Exercise I - A Simple DES-based Encryption Scheme

We consider a DES-based encryption scheme, which operates on 16-bit blocks of plaintext and uses sub-key of length 12. A sketch of the encryption with first round is given in figure 1. Consider the following bit sequence as the input data: 1011000110101100

a. Describe L_1 and R_1 with respect to R_0, L_0 and K_1.

b. The 16 bits of the input are first reorganized by the following initial permutation (IP).

That is the permuted input has bit 8 of the input as its first bit, bit 13 as its second bit and so on.

8	13	4	9
16	5	12	1
7	14	3	10
15	6	11	2

i. Write down the permuted input.

ii. Compute the inverse permutation namely IP^{-1}.

c. Let the 16 bits of the permuted input block consist of an 8-bit block L followed by an 8-bit block R. The internal structure of the cipher function f (see f in figure 1) is given in fig. 2.

E denotes an expansion function, which takes a block of 8 bits as input and yields a block of 12 bits as output according to the table given below. (The first two bits of output are the bits in position 8, 2, and so on.). Write down the expanded output.

8	2	4
1	3	2
6	1	7
5	3	8

d. S denotes the substitution function, which takes a block of 3 bits and yields a block of 2 bits. Function is given with a table, which contains the decimal representations. (Ex: $(101)_2 = 5$, so from the table, 5 corresponds to 3 which is $(11)_2$.)

0	1	2	3	4	5	6	7
1	3	2	1	0	3	0	2

Write down the output bit sequence with a given sub-key K_1=101101100010

e. Write down L_1 and R_1 as a bit sequence.

f. Combine L_1 and R_1 into 16-bits bit sequence and apply the inverse permutation (IP^{-1}).

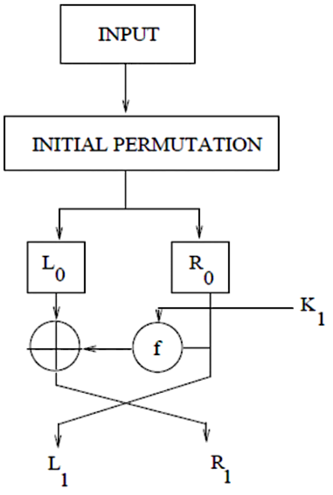


Figure 1

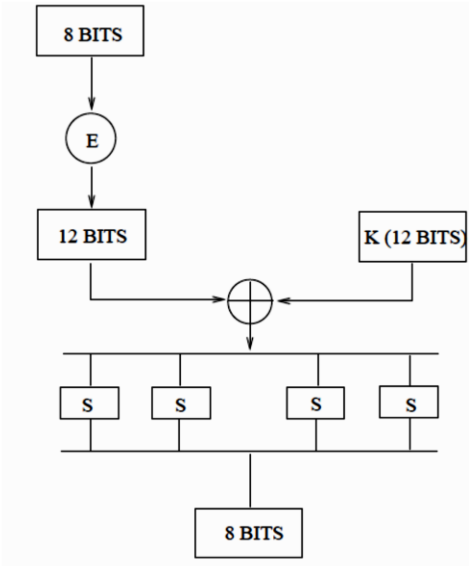
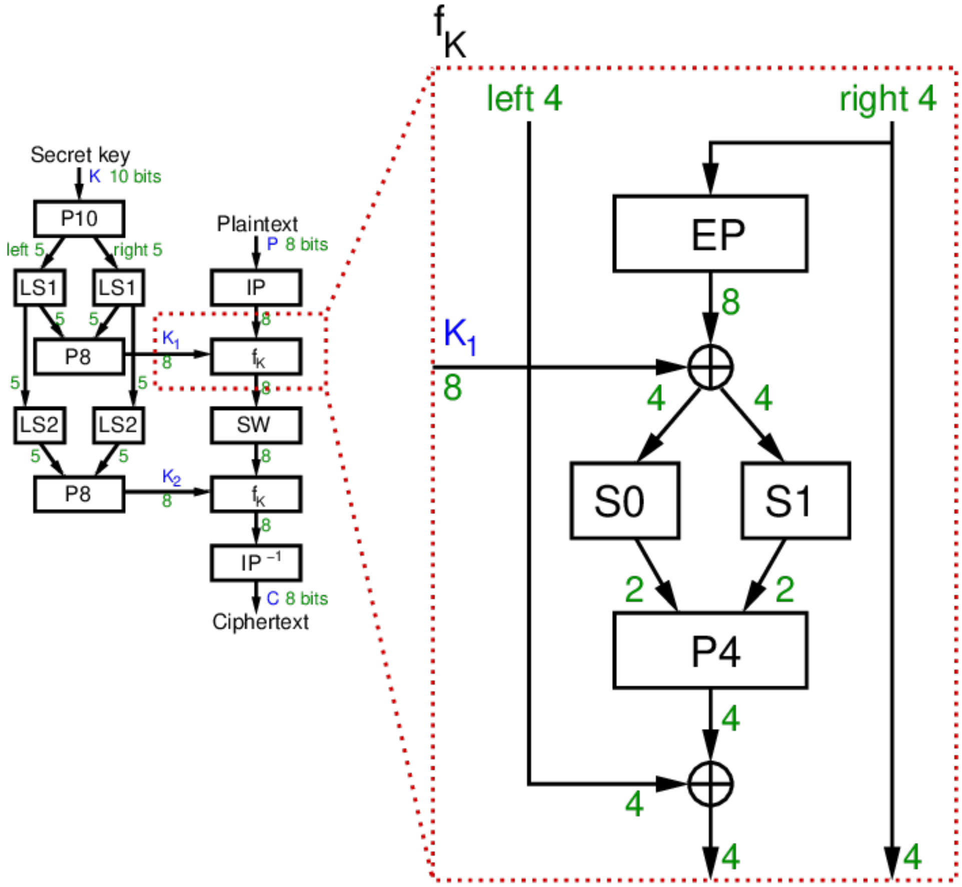


Figure 2

Exercise II - Simplified DES (S-DES)

S-DES (Simplified Data Encryption Standard) is a pedagogical block cipher used to illustrate the principles of DES. It operates on 8-bit blocks using a 10-bit key and follows a two-round Feistel structure as illustrated in the figure below.



The different permutation and substitution functions in S-DES are listed in the table below

Permutation	Values
P10	3 5 2 7 4 10 1 9 8 6
P8	6 3 7 4 8 5 10 9
P4	2 4 3 1
IP	2 6 3 1 4 8 5 7
IP^{-1}	4 1 3 5 7 2 8 6
E/P	4 1 2 3 2 3 4 1

S0

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

S1

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

The substitution boxes take four-bit input to produce 2-bit outputs as follows:
4-bit input: $bit_1, bit_2, bit_3, bit_4$
$bit_1 bit_4$ specifies row (0, 1, 2 or 3 in decimal)
$bit_2 bit_3$ specifies column

Question: Encrypt the plaintext 11010111 using the key 1010000010