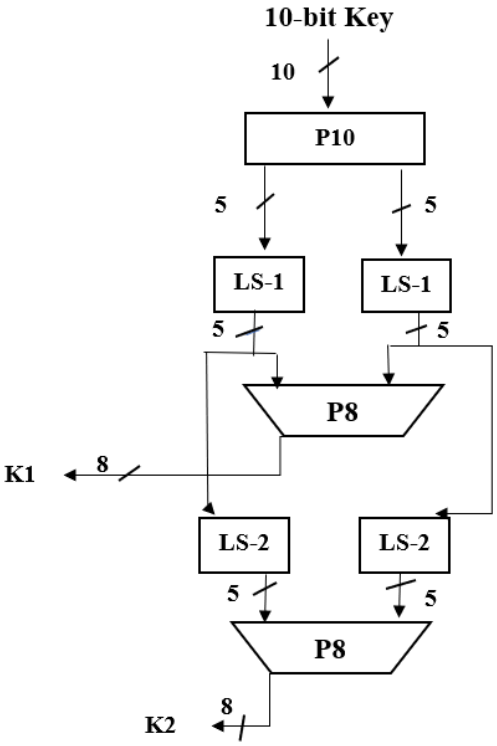
S_1

00	**01**	**10**	**11**
10	**00**	**01**	**11**
11	**00**	**01**	**00**
10	**01**	**00**	**11**

- Assume that the EP table is as follows :

Expansion Permutation(E/P)							
4	1	2	3	2	3	4	1





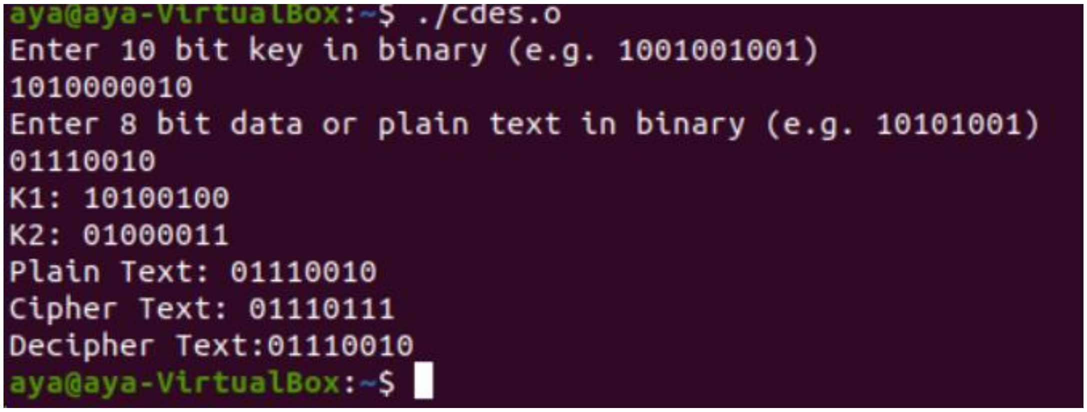
Encryption Scheme

- ***Expected output:***

  Ciphertext:0xD1

2- Write C code corresponding to the proposed block cipher algorithm. Your program should simulate this block cipher and display the ciphertext along with the corresponding plaintext and key.

- ***Expected output:***



```
aya@aya-VirtualBox:~$ ./cdes.o
Enter 10 bit key in binary (e.g. 1001001001)
1010000010
Enter 8 bit data or plain text in binary (e.g. 10101001)
01110010
K1: 10100100
K2: 01000011
Plain Text: 01110010
Cipher Text: 01110111
Decipher Text:01110010
aya@aya-VirtualBox:~$ 
```