Question:

Given a block $(87)_{16}$ in simplified DES (S-DES) and a key k_1 $(16)_{16}$ Find the ciphertext for the next round (simple iteration).

$$S0 = \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \qquad S1 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix}$$

IP:

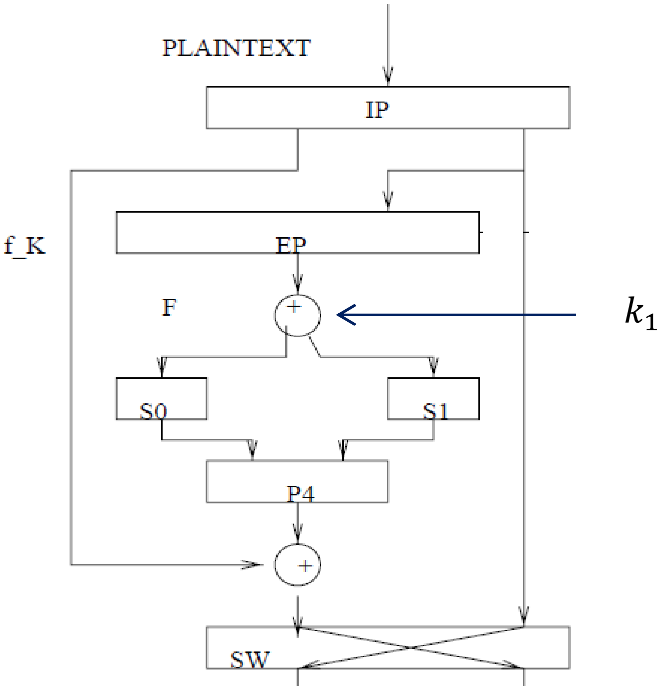
2	6	3	1	4	8	5	7
1	2	3	4	5	6	7	8

EP:

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

P4:

2	4	3	1
1	2	3	4



Answer:

First of all, the hexadecimal values of the plaintext and k_1 should be converted into binary. Also in this example there is no need to do the step of "Round keys generation", because already k_1 is given the question, and the question asks to implement Round 1 only.

$(\mathbf{87})_{16} = (\mathbf{10000111})_2$

$(\mathbf{16})_{16} = (\mathbf{00010110})_{16}$

Plaintext: 10000111

IP: 01010101

R-half: 0101

L-half: 0101

EP: 10101010 (deployed on R-half)

XOR: 10111100 (EP XOR k_1, which represents substitution)

S0: 1011 (left half of XOR deployed on S-Box 0)

row = 11 (decimal 3)

column = 01 (decimal 1)

output = 01

S1: 1100 (right half of XOR deployed on S-Box 1)

row = 10 (decimal 2)

column = 10 (decimal 2)

output = 01

S0S1: 0101

P4: 1100 (deployed on S0S1)

XOR: 1001 (P4 XOR L-half)

Result: 10010101 (XOR + R-half)

SW: 01011001 (swapping the two halves of Result)