**QUIZ CMPE-553 21.01.2015 (120 min, 3 points)**

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

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

Instructor Alexander Chefranov

**Task 1. (0.6 points)** Decide whether x3+x+2 is reducible over GF(3). Give necessary explanations.

Consider all combinations of the first degree polynomials (second degree are not considered as complementing the first order ones to degree 3)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| X^2 | 0 | 0 | 0 | 0 | 0 | 0 |
| X | 1 | 1 | 1 | 2 | 2 | 2 |
| 1 | 0 | 1 | 2 | 0 | 1 | 2 |

Combinations 010 and 020 are excluded since the polynomial is not divisible by x

x3+x+2=( x2+2x+2)(x+1), the polynomial is reducible

**Task 2. (0.6 points)** Decide whether multiplicative inverse of x4+ x+1 mod x5+ x3+x+1 over GF(2) exists. If exists, find it and check its correctness by multiplication. If does not exist, explain why.

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

x5+ x3+x+1=(x4+ x+1)x+ x3+ x2+1 =>q= x

T=A-qB=(1, x, x3+ x2+1)

A=(0,1,x4+ x+1)

B=(1, x, x3+ x2+1)

x4+ x+1=( x3+ x2+1)( x+1)+ x2 =>q= x+1

T=A-qB=( x+1,x2+x+1,x2)

A=(1, x, x3+ x2+1)

B=( x+1,x2+x+1,x2)

x3+ x2+1= x2(x+1)+1 =>q=x+1

T=A-qB=(x2,x+ x3+x2+x+ x2+x+1,1)= (x2, x3 +x+1,1)

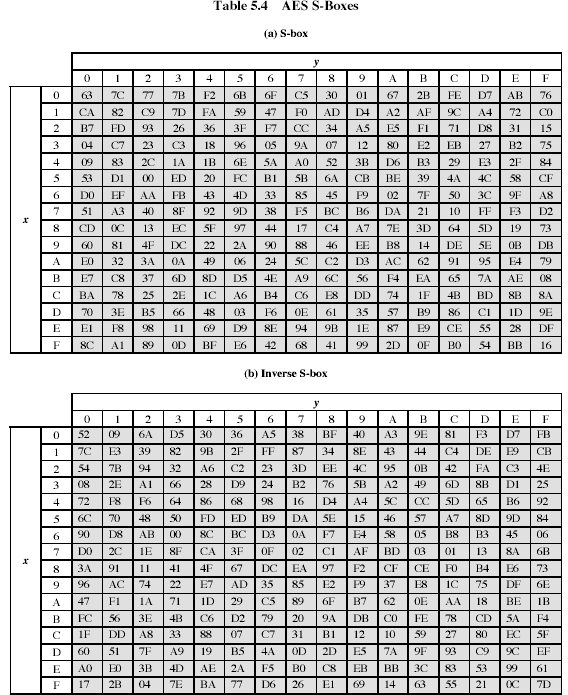
As far as T3=1, multiplicative inverse is x3 +x+1

Check its correctness:

(x4+ x+1)( x3 +x+1)=x7+x4+x3+x5+x2+x+x4+x+1= x7 +x5+x3 +x2 +1

x7 +x5+x3 +x2 +1= (x5+ x3+x+1)x2+1=1mod(x5+ x3+x+1), hence the result is correct

**Task 3. (0.6 points)** Calculate a value of the element (3,7) in the AES S-box (Table 5.4, a; it is 9A). 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}

~~Inverse of (36) is =(01100110)=(66). Applying (5.1) to the binary vector (01100110), we get (00000101)=(05).~~

(37)=(0011 0111)=x5+x4+x2+x+1, calculate its inverse

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

X8+x4+x3+x+1=(x5+x4+x2+x+1)(x3+x2+x)+x4+1=>q= x3+x2+x

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

x5+x4+x2+x+1=( x4+1)(x+1)+x2 =>q=x+1

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

x4+ 1= x2\* x2+1 =>q=x2

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

Inverse is x6 +x=(0100 0010)=b

Let’s check its correctness:

(x6 + x)( x5+x4+x2+x+1)= x11+x6 + x10+x5+x8+ x3+x7 + x2+x6+x= x11 +x10 + x8+x7 +x5+ x3+x2+x

x11 +x10 + x8+x7 +x5+ x3+x2+x = (x8+x4 +x3+ x+1)(x3+ x2+1)+1=1mod(x8+x4 +x3+ x+1)

Now

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| b | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| C | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 |

According to (5.1)

b0’=b0+b4+b5+b6+b7+c0=0+0+0+1+0+1=0

b1’=b1+b5+b6+b7+b0+c1=1+0+1+0+0+1=1

b2’=b2+b6+b7+b0+b1+c1=0+1+0+0+1+0=0

b3’=b3+b7+b0+b1+b2+c3=0+0+0+1+0+0=1

b4’=b4+b0+b1+b2+b3+c4=0+0+1+0+0+0=1

b5’=b5+b1+b2+b3+b2+c5=0+1+0+0+0+1=0

b6’=b6+b2+b3+b4+b5+c6=1+0+0+0+0+1=0

b7’=b7+b3+b4+b5+b6+c7=0+0+0+0+1+0=1

Hence b’=(1001 1010) =(9A) complying with the S-box contents

**Task 4. (0.6 points)** Assume that p=3, q=19. Encrypt and decrypt message M=5 using RSA

N=pq=57, =36

Let e=5, then d=e-1mod36=29

C=Memod57=55mod57=47

M=Cdmod57=4729mod57=5

472mod57=43

474mod57=25

478mod57=55

4716mod57=4

4729mod57=4716+8+4+1mod57=(4\*55)\*(25\*47)mod57=49\*35mod57=5

**Task 5. (0.6 points)** Find a primitive root for q=17. Use it to generate a common key K by Diffie-Hellman key exchange algorithm assuming XA=5, XB=11.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| α\n | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 2 | 2 | 4 | 8 | 16 | 15 | 13 | 9 | 1 |  |  |  |  |  |  |  |  |
| 3 | 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 | 14 | 8 | 7 | 4 | 12 | 2 | 6 | 1 |

Thus, the primitive root α=3

Xa=3 Xb=4

Ya=33mod17=10, Yb=34mod17=13

K=YaXbmod17=104mod17=4=YbXamod17=133mod17=4