Mission 6 **Name:**___________________________________

You are attacking an SDES system (3 rounds) using differential cryptanalysis.

You encrypt the plaintext P=[0,0,0,0,1,1,1,1,1,0,1,1] and get the ciphertext C=[0,1,0,0,1,1,1,1,1,1,0,0]. In Particular you have L_3 = [0,1,0,0,1,1] and R_3=[1,1,1,1,0,0].

In order to attack the system, you also use several different values for a second plaintext, P*. The values of the plaintext, along with the ciphertext and the corresponding values of the xor of the inputs to the sboxes, $(E(L_3)\oplus E(L^*_3))$ and the outputs $((R_3\oplus R^*_3)\oplus(L_0\oplus L^*_0))$ are given. Use this information to determine the value of $K_{3.}$

First alternate plaintext:

P* = [1,0,0,1,1,0,1,1,1,0,1,1]

$(E(L_3)\oplus E(L^*_3))$ = [1,1,1,0,1,0,0,1]

$((R_3\oplus R^*_3)\oplus(L_0\oplus L^*_0))$ = [1,0,0,1,0,1]

Possible values of input to Sbox 1 (From L_0):

Possible values of input to Sbox 2 (From L_0):

Second alternate plaintext:

P* = [0,1,0,1,1,1,1,1,1,0,1,1]

$(E(L_3)\oplus E(L^*_3))$ = [1,0,0,0,0,0,1,1]

$((R_3\oplus R^*_3)\oplus(L_0\oplus L^*_0))$ = [0,1,1,0,1,1]

Possible values of input to Sbox 1 (From L_0):

Possible values of input to Sbox 2 (From L_0):

Third alternate plaintext:

P* = [0,1,1,0,1,1,1,1,1,0,1,1]

$(E(L_3)\oplus E(L^*_3))$ = [1,1,0,1,0,1,0,1]

$((R_3\oplus R^*_3)\oplus(L_0\oplus L^*_0))$ = [1,1,0,1,1,1]

Possible values of input to Sbox 1 (From L_0):

Possible values of input to Sbox 2 (From L_0):

Based on this info, we conclude that the input to the Sboxes when encrypting the original plaintext was: (Concatenate the only remaining values for the input to Sbox 1 and 2 above.)

Input=______________________________

We can now recover the value of K_3 by xoring this string with the value of $E(L_3)$:

$E(L_3)$:_________________________________

⊕ Input:_________________________________

= K3 :_________________________________