Use the Sage code demonstrated in class to attack an SDES system. Do all of your work in the Mission 6 CoCalc Assignment files. (They will be collected as well.)

Part 1: Use differential cryptanalysis to attack SDES (3 rounds).
You encrypt the plaintext $\mathrm{P}=[0,0,0,0,1,1,1,1,1,0,1,1]$ and get the ciphertext $\mathrm{C}=[0,1,0,0,1,1,1,1,1,1,0,0]$.
In particular $\mathrm{L}_{3}=[0,1,0,0,1,1]$ and $\mathrm{R}_{3}=[1,1,1,1,0,0]$.
In order to attack the system, you also use several values for a second plaintext, $\mathrm{P}^{*}$. The values of the plaintext, along with the ciphertext and the corresponding values of the xor of the inputs to the sboxes, $\left(\mathrm{E}\left(\mathrm{L}_{3}\right) \oplus \mathrm{E}\left(\mathrm{L}^{*}{ }_{3}\right)\right)$ and the outputs $\left(\left(\mathrm{R}_{3} \oplus \mathrm{R}_{3}{ }^{*}\right) \oplus\left(\mathrm{L}_{0} \oplus \mathrm{~L}_{0}{ }^{*}\right)\right)$ are given. Determine the value of $\mathrm{K}_{3}$.
First alternate plaintext: $\mathrm{P}^{*}=[1,0,0,1,1,0,1,1,1,0,1,1]$
$\left(\mathrm{E}\left(\mathrm{L}_{3}\right) \oplus \mathrm{E}\left(\mathrm{L}_{3}^{*}\right)\right)=[1,1,1,0,1,0,0,1] \quad\left(\left(\mathrm{R}_{3} \oplus \mathrm{R}_{3}^{*}\right) \oplus\left(\mathrm{L}_{0} \oplus \mathrm{~L}_{0}{ }^{*}\right)\right)=[1,0,0,1,0,1]$
Possible values of input to Sbox 1 (From $\mathrm{L}_{0}$ ):

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

Second alternate plaintext: $\mathrm{P}^{*}=[0,1,0,1,1,1,1,1,1,0,1,1]$
$\left(\mathrm{E}\left(\mathrm{L}_{3}\right) \oplus \mathrm{E}\left(\mathrm{L}^{*} 3\right)\right)=[1,0,0,0,0,0,1,1]$ $\left(\left(\mathrm{R}_{3} \oplus \mathrm{R}^{*}{ }_{3}\right) \oplus\left(\mathrm{L}_{0} \oplus \mathrm{~L}_{0}{ }^{*}\right)\right)=[0,1,1,0,1,1]$
Possible values of input to Sbox 1 (From Lo):

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

Third alternate plaintext: $\mathrm{P}^{*}=[0,1,1,0,1,1,1,1,1,0,1,1]$
$\left(\mathrm{E}\left(\mathrm{L}_{3}\right) \oplus \mathrm{E}\left(\mathrm{L}_{3}^{*}\right)\right)=[1,1,0,1,0,1,0,1] \quad\left(\left(\mathrm{R}_{3} \oplus \mathrm{R}_{3}^{*}\right) \oplus\left(\mathrm{L}_{0} \oplus \mathrm{~L}_{0}{ }^{*}\right)\right)=[1,1,0,1,1,1]$
Possible values of input to Sbox 1 (From $\mathrm{L}_{0}$ ):

Possible values of input to Sbox $2\left(\right.$ From $\left.\mathrm{L}_{0}\right)$ :

Conclude that the input to the Sboxes from the original plaintext was:
Input= $\qquad$ (Concatenate the remaining values for the input to Sbox 1 and 2.)

We can now recover the value of $K_{3}$ by xoring this string with the value of $E\left(L_{3}\right)$ :
$\mathrm{E}\left(\mathrm{L}_{3}\right)$ : $\qquad$ $\oplus$ Input: $\qquad$ $=\mathrm{K} 3$ : $\qquad$

Part 2: Use a meet in the middle attack to recover the two keys $\mathrm{K}_{1}$ and $\mathrm{K}_{2}$ used in an implementation of 2SDES (Double encryption with SDES) using 4 rounds.

First you encrypt $\mathrm{P}=[0,1,0,1,0,1,0,1,0,1,0,1]$ and get $\mathrm{C}=[0,1,0,1,1,1,1,0,0,1,1,0]$.
a. Use a brute force attack to find all possible values of $\mathrm{K}_{1}$ and $\mathrm{K}_{2}$. 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. Explain briefly why this was so much faster. How many encryptions are required in total when doing brute force? How many encryptions/decryptions are required when performing a meet in the middle attack? (Recall, the keys have 9 bits...) How many times faster would you expect meet in the middle to be?

Now you find that encrypting $\mathrm{P}^{*}=[0,0,1,0,0,1,0,0,1,0,0,1]$ 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 $\mathrm{K}_{1}$ and $\mathrm{K}_{2}$ :
f. Use the int2bin function to convert these numbers back into binary and record them here:
$\mathrm{K}_{1}=$ $\qquad$
$\mathrm{K}_{2}=$ $\qquad$

