**Final Exam CMPE-553 04.01.2025 (120 min, 45 points)**

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

**Mobiles are not allowed. Three cheat sheets with your own handwritings and calculators can be used**

Instructor Alexander Chefranov

**7 questions, 12 pages**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Task** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **Total** |
| **Point** | **5** | **5** | **5** | **8** | **8** | **7** | **7** | **45** |
| **Grade** |  |  |  |  |  |  |  |  |

**Task 1. (5 points)** Encrypt the plaintext “plain” by the Hill cipher and decrypt it back for the key matrix and the plaintext alphabet having 26 English letters. Check correctness of the inverse matrix by multiplication. Show details of your calculations, explain your answer.

Hints:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

C=EK(P)=KP mod 26

P= DK(C)=K-1C mod 26 = K-1KP = P

where C and P are column vectors of length n, representing the plaintext and ciphertext, K is nxn matrix, representing the encryption key, and K-1 is inverse of K.



 (1)

where - is a determinant of sub matrix of A, obtained by deletion of i-th row and j-th column, det(A) – determinant of A. Taking into account that we work with integers on modulo n, we rewrite (1):

 (2)

Let , then

det(A) =40+84+96-105-64-48=220-217=3, and

From (2):



















Thus, we get



and



EXTENDED EUCLID(m,b)

1. (A1,A2,A3):=(1,0,m); (B1,B2,B3):=(0,1,b);
2. if B3=0 return A3=gcd(m,b); no inverse
3. if B3=1 return B3 = gcd(m,b); B2= b-1 mod m
4. Q=
5. (T1,T2,T3):=(A1-QB1, A2-QB2, A3-QB3)
6. (A1,A2,A3):= (B1,B2,B3)
7. (B1,B2,B3):= (T1,T2,T3)
8. goto 2

Solution

D=detK=4-1=3

D^(-1) mod 26=9; check it: 3\*9 mod 26 = 27 mod 26 =1

It can be found EEA:

A=(1,0,26), B=(0,1,3)

Q=floor(26/3)=8

T=A-Q\*B=(1-8\*0,0-8\*1, 26-8\*3)=(1,-8,2)

A=(0,1,3), B=(1,-8,2)

Q=floor(3/2)=1

T=A-Q\*B = (0-1\*1, 1-1\*(-8), 3-1\*2)=(-1, 9,1)

A=(1,-8,2), B=(-1,9,1)

B3=1=>B2=9=3^(-1) mod 26 =D^(-1)

Check correctness of it:

 , i.e. it is correct.

Pad the plaintext by x: “plainx”= (15, 11, 0, 8, 13, 23)

Encryption:

 =”ah”

 =”ig”

 =”kb”

Thus, C=”ahigkb”.

Decryption:

 =”pl”

 =”ai”

 =”nx”

Thus, the plaintext restored is “plainx”, equal to the original plaintext.

**Task 2. (5 points)** Assuming that the 48-bit round key K1 is 0x CDECF4CDEFE5, and R0=0x67812545, calculate 4-bit output of the S-box S1. Show details of your calculations, explain your answer

Hints:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |

|  |
| --- |
| Expansion/Permutation (E table) |
| 32 | 1 2 3 4 | 5 |
| 4 | 5 6 7 8 | 9 |
| 8 | 9 10 11 12 | 13 |
| 12 | 13 14 15 16 | 17 |
| 16 | 17 18 19 20  | 21 |
| 20 | 21 22 23 24 | 25 |
| 24 | 25 26 27 28 | 29 |
| 28 | 29 30 31 32 | 1 |

 |
|  |
| S1 |

Solution:

Expanded R0=0110 0111 1000 0001 0010 0101 0100 0101 is

|  |
| --- |
| Expansion/Permutation of R0 |
| 1 | 0110 | 0 |
| 0 | 0111 | 1 |
| 1 | 1000 | 0 |
| 0 | 0001 | 0 |
| 1 | 0010  | 0 |
| 0 | 0101 | 0 |
| 1 | 0100 | 0 |
| 0 | 0101 | 0 |

The first 6 bits of XORing of expanded R0 and K1 is

101100

XOR

110011

=

011111

which are used as an input to S1 with 01=1 defining its row and 1111 = 15 defining its column. On the cross row 1 and column 15 there is 8, which is output by S1 as a 1-bit entity: 1000.

**Task 3. (5 points)** Apply Inverse Shift Row transformation to the state array below:

|  |  |  |  |
| --- | --- | --- | --- |
| 83 | F2 | 4D | 97 |
| ED | 6E | 4C | 90 |
| 4B | C8 | 47 | E9 |
| 8C | D8 | 9E | AC |

Explain your answer

Hints:

**Shift Row Transformation (Cont 1)**

The 1st row (number 0) is not altered, row number i is shifted left by i-byte circular left shift, i=1, 2, 3. The following is the example of such shift:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 87 | F2 | 4D | 97 |  | 87 | F2 | 4D | 97 |
| EC | 6E | 4C | 90 | => | 6E | 4C | 90 | EC |
| 4A | C3 | 46 | E7 |  | 46 | E7 | 4A | C3 |
| 8C | D8 | 95 | A6 |  | A6 | 8C | D8 | 95 |

The inverse shift row transformation, called InvShiftRows, performs the right circular shift of i-th row by i bytes, i=0,1,2,3.

Shift row transformation ensures that the 4 bytes of one column are spread out to four different columns (Fig. 5.3 illustrates this effect).

Solution:

i-th row is shifted I positions right circularly

|  |  |  |  |
| --- | --- | --- | --- |
| 83 | F2 | 4D | 97 |
| 90 | ED | 6E | 4C |
| 47 | E9 | 4B | C8 |
| D8 | 9E | AC | 8C |

**Task 4. (8 points)** The AES state array (shown below left) is transformed by the MixColumn transformation to the state shown below right:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

Applying the InverseMixColumn transformation prove that restored state array element in row 3, column 2 shall actually be E7.

Show details of your calculations, explain your answer

Hints:

AES uses arithmetic in the finite field GF(28), with the irreducible polynomial .

The inverse mix column transformation, called InvMixColumns, is defined by the following matrix multiplication:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0E | 0B | 0D | 09 |  | S00 | S01 | S02 | S03 |  | S00’ | S01’ | S02’ | S03’ |  |
| 09 | 0E | 0B | 0D | \* | S10 | S11 | S12 | S13 | = | S10’ | S11’ | S12’ | S13’ | (5.5) |
| 0D | 09 | 0E | 0B |  | S20 | S21 | S22 | S23 |  | S20’ | S21’ | S22’ | S23’ |  |
| 0B | 0D | 09 | 0E |  | S30 | S31 | S32 | S33 |  | S30’ | S31’ | S32’ | S33’ |  |

E7 shall be calculated by multiplication of the row 3 of the inverse mix column matrix (0d 09 0e 0b) by the 2nd column of the state array (40 d4 e4 a5):

0d\*40+09\*d4+0e\*e4+0b\*a5

1. 0d\*40=(0000 1101)\*(0100 0000)=(x^3+x^2+1)\*x^6=x^9+x^8+x^6 mod x^8+x^4+x^3+x+1 = X^6+x^5+x^3+x^2+1 =01101101=6d

|  |  |  |
| --- | --- | --- |
| Dividend | divisor | Quotient |
| x^9+x^8+x^6+x^9+x^5+x^4+x^2+x= | x^8+x^4+x^3+x+1 | X+1 |
| X^8+x^6+x^5+x^4+x^2+x+x^8+x^4+x^3+x+1= |  |  |
| X^6+x^5+x^3+x^2+1 |  |  |

1. 09\*d4=(0000 1001)\*(1101 0100)=(x^3+1)\*(x^7+x^6+x^4+x^2)= x^10+x^9+x^7+x^5+ x^7+x^6+x^4+x^2= x^10+x^9+x^6+x^5+x^4+x^2 mod x^8+x^4+x^3+x+1 = X^5+x^3+x^2+x = (00101110)=2e

|  |  |  |
| --- | --- | --- |
| Dividend | divisor | Quotient |
| x^10+x^9+x^6+x^5+x^4+x^2+x^10+x^6+x^5+x^3+x^2= | x^8+x^4+x^3+x+1 | X^2+x |
| X^9+x^4+x^3+x^9+x^5+x^4+x^2+x= |  |  |
| X^5+x^3+x^2+x |  |  |

1. 0e\*e4=(00001110)\*(11100100)=(x^3+x^2+x)\*(x^7+x^6+x^5+x^2)= x^10+x^9+x^8+x^5+x^9+x^8+x^7+x^4+ x^8+x^7+x^6+x^3= x^10+ x^8+x^6+x^5+x^4+x^3 mod x^8+x^4+x^3+x+1 = X^3+x^2+x+1 =(0000 1111) = 0F

|  |  |  |
| --- | --- | --- |
| Dividend | divisor | Quotient |
| x^10+ x^8+x^6+x^5+x^4+x^3+x^10+x^6+x^5+x^3+x^2= | x^8+x^4+x^3+x+1 | X^2+1 |
| X^8+x^4+x^2+x^8+x^4+x^3+x+1= |  |  |
| X^3+x^2++x+1 |  |  |

1. 0b\*a5 = (0000 1011)\*(10100101)=(x^3+x+1)\*(x^7+x^5+x^2+1)= x^10+x^8+x^5+x^3+ x^8+x^6+x^3+x+ x^7+x^5+x^2+1 = x^10+ x^7+x^6+x^2+x+1 mod x^8+x^4+x^3+x+1 = X^7+x^5+x^3+x+1=(10101011) = ab

|  |  |  |
| --- | --- | --- |
| Dividend | divisor | Quotient |
| x^10+ x^7+x^6+x^2+x+1+x^10+x^6+x^5+x^3+x^2= | x^8+x^4+x^3+x+1 | X^2+ |
| X^7+x^5+x^3+x+1 |  |  |

6d+2e+0f+ab=

01101101

+

00101110

+

00001111

+

10101011

=

11100111 = e7

**Task 5. (8 points)** Assuming modulus , define , RSA keys, and encrypt and decrypt back the plaintext, P=123. Show details of your calculations, explain them.

Hints:

|  |  |
| --- | --- |
|  |  |

Solution

N=143==11\*13=p\*q=>p=11, q=13

Fi(N)=(p-1)\*(q-1)=10\*12=120

Let e=7, then d=7^(-1) mod 120 = 103

Let’s find it by Extended Euclid algorithm:

A=(1,0,120), B=(0,1,7)

Q=floor(120/7)=17

T=A-Q\*B=(1-17\*0,0-17\*1, 120-17\*7)=(1,-17,1)

A=(0,1,7) B=(1,-17,1)

B3=1 =>B2=-17 mod 120 =103 =d

Check correctness of d: e\*d mod 120 = 7\*103 mod 120 = 721 mod 120 = 6^120+1 mod 120 = 1

Encryption:

C=P^e mod N = 123^7 mod 143 = (-20)^7 mod 143 = -20^7 mod 143 =7

Calculate it:

20^2 mod 143 = 400 mod 143 = 2\*143+114 mod 143 = 114

20^4 mod 143 = 114^2 mod 143 = 29^2 mod 143 = 841 mod 143 = 5\*143+126 mod 143 = 126 = -17

123^7 mod 143 =-20^4\*20^2\*20 mod 143 = 17\*114\*20 mod 143 = - 17\*29\*20 mod 143 = -340\*29 mod 143 =-54\*29 mod 143 = -9\*6\*29 mod 143 = -9\*174 mod 143 = -9\*31 mod 143 = -279 mod 143 = - 136 mod 143 =7

P’=C^d mod N = 7^103 mod 143

7^2=49

7^4=49^2 mod 143 = 343\*7 mod 143 = 57\*7 mod 143 = 3\*19\*7 mod 143 = 3\*133 mod 143 = -30 mod 143

7^8 = 30^2 mod 143 = 15^2\*4 mod 143 = 225\*4 mod 143 = 82\*4 mod 143 = 328 mod 143 = 42

7^16 = 42^2 mod 143 =441\*4 mod 143 = 12\*4 = 48

7^32 = 48^2 mod 143 = 144\*16 mod 143 = 16

7^64 = 16^2 mod 143 = 256 mod 143 = 113

7^103= 7^64\*7^32\*7^4\*7^2\*7 mod 143 = 113\*16\*113\*49\*7 mod 143 = 30^2\*16\*49\*7 mod 143 =42\*16\*49\*7 mod 143 = 168\*4\*49\*7 mod 143 = 25\*4\*49\*7 mod 143 = 100\*49\*7 mod 143 = -43\*7\*49 mod 143 = -301\*49 mod 143 = -15\*49 mod 143 = -15\*7\*7 mod 143 = -105\*7 mod 143 = 38\*7 mod 143 = 266 mod 143 = 123 = P.

Thus decryption returns back the original plaintext.

**Task 6. (7 points)** Use Diffie-Hellman to exchange keys between Alice and Bob assuming that . Show details of your calculations, explain them.

Hints:



Solution:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| X | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 2^x mod 29 | 2 | 4 | 8 | 16 | 3 | 6 | 12 | 24 | 19 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| X | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 2^x mod 29 | 9 | 18 | 7 | 14 | 28 | 27 | 25 | 21 | 13 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| X | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 2^x mod 29 | 28 | 23 | 17 | 5 | 10 | 20 | 11 | 22 | 15 |

|  |  |
| --- | --- |
| X | 28 |
| 2^x mod 29 | 1 |

 Let g=2, XA=2, XB=3

Then YA=g^XA mod q = 2^2 mod 29 = 4, YB= g^XB mod q = 2^3 mod 29 = 8

K=YA^XB mod q = 4^3 mod 29 = 6

K=YB^XA mod q = 8^2 mod 29 = 6

**Task 7. (7 points)** Consider SHA-512 round below





Assume input register values of a,b,,c,d,e,f,g,h are as below



What are the output register values of b,c,d,f,g, and h? Show details of your calculations, explain them.

Solution:

According to the scheme of a round, the new values of the registers b,c,d,f, g, and h are just copies of the old values of the registers a,b,c, e, f, and g, respectively, i.e. they are b’=a=6a09…; c’=b=BB67.., d’=c=3C6E…, f’=e = 510E.., g’=f=9B05.., h’=g=1F83…