Cryptography Project 3

INSTRUCTIONS: You may use any computer language or mathematical software for this project.

Consider the simple substitution permutation network shown in Figure 1 on the second page. Assume that the S-box is as given below:

input	000	001	010	011	100	101	110	111
ouput	110	101	001	000	011	010	111	100

In terms of hexadecimal notation, the S-box is given by

input	0	1	2	3	4	5	6	7
ouput	6	5	1	0	3	2	7	4

1. Create the normalized linear approximation table for the given S-box similar to the table given in the slide 18 of sec4.3 class notes.

   Remark: Your input sum and output sum should be from 0 to 7 in hexadecimal notation. So your table should be an 8×8 table and the formula for the entries are $N_L(a, b) - 4$.

2. Find a linear approximation trail with nonzero bias, analogous to slides 22 of section 4.3 in class notes, which relates the plaintext bits P1, P2, P4, and P5 to the bit $H1$. You should sketch the trail and attach as a pdf file.

3. What is the **total bias** of the linear approximation trail you found?

   Note: Remember that $n = 4$ for the original SPN discussed in the class notes. Therefore for each input sum a and the output sum b, the bias was calculated by the formula

   $$\epsilon(a, b) = \frac{N_L(a, b)}{2^n} - \frac{1}{2} = \frac{N_L(a, b)}{16} - \frac{1}{2} = \frac{N_L(a, b) - 8}{16}.$$

   But $n = 3$ for the Simple SPN given in this project, and so

   $$\epsilon(a, b) = \frac{N_L(a, b)}{2^n} - \frac{1}{2} = \frac{N_L(a, b)}{8} - \frac{1}{2} = \frac{N_L(a, b) - 4}{8}.$$

4. Suppose you are given the following known plaintext and ciphertext pairs for this cipher, all encrypted with the same (unknown) key:

Plaintext	Ciphertext
100111	100100
000111	110010
001100	111001
011000	011101
001000	001101
011010	101001

   Using the linear approximation trail from part (2), determine the first and third bits of the subkey K_4.

   Remark: This problem has been specifically constructed so that a very small number of plaintexts and ciphertexts is sufficient to determine two subkey bits.

5. Why is this information insufficient to determine the second bit of the subkey K_4?.

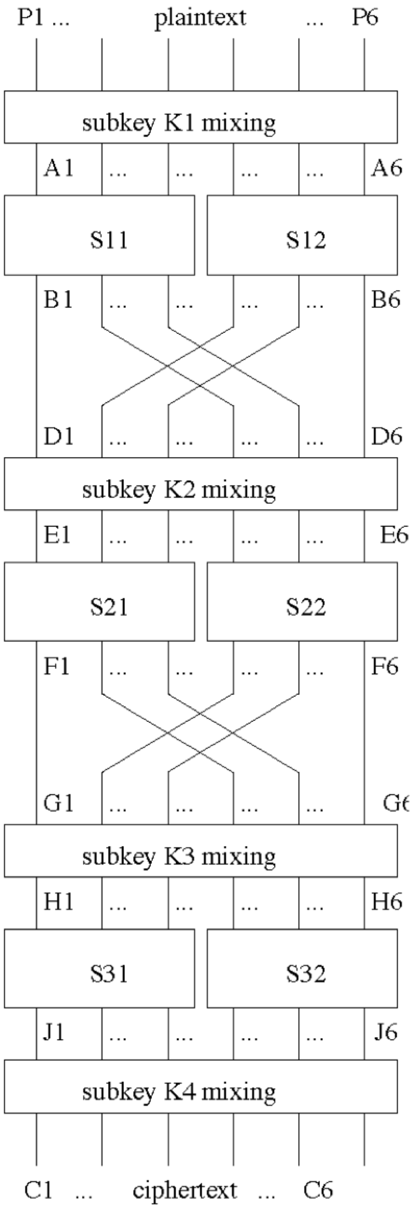

Figure 1: A very simple SPN network