UNIVERSITY of WASHINGTON
BOTHELL

CSS 527 Cryptography

Assignment 1

Due date: Jan 27

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 15 10
8 9 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]

1. Draw a chart showing the relation between P, C, and K according to this cipher [5%].
2. Implement the above cipher and calculate the cipher text for the plaintext provided in Appendix I using the two keys provided in Appendix II. [30%]
3. Measure the avalanche effect for the encryption algorithm using the provided plaintexts and keys. Change 1 bit in the input and calculate the percentage of how many bits are changed in the cipher text. Repeat this for the provided 10 plaintext inputs; this will give 10 x 16 x 2 rounds. Calculate the average avalanche effect. [50%]
4. Suggest a change to the encryption algorithm to enhance the avalanche effect. Repeat 3 and comment on your findings. [15%]

Appendix I: Test Plain Text

1001 0100 0110 0110

0010 1001 1100 0010

0101 1100 1110 0010

1001 1100 0010 0111

1011 1101 1101 1111

0001 1101 0001 0011

1110 0001 1100 0011

0011 1110 0000 0010

0101 0011 1101 1011

1100 0010 0111 0100

Appendix II: Test Keys

1010 0010 0011 1010

1110 1111 0001 1000