

Assignment B1

Title: Implementation of S-DES

Problem Statement:

Implement the simplified DES algorithm.

Objectives:

- ❖ To learn, understand the basics of encryption
- ❖ To learn encryption algorithm and its uses. – To implement simplified DES algorithm.

Outcomes:

Students will be able to:

- ❖ Study the basics of encryption
- ❖ Understand encryption algorithms and its uses.
- ❖ Implement simplified DES algorithm.

Software and Hardware Requirements:

Laptop / Desktop system with i5 processor, 4GB RAM: 500 GB HDD

OS: Fedora 20, Jupyter Notebook, Eclipse IDE

Theory:

Introduction

Simplified DES is an algorithm that has many features of DES but it is much more simpler than DES. Like DES this algorithm is also a block cipher.

Block size

In SDES encryption and decryption is done on blocks of 12 bits. The plaintext / cipher text is divided into blocks of 12 bits and algorithm is applied on each block.

Key

The key has 9 bits. The key k_i for i th round of encryption is obtained by using 8 bits of k . starting with j th bit.

Algorithm:

The block of 12 bits is written in the form L_0R_0 , where L_0 consists of first 6 bits and R_0 consists of last 6 hits.

The i th round of algorithm transforms an input $L_{i-1}R_{i-1}$ to the output L_iR_i using 8 bit K_i derived from K .

The output of i th round is as follows.

$$L_i = R_{i-1} \text{ and } R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

The operation is performed for a certain number of rounds say n and produce in R_n . The cipher text will be R_n . The

decryption is done in the same way, except the keys are selected in reverse order.

The keys of encryption will be k_1, k_2, \dots and for decryption will be k_n, k_{n-1}, \dots, k_1

1- The 6 bits are expanded using following function. The expansion function takes 6 bits input and produces an 8 bit output. This output is the input for the two 5 boxes.

2- The 8 bit output from the previous step is exclusively ORed with key k_i

3 - The 8 bit output is divided into 2 blocks. The first block consists of the first 4 bits and the last 4 bits make the second block. The first block is the input for first S-box (S_1) and second is input for second sbox (S_2).

4- The S-boxes take 4 bits as input and produce 3 bits of output. The first bit of input is used to select rows from the S-box; 0 for first row and 1 for second row.

5- The output from S-boxes is combined to form a single block of 6 bits. These 6 bits will be the output of the function $f(R_{i-1}, k_i)$.

Conclusion:

We have successfully learnt how to encrypt and decrypt the message by using simplified DES algorithm.

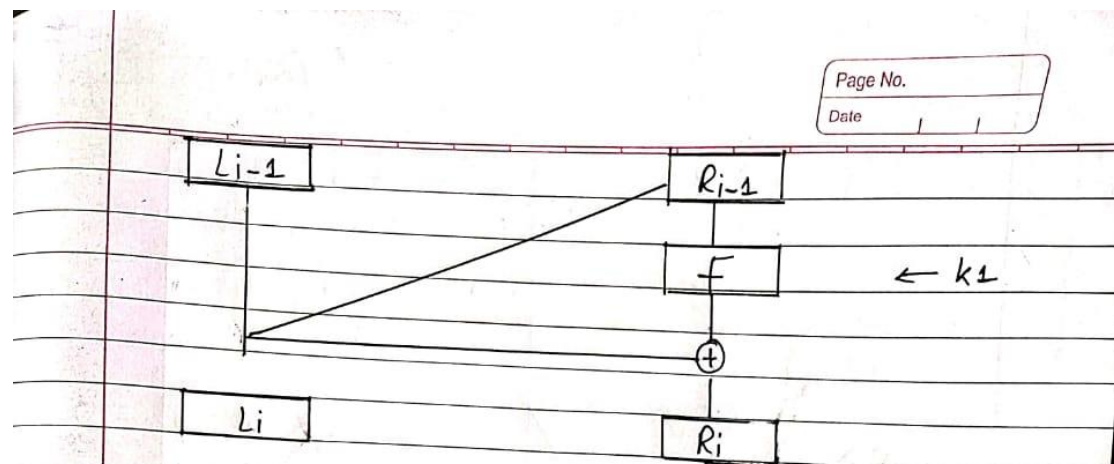


Fig: one Round of feistel system.

Function : $f(R_{i-1}, R_i)$ -
The function is \rightarrow

