PUNE INSTITUTE OF COMPUTER TECHNOLOGY
DHANKAWADI, PUNE –43

LAB MANUAL

ACADEMIC YEAR: 2019- 2020

DEPARTMENT: **COMPUTER ENGG**
CLASS: **B.E** SEMESTER: **II**
SUBJECT: **Laboratory Practice III (410254)**

INFORMATION & CYBER SECURITY

ASSIGNMENT NO	01
TITLE	To implement S – DES
PROBLEM STATEMENT/DEFINITION	Write a program to implement Simplified Data Encryption Standard (S–DES)
OBJECTIVE	
OUTCOME	
S/W PACKAGES AND HARDWARE APPARATUS USED	Core 2 DUO/i3/i5/i7 64-bit processor OS-LINUX 64 bit OS Editor-gedit/Eclipse S/w- Jupyter Notebook/ Weka/ Python
REFERENCES	Cryptography & Network Security, Behrouz A. Forouzan, Tata McGraw Hill.
STEPS	1.
INSTRUCTIONS FOR WRITING JOURNAL	1. Date 2. Assignment No. 3. Problem Definition 4. Learning Objective 5. Learning Outcome 6. Concepts Related Theory 7. Algorithm 8. Test Cases & Troubleshooting 9. Conclusion/Analysis

- **Prerequisites:** Basic knowledge about Algorithms and any programming knowledge.

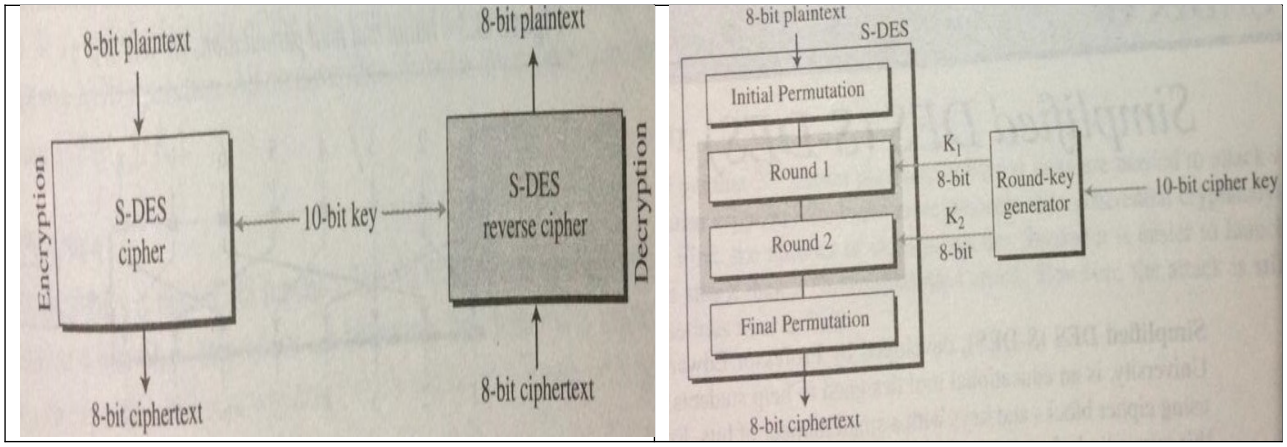
- **Concepts related Theory**

S – DES:

Simplified DES (S – DES), developed by Professor Edward Schaefer of Santa Clara University, is an educational tool designed to help students learn the structure of DES using cipher blocks & keys with a small number of bits.

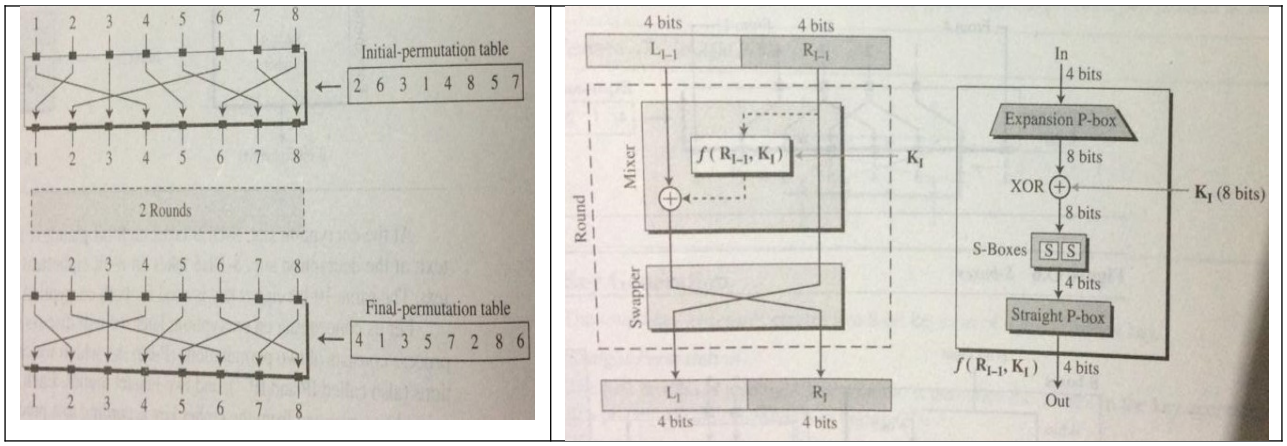
i. It is a block cipher
ii. It has 8–bits block size of plain text or cipher text

iii. It uses 10–bits key size for encryption
iv. It is a symmetric cipher
v. It has two rounds



Steps:
1) Key generation
2) Encryption
3) Switch function
4) Decryption

Encryption algorithm involves five functions:
i. Initial permutation (IP)
ii. complex function f_K
iii. Simple permutation function that switches (SW) the two halves of the data
iv. function f_K again
v. inverse of initial permutation IP^{-1}

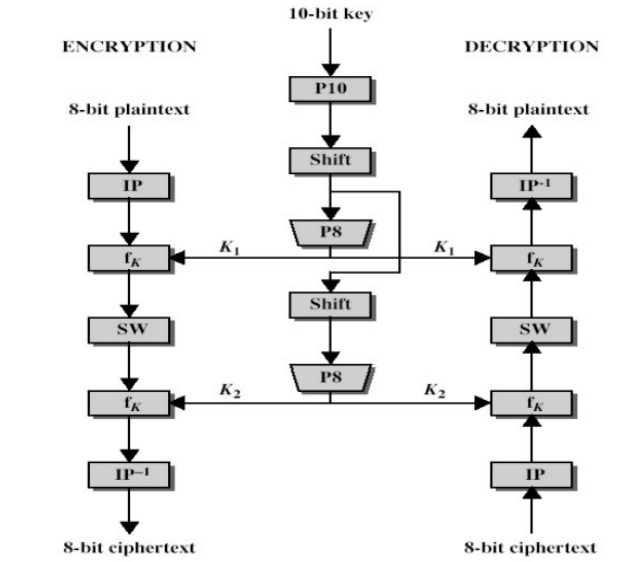


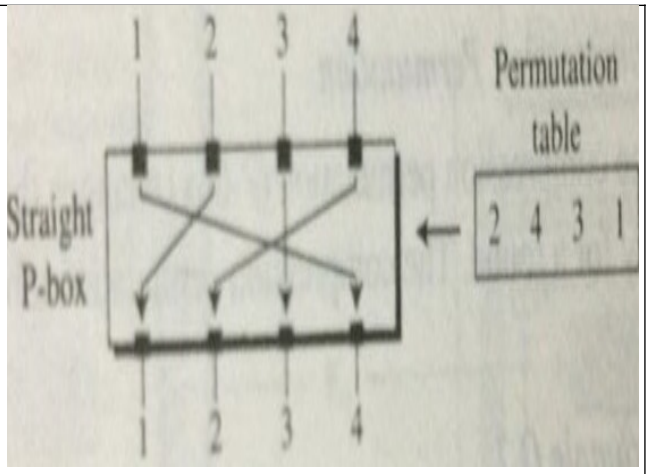
Encryption expressed as a composition function:
IP^{-1} o f_{K2} o SW o f_{K1} o IP

also written as
Ciphertext = IP^{-1} (f_{K2} (SW (f_{K1} (IP (plaintext)))))

where
K1 = P8 (Shift (P10 (Key)))
K2 = P8 (shift (shift (P10 (Key))))

Decryption:
Plaintext = IP^{-1} (f_{K1} (SW (f_{K2} (IP (ciphertext)))))





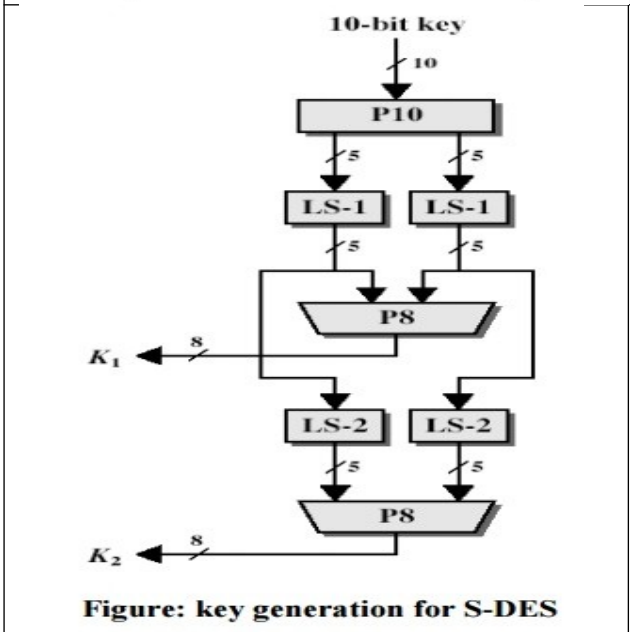
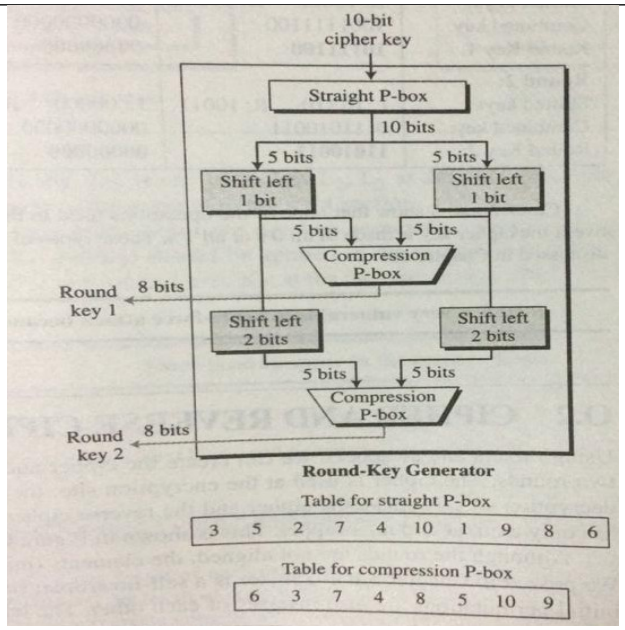
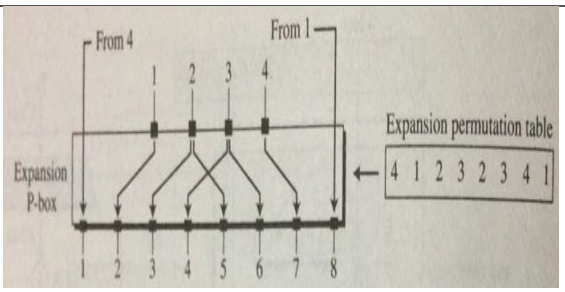
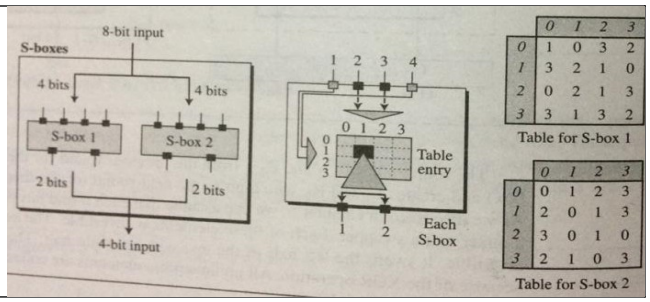


Figure: key generation for S-DES



Expansion P–box	*S–boxes*

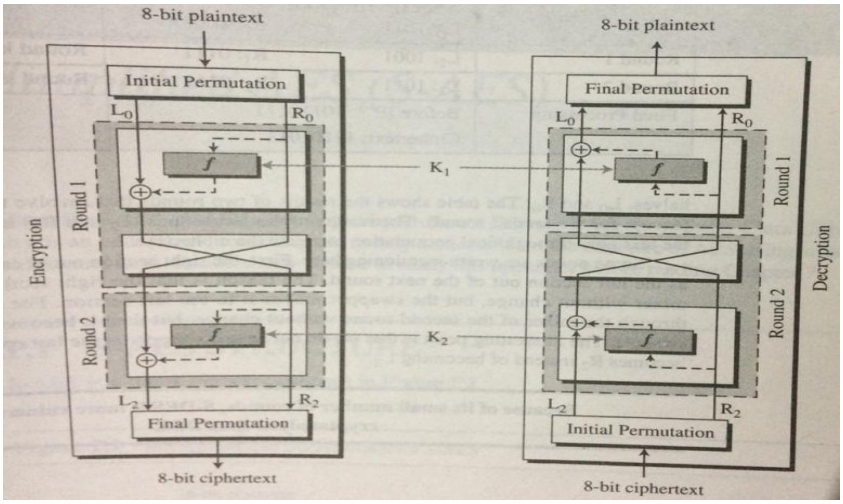




The exact realization of a Feistal network depends on the choice of following parameters & design features:

- Block size: increasing size improves security, but slows cipher
- Key size: increasing size improves security, makes exhaustive key searching harder, but may slow cipher
- Number of rounds: increasing number improves security, but slows cipher
- Subkey generation & round function: Greater complexity can make analysis harder, but slows cipher
- Fast software en/decryption & ease of analysis: are more recent concerns for practical use & testing.

S – DES Cipher & reverse Cipher



S–DES is very vulnerable to brute – force attack because of its key size (10–bits)
Because of its small number of rounds, S–DES is more vulnerable to cryptanalysis that DES

None of the operations used in the key generation process is effective if the cipher key is made of all 0's or all 1's; ∴ these types of cipher keys need to be avoided.

Steps	*Case 1*	*Case 2*	*Case 3*
Cipher Key	**1011100110**	**0000000000**	**1111111111**
After permutation	1100101110	0000000000	1111111111
After splitting	L: 11001 R: 01110	L: 00000 R: 00000	L: 11111 R: 11111
Round 1:			
Shifted keys:	L: 10011 R: 11100	L: 00000 R: 00000	L: 11111 R: 11111
Combined key:	1001111100	0000000000	1111111111
Round Key 1:	**10111100**	**00000000**	**11111111**
Round 2:			
Shifted keys:	L: 01110 R: 10011	L: 00000 R: 00000	L: 11111 R: 11111
Combined key:	0111010011	0000000000	1111111111
Round Key 2:	**11010011**	**00000000**	**11111111**

- **Conclusion:**