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 is 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 ki for ith round of encryption is obtained by using 8 bits of k. starting with jth bit.

Algorithm:

The block of 12 bits is written in the form LoRo, where Lo consists of first 6 bits and Ro consists of last 6 hits.

The ith round of algorithm transforms an input Ii- Ri-l to the output LiRi using 8 bit Ki derived from K.

The output of ith round is as follows.

Li - Ri-1 and Ri = li-l + y(Ri-1, ki)

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

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

The keys of encryption will be ki. k2,. and for decryption will be kn, kn-1... k1

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 ki

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 black. The first block is the input for first S-box (si) 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 rowks from the S-box; o 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 (Ri-1, ki).

Conclusion:

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