Mission 6 **Name:**__________________________________

Use the CoCalc code for SDES to do the following problems. Make sure to show all of your work in the CoCalc assignment, as it will be collected as well

Part 1: Use a meet in the middle attack to recover the two keys K_1 and K_2 used in an implementation of 2SDES (Double encryption with SDES) using **4 rounds**. (Refer to the handout on CoCalc)

First you encrypt P=[0,1,0,1,0,1,0,1,0,1,0,1] and get C=[0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0].

a. Use a brute force attack to find all possible values of K_1 and K_2. How many seconds does it take?

b. Use the Meet-In-The-Middle attack to find the same information. Are they the same as the ones you found by brute force?

c. How many seconds did this take?

d. How many encryptions does each method require? (In other words, how many total calls to SDES are used in each method?) How many times faster would you expect a meet in the middle attack to be in this situation? (Recall, the SDES keys have 9 bits **not** 56 bits like DES...)

Now you find that encrypting P*=[0, 0, 1, 0, 0, 1, 0, 0,1, 0, 0, 1] with the same keys produces the ciphertext C*=[1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0].

e. Repeat the meet in the middle attack, and compare the pairs of keys you got using P and C to obtain the binary values of K_1 and K_2:

f. Use the int2bin function to convert these numbers back into binary and record them here:

K_1=____

K_2=____

Part 2: Modes of Operation To encrypt P=[0,0,0,0,0,1,0,1,0,0,1,1,1,0,0,1,0,1,1,1,0,1,1,1] (which has 24 bits) with SDES, using the key K=[0,1,0,1,1,1,0,1,1] we break P into the two blocks P_1=[0,0,0,0,0,1,0,1,0,0,1,1] and P_2=[1,0,0,1,0,1,1,1,0,1,1,1]. Now, use the SDES code in CoCalc encrypt these blocks using each mode of operation discussed in class.

Electronic Codebook (ECB)

$C_1 = E(P_1) =$ ____

$C_2 = E(P_2) =$ ____

Cipher Block Chaining (CBC) use C_0=[0,1,0,1,0,1,0,1,0,1,0,1]

$P_1 \oplus C_0 =$ ____

$C_1 = E(P_1 \oplus C_0) =$ ____

$P_2 \oplus C_1 =$ ____

$C_2 = E(P_2 \oplus C_1) =$ ____

Cipher Feedback (CFB) use C_0=[0,1,0,1,0,1,0,1,0,1,0,1]

$E(C_0)=$ ____

$C_1 = P_1 \oplus E(C_0) =$ ____

$E(C_1)=$ ____

$C_2 = P_2 \oplus E(C_1) =$ ____

Output Feedback (OFB) use O_0=[0,1,0,1,0,1,0,1,0,1,0,1]

$E(O_0)=$ ____

$C_1 = P_1 \oplus E(O_0) =$ ____

$E(O_1)=$ ____

$C_2 = P_2 \oplus E(O_1) =$ ____

Counter (CTR) use X_1=[0,0,0,0,0,0,0,0,0,0,0,1]

$E(X_1) =$ ____

$C_1 = P_1 \oplus E(X_1) =$ ____

$X_2 = X_1 + 1 =$ ____

$E(X_2) =$ ____

$C_2 = P_2 \oplus E(X_2) =$ ____