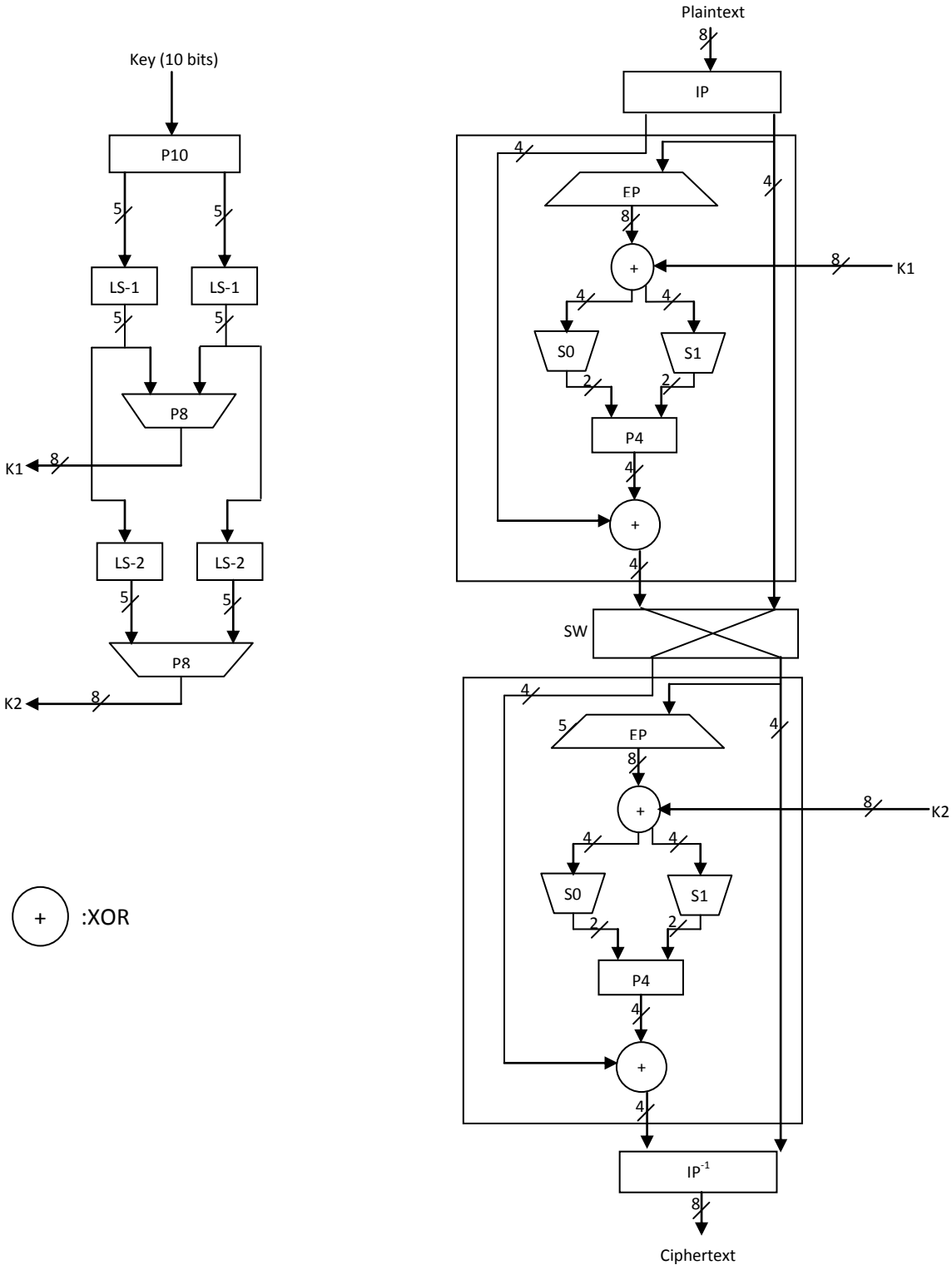

Key (10 bits)
P10
5
5
LS-1
LS-1
5
5
P8
K1
8
LS-2
LS-2
5
5
P8
K2
8
+ :XOR
Plaintext
8
IP
4
FP
4
8
+
8
K1
4
4
S0
S1
2
2
P4
4
+
4
SW
4
5
FP
4
8
+
8
K2
4
4
S0
S1
2
2
P4
4
+
4
IP-1
8
Ciphertext

IP(b0, b1, b2, b3, b4, b5, b6, b7) = (b1, b5, b2, b0, b3, b7, b4, b6)

IP^{-1}(b0, b1, b2, b3, b4, b5, b6, b7) = (b3, b0, b2, b4, b6, b1, b7, b5)

EP(b0, b1, b2, b3) = (b3, b0, b1, b2, b1, b2, b3, b0)

P4(b0, b1, b2, b3) = (b1, b3, b2, b0)

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

S0 and S1 get 4 bits and deliver 2 bits.

For example: S0(1101) = $S0_{11,01}$ = $S0_{3,1}$ = 1 = 01

P10(b0 , b1, b2, b3, b4, b5, b6, b7, b8, b9) = (b2, b4, b1, b6, b3, b9, b0, b8, b7, b5)

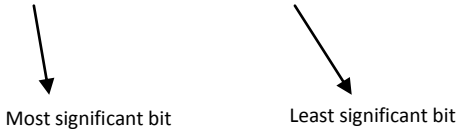
P8(b0, b1, b2, b3, b4, b5, b6, b7, b8, b9) = (b5, b2, b6, b3, b7, b4, b9, b8)

LS-1 = Rotate Left – 1 bit

LS-2 = Rotate Left – 2 bits

Important:

b0 b1 b2 b3 b4 b5 b6 b7



Example:

K = 10100 00010

P10 10000 01100

LS-1 00001 11000 -> P8 -> K1 = 1010 0100

LS-2 00100 00011 -> P8 -> K2 = 0100 0011