Reem Sayes
1220827

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**