GHARDA FOUNDATION'S

GHARDA INSTITUTE OF TECHNOLOGY

Department of Computer Engineering

Evaluation Sheet

Class: T.E Computer Engineering **Sem:** VI

Subject: Cryptography and System Security

Experiment No: 15

Date:

Title of Experiment: Virtual Lab Experiment – Triple DES.

Sr. No.	Evaluation Criteria	Max Marks	Marks Obtained
1	Practical Performance	12	
2	Oral	2	
3	Timely Submission	1	
	Total	15	

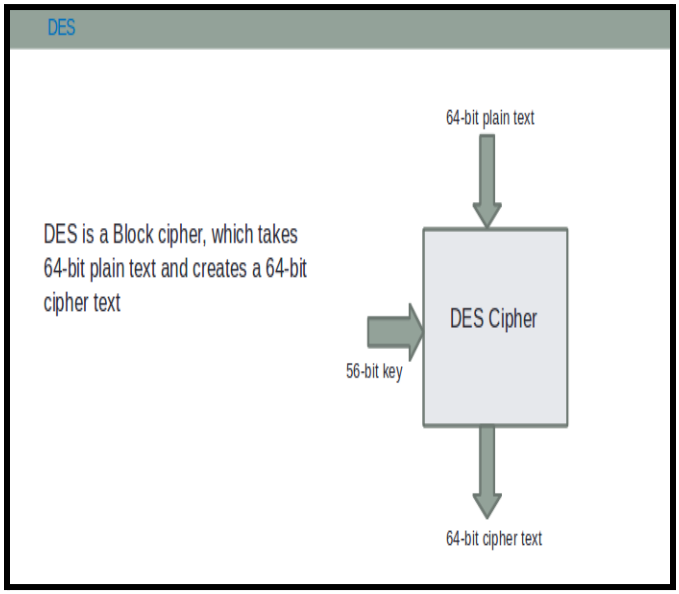
Signature of Subject Teacher
[Vijesh M.Nair]

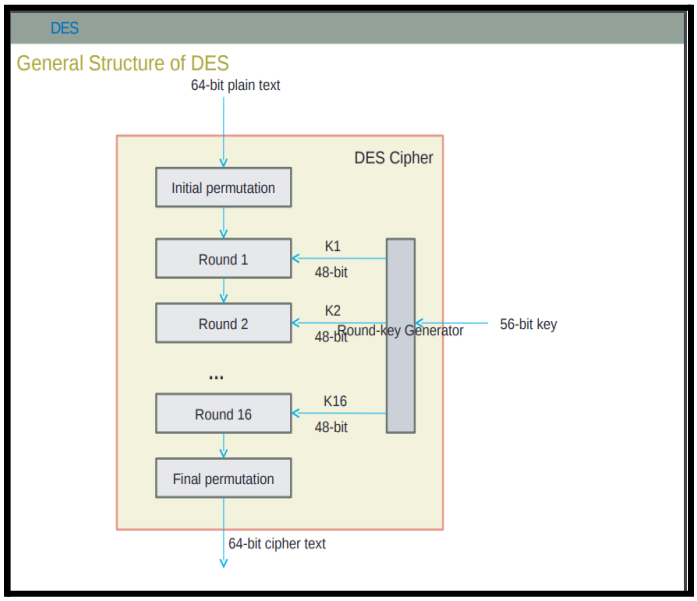
Experiment No. 15

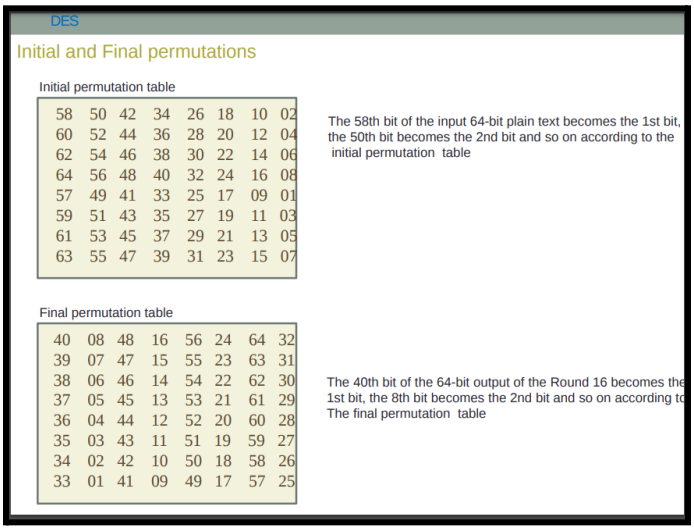
Aim : In this experiment, you are asked to design the triple DES cryptosystem provided that you are given an implementation of DES.

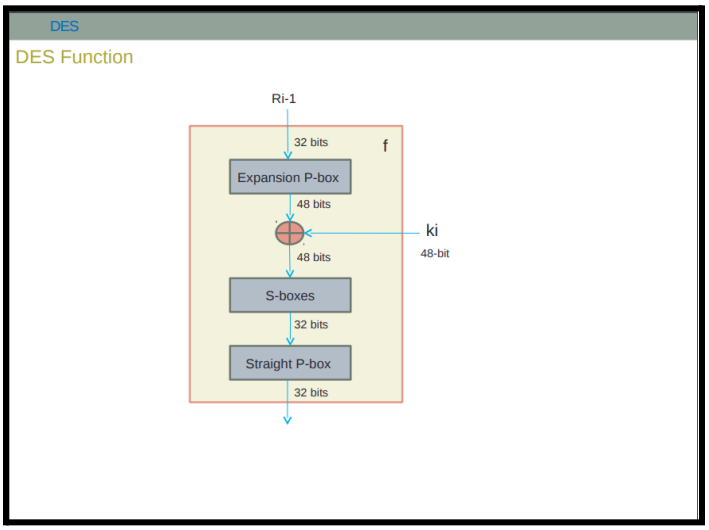
Theory :

From DES to 3-DES



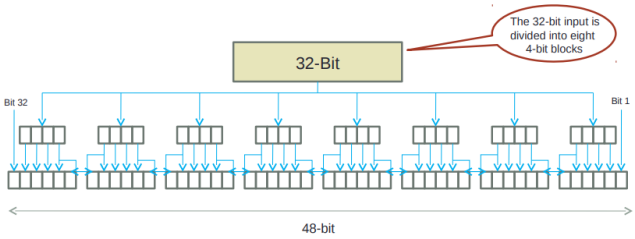






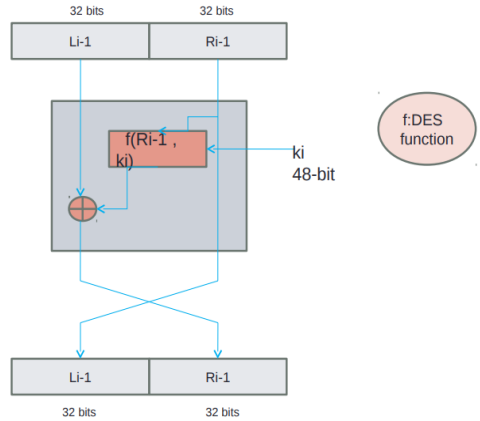
DES Function : Expansion permutation

The input 32-bits are expanded to 48 bits in the Expansion P-Box module in the following way



The resulting 48-bit output is permuted using the Expansion P-Box

One round in DES (Feistel structure)



DES Function : Expansion Permutation and Straight permutation

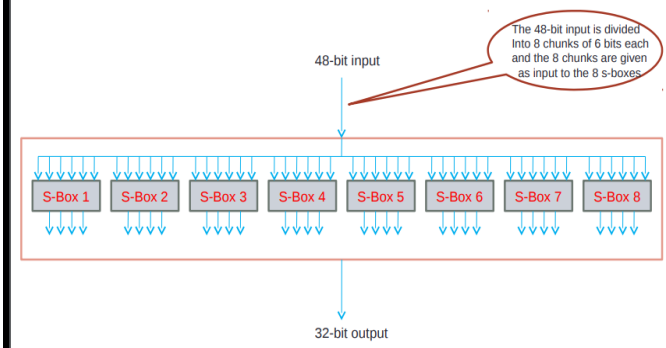
Expansion P-box

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	01

Straight P-box

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

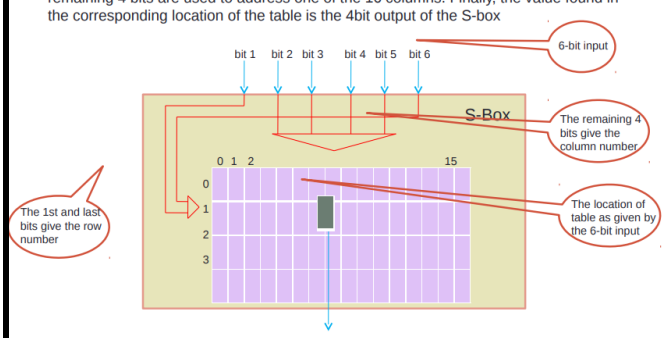
DES Function : Substitution Boxes



The output of each S-box is 4-bit. When these are combined the result is a 32-bit output

DES Function : Substitution Boxes

Each S-box uses a corresponding 4 row by 16 column table
Given a 6-bit input, the 1st and the 6th bits are used to address one of the rows and the remaining 4 bits are used to address one of the 16 columns. Finally, the value found in the corresponding location of the table is the 4bit output of the S-box



DES Function : Substitution Boxes

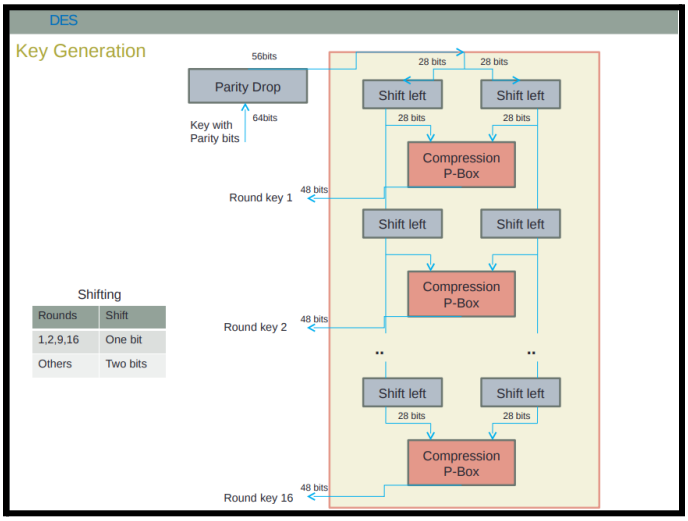
An Example

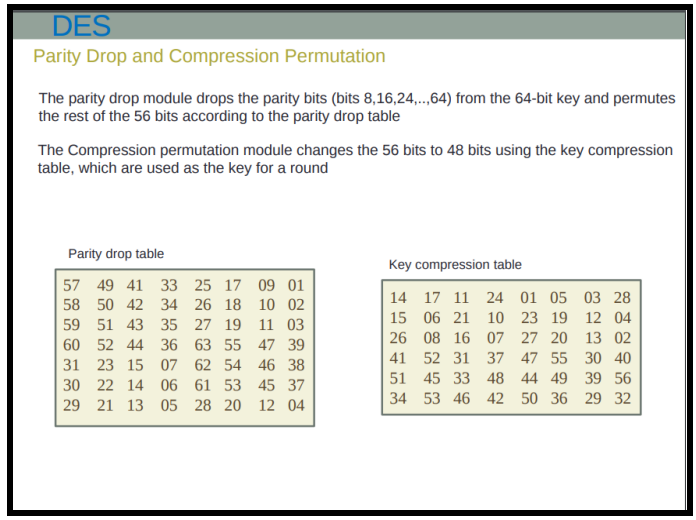
Consider the 6-bit input to s-box 1 is 100011
The 1st and last bits put together is 11 which is '3' in decimal. So we select the 3rd row
The middle bits are 00001 which is '1' in decimal. So we select the 1st column

The corresponding table for S-box 1 is shown below

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

The value in the 3rd row and 1st column is 4 (in binary)





Objective : To understand how to convert a DES implementation to a triple-DES implementation.

Procedure :

Step 1 : Generate Plaintext m, keyA and keyB by clicking on respective buttons PART I of the simulation page.

Step 2 : Enter generated Plaintext m from PART I to PART II in "Your text to be encrypted/decrypted:" block.

Step 3 : Enter generated keyA from PART I to PART II "Key to be used:" block and click on DES encrypt button to output ciphertext c1.This is First Encryption.

Step 4 : Enter generated ciphertext c1 from PART II "Output:" Block to PART II in "Your text to be encrypted/decrypted:" block.

Step 5 : Enter generated keyB from PART I to PART II in "Key to be used:" block and click on DES decrypt button to output ciphertext c2.This is Second Encryption.

Step 6 : Enter generated ciphertext c2** from PART II "Output:" block to PART II in "Your text to be encrypted/decrypted:" block.

Step 7 : Enter generated keyA from PART I to PART II "Key to be used:" block and click on DES encrpt button to output ciphertext c3.This is Third Encryption. Encryption is done thrice.This Scheme is called triple DES.

Step 8 : Enter generated ciphertext c3 from PART II "Output:" Block to PART III "Enter your answer here:" block inorder to verify your Triple DES.

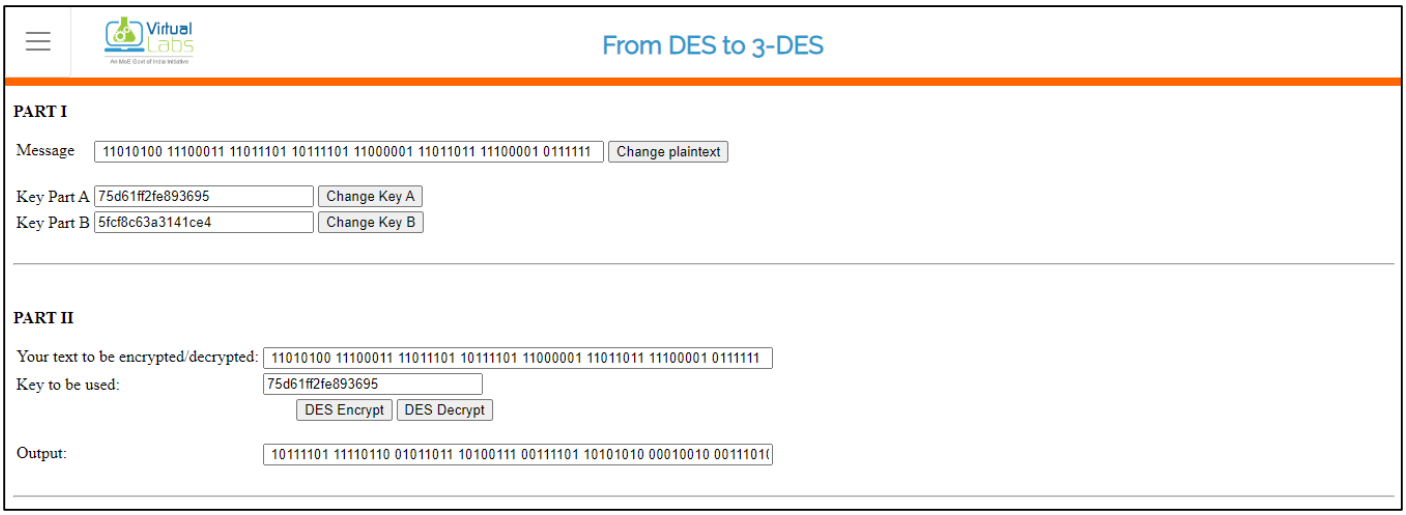
Assignment :

1. In DES input, key length ___ bits and plaintext length ____ bits.
   (a) 56 bit key length, 64 bit plaintext
   (b) 56 bit key length, 120 bit plaintext
   (c) 64 bit key length, 120 bit plaintext
   (d) 64 bit key length, 64 bit plaintext
   Ans- a)
2. DES stands for _____ and AES stands for _____
   (a) Data Encryption software, Advanced Encryption Software
   (b) Data Encryption Standard, Advanced Encryption Standard
   (c) Data Encryption System, Advanced Encryption System
   (d) None
   Ans- b)
3. DES has an initial and final permutation block and ____ rounds
   (a) 14
   (b) 16
   (c) 8
   (d) 12
   Ans- b)
4. In DES the length of each round key?
   (a) 16 bit (b) 32 bit (c) 54 bit **(d) 48 bit**
   Ans- d)

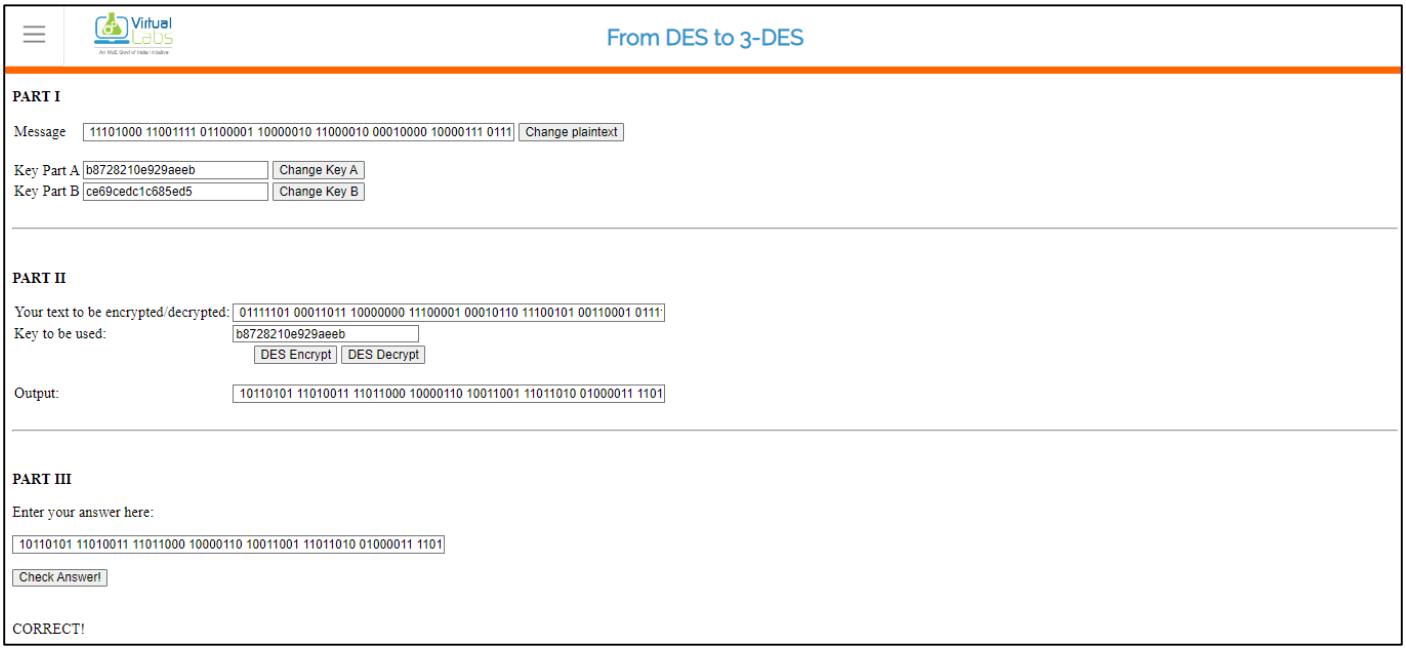
References :

- Wikipedia On Triple DES
- Wikipedia On DES
- Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell.

Output –


Virtual Labs
From DES to 3-DES
PART I
Message
11010100 11100011 11011101 10111101 11000001 11011011 11100001 0111111
Change plaintext
Key Part A
75d61ff2fe893695
Change Key A
Key Part B
5fcf8c63a3141ce4
Change Key B
PART II
Your text to be encrypted/decrypted:
11010100 11100011 11011101 10111101 11000001 11011011 11100001 0111111
Key to be used:
75d61ff2fe893695
DES Encrypt
DES Decrypt
Output:
10111101 11110110 01011011 10100111 00111101 10101010 00010010 0011101


Virtual Labs
From DES to 3-DES
PART I
Message
11010100 11100011 11011101 10111101 11000001 11011011 11100001 0111111
Change plaintext
Key Part A
75d61ff2fe893695
Change Key A
Key Part B
5fcf8c63a3141ce4
Change Key B
PART II
Your text to be encrypted/decrypted:
10111101 11110110 01011011 10100111 00111101 10101010 00010010 0011101
Key to be used:
5fcf8c63a3141ce4
DES Encrypt
DES Decrypt
Output:
01000110 00001011 10101010 01001100 01011100 01101100 01111011 1111111


Virtual Labs
From DES to 3-DES
PART I
Message
11101000 11001111 01100001 10000010 11000010 00010000 10000111 0111
Change plaintext
Key Part A
b8728210e929aeeb
Change Key A
Key Part B
ce69cedc1c685ed5
Change Key B
PART II
Your text to be encrypted/decrypted:
01111101 00011011 10000000 11100001 00010110 11100101 00110001 0111
Key to be used:
b8728210e929aeeb
DES Encrypt
DES Decrypt
Output:
10110101 11010011 11011000 10000110 10011001 11011010 01000011 1101
PART III
Enter your answer here:
10110101 11010011 11011000 10000110 10011001 11011010 01000011 1101
Check Answer!
CORRECT!