Page :
Date : / /

ASSIGNMENT B1

Title : S-DES

Problem Statement : Implementation of S-DES

Objective : To understand and implement S-DES

Outcome : Students will be able to understand the concept of DES and implement S-DES

Requirements : python3, IDE / text-editor

Concept related theory

- Data Encryption Standard (DES) is a symmetric-key block cipher, and is an implementation of Feistel Cipher.

- DES uses a 16-round Feistel structure with a block size of 64 bit and an effective key length of 56 (8 bits unused)

- Since it is based on the Feistel cipher, its components are mainly a round function, a key schedule, and the initial and final permutation.

- DES satisfies two very desirable properties of a block cipher:
  - It has an avalanche effect (small plaintext change results in a very big change in the ciphertext)
  - It has 'completeness' - each bit of the ciphertext depends on many bits of plaintext.

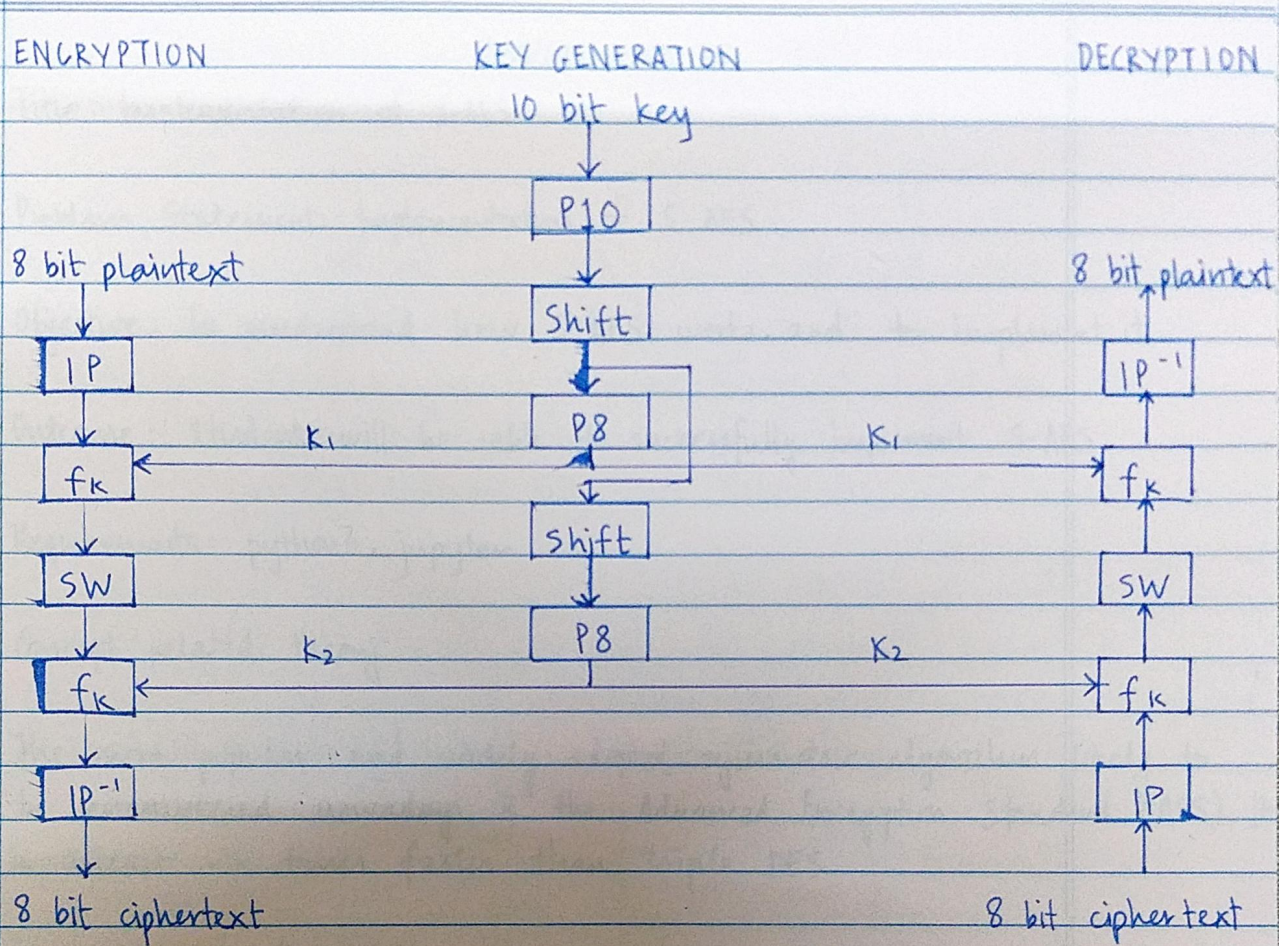
- S-DES, or Simplified-DES is a not-cryptographically secure toy cipher designed to help understand the process behind DES

- S-DES takes an 8-bit plaintext as input, and uses a 10-bit input key, and produces a 8-bit ciphertext after 2 rounds during the encryption process. The decryption module takes the 8-bit ciphertext and the same 10-bit key used in encryption to return the same 8-bit plaintext as the original output after 2 rounds.

- The encryption algorithm involves 5 functions: an initial permutation (IP), a complex function labelled f_K which involves both permutation and substitution operations and depends on a key input, a simple permutation function (SW) that switches two halves of the data, the function f_K again, followed by the final permutation function which is the inverse of the original initial permutation function.

- S-DES depends on the use of a 10-bit key shared between the sender and receiver. From this key, two 8-bit subkeys are produced for use in particular stages of the encryption and decryption algorithm

- The following flowchart describes the encryption, key generation and decryption process in simplified DES algorithm



Test Cases

Input String	Key	Encrypted String	Decrypted String
abcd	1011101110	f ½ 4 z	abcd
hello world	1011101010	nIëëoâko.ëw	hello world

Conclusion

Successfully implemented S-DES algorithm for both 8 bit (integer) input as well as plain text (string) with the execution obtaining the desired results.