UNIVERSITY *of* WASHINGTON | BOTHELL

SCHOOL OF STEM

Computing & Software Systems

CSS 337 Secure Systems

Assignment 1

Due date: Monday 4 Feb

Given the following S-Boxes:

```
S1= [   15      10      2       5

        8       4       11      6

        1       0       14      7

        9       3       12      13      ];


S2= [   4       0       10      15

        9       8       7       13

        5        1      6       11

        2       3       14      12      ];
```

Implement the following 16 bit cipher:

Plain text: *P* = [*a1 a2 a3 a4*] where *a1..a4* are 4 bits each

Key: *K* = [*k1 k2 k3 k4*] where *k1..k4* are 4 bits each

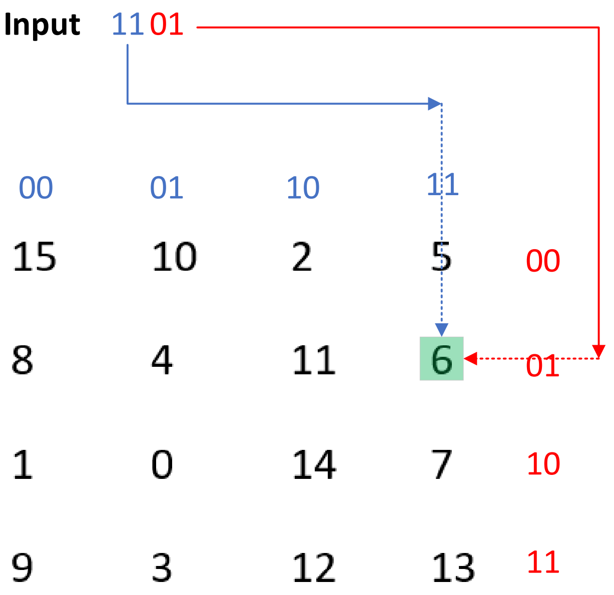
Cipher text: $C = E(p) = [\ S1(a2 \oplus k1)\ \ S2(a4 \oplus k3)\ S1(a1 \oplus k2)\ \ S2(a3 \oplus k4)\ \ ]$

Example: *P = [1000 1100 1101 0110], K = [0001 0011 0010 1111]*

C = [S1(1101) S2(0100) S1(1011) S2(0010] = [*6 0 12 5*]

= [0110 0000 1100 0101]

Example calculating *S1(1101)*:



Input 1101

00	01	10	11	
15	10	2	5	00
8	4	11	6	01
1	0	14	7	10
9	3	12	13	11

Output 6 or 0110

1. Draw a chart showing the relation between P, K, and C according to this cipher. [10%]
2. Implement the above cipher and calculate the cipher texts for the plaintexts provided in Appendix I and the keys provided in Appendix II. [40%].
3. Measure the avalanche effect for the encryption algorithm using the provided plaintexts. [30%]

   To calculate the avalanche effect:

   a. For a given input, change 1 bit in the key and calculate the number of bits changed in the resulted cipher text.
   b. Repeat (a) for the provided 5 plaintexts and 2 keys. This represents a total of 160 rounds (5 x 2 x 16).
   c. Calculate the average avalanche effect. It can be calculated as:
      (The sum of the number of bits changed in each round) / (5 x 2 x 16 x 16)
4. Suggest a change to the encryption algorithm to enhance the avalanche effect. Repeat (3) using the enhanced algorithm and comment on your findings. [20%]

Appendix I: Test Plain Texts

1111 0101 0110 0110

0010 1001 1100 0010

0101 1100 1110 0010

1110 0111 1100 0011

0011 1110 1111 0010

Appendix II: Test Keys

1110 1010 0011 1000

1011 1101 1000 0001