Problem Set 5

INSTRUCTIONS: These are additional problems for you to practice and improve your skill in this area. DO NOT turn in your solution for these problems for grading. These problems are only to test yourself and solutions for these problems will not be posted.

1. Let M be the Multiplicative Cipher and S be the Shift Cipher. For the encryption rule $e_{(7,12)}$ in $M \times S$, find the corresponding encryption rule in $S \times M$.

2. Let S_1 and S_2 be the standard Vigenere and Permutation ciphers, respectively, with the block length of each is $m = 4$ and so $\mathcal{P} = (\mathbb{Z}_{26})^4$. Consider the product cipher $S_1 \times S_2$. Letting the Vigenere keyword $k_1 =$ `bead`, and the index permutation key k_2 is given by

1	2	3	4
4	1	3	2

   (a) Find the encryption $e_{(k_1,k_2)}(\texttt{hack})$ in $S_1 \times S_2$.

   (b) Find the encryption $e_{(k_2,k_1)}(\texttt{hack})$ in $S_2 \times S_1$.

   (c) Find a Vigenere keyword k_1' and a permutation k_2' such that

$$e_{(k_1,k_2)}(x) = e_{(k_2',k_1')}(x)$$

   for all $x \in \mathcal{P}$. That is, find a key (k_2', k_1') for $S_2 \times S_1$ that is equivalent to the key (k_1, k_2) for $S_1 \times S_2$.

   (d) Do the ciphers S_1 and S_2 commute with each other?

3. Consider the SPN discussed in class with the given round keys.

   (a) Find the encryption of the plaintext 16FD.

   (b) Find the decryption of the ciphertext 16FD

4. Consider a very simple substitution permutation network shown in Figure 1 on the next page at the end of this homework problems set. 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

   Find the encryption of the plaintext "100101", using the key

$$(K1, K2, K3, K4) = (010101, 001011, 111000, 111110).$$

   You should also show the intermediate results (i.e., the rows A, B, D, E, F, G, H, and J from Figure 1).

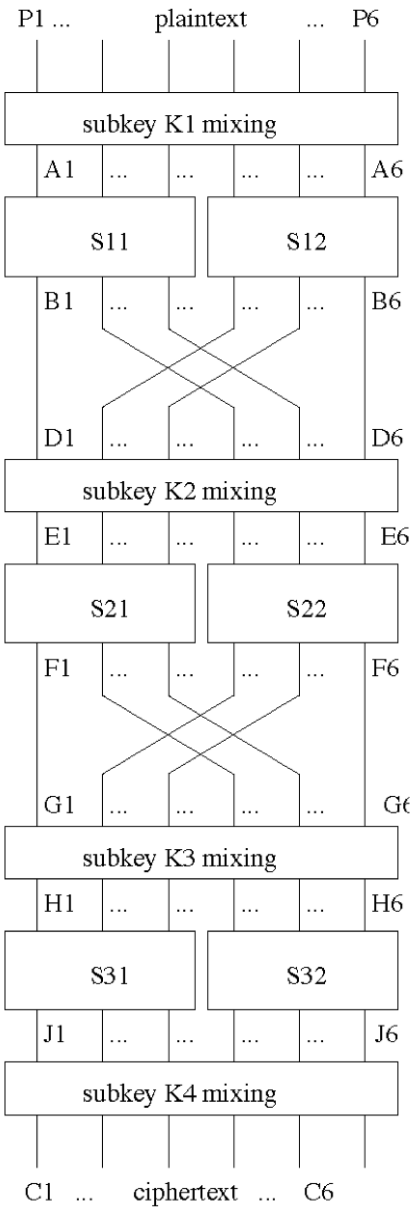

Figure 1: A very simple SPN network