**Final Exam CMPE-553 23.01.2015 (120 min, 40 points)**

St. Name, Surname\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ St.Id#\_\_\_\_\_\_\_\_\_\_\_\_\_

**Mobiles are not allowed. Calculators may be used**

Instructor Alexander Chefranov

**Task 1. (10 points)** Decide whether multiplicative inverse of x4+2 x3+2x mod x5 + 2x3+2x2+x+1 over GF(3) exists. If exists, find it and check its correctness by multiplication. If does not exist, explain why.

A=(1,0, x5 + 2x3+2x2+x+1), B=(0,1, x4+2 x3+2x )

x5 + 2x3+2x2+x+1=(x+1)( x4+2 x3+2x)+2x+1 => Q= x+1

A=(0,1, x4+2 x3+2x ), B=(1,2x+2,2x+1)

x4+2 x3+2x=(2x3+1)( 2x+1)+2 =>Q=2x3+1

A=(1,2x+2,2x+1), B=(x3+2,2x4+2x3+x+2,2)

As far as B3 is a polynomial of degree 0,

Inverse=(2x4+2x3+x+2)\*B3-1=(2x4+2x3+x+2)\*2=x4+x3+2x+1

Check it:

(x4+x3+2x+1)( x4+2 x3+2x)=x8+2x6+x5+x4+2x3+x2+2x=(x3+2)( x5 + 2x3+2x2+x+1)+1

**Task 2. (10 points)** Calculate a value of the element (6,4) in the AES inverse S-box (Table 5.4, b; it is 8C). Show all intermediate steps of the calculation.



Hint: The S-box is constructed in the following fashion:

1. Initialize the S-box with the byte values in ascending order row by row. Thus, the value of the byte at row x, column y is {xy}
2. Map each byte in the S-box to its multiplicative inverse in the finite field GF(28) , with the irreducible polynomial ; the value {00} is mapped to itself.
3. Consider that each byte in the S-box consists of 8 bits labeled (b7,b6,b5,b4,b3,b2,b1,b0). Apply the following transformation to each bit of each byte in the S-box:

 (5.1)

where ci is the i-th bit of byte c with the value {63}. The inverse S-box is constructed by applying the inverse of the transformation in (5.1) followed by taking the multiplicative inverse in GF(28).

The inverse transformation is



where d={05}, or 0000 0101.

B=(64)=(0110 0100)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| B | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| D | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |

b0’=b2+b5+b7+d0=1+1+0+1=1

b1’=b3+b6+b0+d1=0+1+0+0=1

b2’=b4+b7+b1+d2=0+0+0+1=1

b3’=b5+b0+b2+d3=1+0+1+0=0

b4’=b6+b1+b3+d4=1+0+0+0=1

b5’=b7+b2+b4+d5=0+1+0+0=1

b6’=b0+b3+b5+d6=0+0+1+0=1

b7’=b1+b4+b6+d7=0+0+1+0=1

b’=(1111 0111)=(F7)=x7+x6+x5+x4+x2+x+1

A=(1,0,x8+x4+x3+x+1), B=(0,1, x7+x6+x5+x4+x2+x+1)

x8+x4+x3+x+1=(x+1)( x7+x6+x5+x4+x2+x+1)+x =>Q=x+1

A=(0,1, x7+x6+x5+x4+x2+x+1), B=(1, x+1, x)

x7+x6+x5+x4+x2+x+1=(x6+x5+x4+x3+x+1)x+1 => Q= x6+x5+x4+x3+x+1

A=(1, x+1, x), B=( x6+x5+x4+x3+x+1, x7+x3+x2,1)

Inverse= x7+x3+x2+1=(1000 1100)=(8C)

**Task 3. (10 points)** Assume that RSA algorithm is used with the public key (N=57, e=7), and the ciphertext is C=15. Find the plaintext M. Provide details of your work.

N=p\*q=3\*19, 

d=e-1mod36=7-1mod36=31

M=CdmodN=1531mod57=48

C=MemodN=487mod57=15

**Task 4. (10 points)** Consider the following excerption from the lecture notes:

The forward mix column transformation, called MixColumns, operates on each column individually. Each byte is mapped into a new value that is a function of all four bytes in the column. The transformation can be defined as the following matrix multiplication on State:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 02 | 03 | 01 | 01 |  | S00 | S01 | S02 | S03 |  | S00’ | S01’ | S02’ | S03’ |  |
| 01 | 02 | 03 | 01 | \* | S10 | S11 | S12 | S13 | = | S10’ | S11’ | S12’ | S13’ | (5.3) |
| 01 | 01 | 02 | 03 |  | S20 | S21 | S22 | S23 |  | S20’ | S21’ | S22’ | S23’ |  |
| 03 | 01 | 01 | 02 |  | S30 | S31 | S32 | S33 |  | S30’ | S31’ | S32’ | S33’ |  |

Each element in the product matrix is the sum of products of elements of one row and one column. In this case, multiplications and additions are performed in GF(28).

The following is the example of MixColumns;

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 87 | F2 | 4D | 97 |  | 47 | 40 | A3 | 4C |
| 6E | 4C | 90 | EC | => | 37 | D4 | 70 | 9F |
| 46 | E7 | 4A | C3 |  | 94 | E4 | 3A | 42 |
| A6 | 8C | D8 | 95 |  | ED | A5 | A6 | BC |

Prove that actually S20’=94. Show you calculations

S20’=(01)S00+(01)S10+(02)S20+(03)S30=(01)(87)+(01)(6E)+(02)(46)+(03)(A6)=(87)+(6E)+ (02)(46)+(03)(A6)

(02)(46)=(0000 0010)(0100 0110)=x(x6+x2+x)= x7+x3+x2=(1000 1100)=(8C)

(03)(A6)=(0000 0011)(1010 0110)=(x+1)(x7+x5+x2+x)=x8+x7+x6+x5+x3+x=1\*( x8+x4+x3+x+1)+ x7+x6+x5+x4+1=(1111 0001)=(F1)

S20’=87+6E+8C+F1=(1000 0111)+(0110 1110)+(1000 1100)+(1111 0001)=(1001 0100)=(94)

+