

	Date: / /
	Assignment BI
	Execution Put: 03/02/2021
. 3	Submission Po4: 19/05/2021
	litle: S-PES Implementation
	Problem Stutement:
	10 implement simplified DES algorithm
	and the second s
	Objectives:
	Unkertood Busic of sinchure of SDES
	Unverstand concepts of J.DES
	Logical implementation of SDES

autromes: Will understand and implement S-DES algorithm.

Softhwere Requirements:

- Pymon 3.8.5 - 64 bit openting system

Computer with 64 bit processor.

- Jupyler Northook

Mard wave Requirements:



1	
Them	
11.6014	•

Simplified OFS is on algorithm Thut has many features of DES, but is much more simpler than DES. Like DES, This algorithm is also a brock cipher.

Block Size:

In J-DES, encryption and decryption is done on brocks of 8 biss. The plain text Ripmer text is divided into brocks of 8 bits and algorithms is applied on euch brock

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

Algorithm:

1) Expund KI and K2 from K

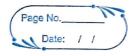
- 2) IP(H)= L(N) 11P(H)
- 3) Find FP(R(H)) (F) K1 = MINING MA HSHONAMS
- 4) Apply Sboxes

30 (n, n 2 n 2 n 4) 11 S, (n 5 n 6 n 7 n 8) = 4, 42 43 44

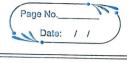
5) Compule

$$L^{(n)} = L(n) \oplus P_n(y_1y_1y_2y_3)$$

R'(n) = R(n)



	6) Switch L'(n) and PI(n) to get new input
	P'(n) 11 L'(n)
	7) Repeat steps 3-5 for 2nd round
	o) Apply the inverse permutation to the output of round
	2 to get the final onswer.
	J T T T T T T T T T T T T T T T T T T T
	Permutotions:
	IP (HIN2 N3 M4M5 MINA)
	1 2 3 4 5 6 7 8
	2 6 3 1 4 8 5 7
	EP (x1x23334)
	1 2 3 4
	4 1 2 3 2 3 4 1
9	
	P4 (x, 2127374)
	1 2 3 4
	ų ,
	2 4 3 1



	1p-1 (n, n2 n3 H4 N5 X6 N7 N5)
	A CONTRACTOR OF THE PARTY OF TH
	1 2 3 4 5 6 7 8
1	the state of the s
	4 1 3 5 7 2 8 6
	Conclusion:
	Thus we learn't how to encrypt and decrypt
	The message by using DES algorithm.

. 3