**QUIZ CMPE-553 25.11.2022 (90 min, 2 points)**

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

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

Instructor Alexander Chefranov

**3 questions, 8 pages**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Task** | **1** | **2** | **3** | **Total** |
| **Point** | **0.7** | **0.6** | **0.7** | **2** |
|  |  |  |  |  |

**Task 1. (0.7 points)** Encrypt the plaintext “text” by Hill cipher, and decrypt back the ciphertext obtained. The key matrix is $K=\left[\begin{matrix}1&2\\1&3\end{matrix}\right]$. Use the following encoding

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

Show intermediate calculations, explain you answer

Hint: C=KP mod 26

P=K-1C mod 26

 mod n

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

Ciphertext of “TE”=[19 4[:

$$\left[\begin{matrix}1&2\\1&3\end{matrix}\right]\left[\begin{array}{c}19\\4\end{array}\right]=\left[\begin{array}{c}19+8\\19+12\end{array}\right] mod 26=\left[\begin{array}{c}1\\5\end{array}\right]="B F"$$

“X T”=[23 19]

$$\left[\begin{matrix}1&2\\1&3\end{matrix}\right]\left[\begin{array}{c}23\\19\end{array}\right]=\left[\begin{array}{c}23+38\\23+57\end{array}\right] mod 26=\left[\begin{array}{c}9\\2\end{array}\right]="J C"$$

Thus, ciphertext is “BFJC”

Inverse matrix calculation: det(K)=3-2=1

$$K^{-1}=\left[\begin{matrix}3&-2\\-1&1\end{matrix}\right]$$

Check its correctness:

$$K^{-1}K=\left[\begin{matrix}3&-2\\-1&1\end{matrix}\right]\left[\begin{matrix}1&2\\1&3\end{matrix}\right]=\left[\begin{matrix}3-2&6-6\\-1+1&-2+3\end{matrix}\right]=\left[\begin{matrix}1&0\\0&1\end{matrix}\right]$$

Decryption:

Plaintext for “B F:

$$\left[\begin{matrix}3&-2\\-1&1\end{matrix}\right]\left[\begin{array}{c}1\\5\end{array}\right]=\left[\begin{array}{c}3-10\\-1+5\end{array}\right] mod 26=\left[\begin{array}{c}-7\\4\end{array}\right]mod26=\left[\begin{array}{c}19\\4\end{array}\right]="T E"$$

Plaintext for “J C”

$$\left[\begin{matrix}3&-2\\-1&1\end{matrix}\right]\left[\begin{array}{c}9\\2\end{array}\right]=\left[\begin{array}{c}27-4\\-9+2\end{array}\right] mod 26=\left[\begin{array}{c}23\\-7\end{array}\right]mod26=\left[\begin{array}{c}23\\19\end{array}\right]="X T"$$

Plaintext restored is “TEXT”

**Task 2. (0.6 points)** Calculate a value of S-box S3 output if the result of XOR inside the function F is 0x123321456654. Show intermediate calculations, explain you answer

Solution:

In binary 0x123321456654 is

0001 0010 0011 0011 0010 0001 0100 0101 0110 0110 0101 0100

S3 input is bits in positions 13-18:

001100

Two end bits, 00, define row number 0, and four middle bits, 0110, define column number 6. On the cross of row=0 and column=6 is value 15, in binary 1111 that is the output of S3.

Hints:

.

**Task 3. (0.7 points)** Calculate result of MixColumn transformation of the he state array S just for, S’(1,2), in the numerical example below that shall be equal to {70}. Show your intermediate calculations and explain them.

Hints:

**Mix Column Transformation**

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 (Fig. 5.5b):

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

As was mentioned in Chapter 4, AES uses arithmetic in the finite field GF(28), with the irreducible polynomial .

Solution:

S’(1,2)=(01 02 03 01)\*(4d 90 4a d8)={4d}+{02}\*{90}+{03}\*{4a}+{d8}={4d}+{3B}+{DE}+{d8}=

0100 1101+

0011 1011+

1101 1110+

1101 1000=

0111 0000={70} as expected

{02}\*{90}={0000 0010}\*{1001 0000}=x\*(x^7+x^4)=x^8+x^5 mod x^8+x^4+x^3+x+1=x^5+x^4+x^3+x+1=(0011 1011)={3B}

{03}\*{4a}=(0000 0011)\*(0100 1010)=(x+1)\*(x^6+x^3+x)=x^7+x^4+x^2+x^6+x^3+x= x^7+x^6+x^4+x^3+x^2+x=(1101 1110)={D E}