Cryptography Assignment - 8

Pramod Aravind Byakod

Question 1:

Suppose that a Hill cipher with alphabet {0,1}and block length 3 is used to encrypt messages. And suppose that we discover three plaintext- cipher text pairs: (100)→(101),(110)→(110),(111)→(001). Recover the encryption key.

Assuming we have,

W = [a1 b1 c1
a2 b2 c2
a3 b3 c3]

C = [1 1 0
0 1 0
1 0 1]

We have equations as following:

W*[1 0 0]' = [1 0 1]

W*[1 1 0]' = [1 1 0]

W*[1 1 1]' = [0 0 1]

So a1=1, b1=0, c1=1, a2=0, b2=1, c2=1; a3=1, b3=1, c3=1

A = [1 0 1
0 1 1
1 1 1]

Question 2:

Explain why in the AES S-box, the hexadecimal number0x93is substituted by0xdc. Please show step-by-step calculations.

93 can be represented in binary as: 10010011

Using extended Euclidean Algorithm:
x^8+x^4+x^3+x+1=x*(x^7+x^4+x+1) + (x^5+x^4+x^3+x^2+1)
x^7+x^4+x+1=(x+x^2) * (x^5+x^4+x^3+x^2+1) + (x^4+x^3+x^2+1)
x^5+x^4+x^3+x^2+1=x*(x^4+x^3+x^2+1) + (x^2+x+1)
x^4+x^3+x^2+1=x^2*(x^2+x+1) + 1
And we have:
1=(x^6+x^5+x^3+x^2+1) (x^7+x^4+x+1)+(x^5+x^4+)(x^8+x^4+x^3+x+1)
Now, calculate the inverse of x^7+x^4+x+1, using sage:

```
F2.<x>=GF(2)[]
F2_8.<x>=GF(2^8,modulus=x^8+x^4+x^3+x+1)
1/(x^7+x^4+x+1)
```

Out:
x^6 + x^5 + x^3 + x^2 + 1
The result above is the multiplicative inverse of x^7+x^4+x+1
Then using the multiplicative inverse is transformed using the following affine transformation:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

where [x7, ..., x0] is the multiplicative inverse as a vector.
Then the result is:
[0 0 1 1 1 0 1 1]’, hence in hexadecimal is 0xdc

Question 3:
Suppose the current state matrix before the AES MixColumns transformation is

[O K L A
H O M A
I L L I
N O I S]
(each letter is encoded as a byte according to the ASCII table), write a program to calculate the output state after the MixColumns transformation.

Program:

```
#include <stdio.h>
int main()
{
   unsigned char col1[4] = {'O','H','I','N'};
   unsigned char col2[4] = {'K','O','L','O'};
   unsigned char col3[4] = {'L','M','L','I'};
   unsigned char col4[4] = {'A','A','I','S'};
   unsigned char *result;
   gmix_column(col1);
   gmix_column(col2);
   gmix_column(col3);
   gmix_column(col4);
}
void gmix_column(unsigned char r[4]) {
   unsigned char a[4];
   unsigned char b[4];
   unsigned char c;
   unsigned char h;
   for (c = 0; c < 4; c++) {
      a[c] = r[c];
      h = (unsigned char)((signed char)r[c] >> 7);
      b[c] = r[c] << 1;
      b[c] ^= 0x1B & h;
   }
```

```
    r[0] = b[0] ^ a[3] ^ a[2] ^ b[1] ^ a[1];
    r[1] = b[1] ^ a[0] ^ a[3] ^ b[2] ^ a[2];
    r[2] = b[2] ^ a[1] ^ a[0] ^ b[3] ^ a[3];
    r[3] = b[3] ^ a[2] ^ a[1] ^ b[0] ^ a[0];
    printf("%c,%c,%c,%c \n",r[0],r[1],r[2],r[3]);
}
```

Output:
A,J,G,L
D,N,M,@
J,K,B,G
[,K,g,m

Transpose:
A,D,J,[
J,N,K,K
G,M,B,g
L,@,G,m