Roll No. 41163

Page No.________

Date: / /

Assignment B1

Execution Date: 03/02/2021

Submission Date: 19/05/2021

Title: S-DES Implementation

Problem Statement:

To implement Simplified DES algorithm

Objectives:

Understand Basic of structure of SDES

Understand concepts of S-DES

Logical implementation of SDES

Outcomes:

Will understand and implement S-DES algorithm.

Software Requirements:

- Jupyter Notebook
- Python 3.8.5
- 64 bit operating system

Hardware Requirements:

Computer with 64 bit processor.

Theory:

Simplified DES is an algorithm That has many features of DES, but is much more simpler than DES. Like DES, This algorithm is also a block cipher.

Block Size:

In S-DES, encryption and decryption is done on blocks of 8 bits. The plain text /cipher text is divided into blocks of 8 bits and algorithms is applied on each block.

Key:

The key has 10 bits. The key ki for ith round is obtained by using a set of operations on original key.

Algorithm:

1) Expand K1 and K2 from K
2) $IP(x) = L(x) \| R(x)$
3) Find $EP(R(x)) \oplus K_1 = x_1x_2x_3x_4\ x_5x_6x_7x_8$
4) Apply Sboxes

   $S_0(x_1x_2x_3x_4) \| S_1(x_5x_6x_7x_8) = y_1y_2y_3y_4$

5) Compute

   $L'(x) = L(x) \oplus P_4(y_1y_2y_3y_4)$

   $R'(x) = R(x)$

6) Switch $L'(x)$ and $R'(x)$ to get new input
$R'(x) \; || \; L'(x)$

7) Repeat steps 3-5 for 2nd round

8) Apply the inverse permutation to the output of round 2 to get the final answer.

Permutations:

IP ($x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8$)

1	2	3	4	5	6	7	8

↓

2	6	3	1	4	8	5	7

EP ($x_1 x_2 x_3 x_4$)

1	2	3	4

↓

4	1	2	3	2	3	4	1

P_4 ($x_1 x_2 x_3 x_4$)

1	2	3	4

↓

2	4	3	1

$IP^{-1} (x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8)$

1	2	3	4	5	6	7	8

↓

4	1	3	5	7	2	8	6

Conclusion:

Thus we learnt how to encrypt and decrypt the message by using DES algorithm.