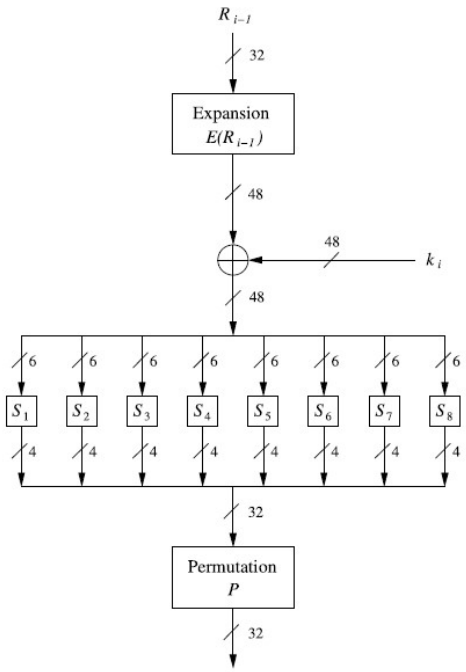
FAST NATIONAL UNIVERSITY
School of Computing
Spring 2021

Course Title:	Computer Organization and Assembly Language
Task:	Assignment #6
Weightage:	3%

Q1. In this assignment, you can work in group of two students. You have to implement the f-Function, which is an essential part of the Data Encryption Standard (DES). In round *i*, it takes the right half of the output of the previous round and the current round key as an input. The output of the f-Function is used as an XOR-mask for encrypting the left half input bits. The block diagram of f-Function is given below:



The expansion permutation is implemented as explained in the table below. You can observe that exactly 16 of the 32 input bits appear twice in the output.

Expansion permutation E

E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

You have to use the code of s-box subroutines from the Assignment # 5. Finally, the sequence of permutation *P* within the f-Function is given below:

The permutation P within the f-function

P							
16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

In this assignment, your task is to implement the f-Function in Assembly language as a subroutine and share its code.