**MT Exam CMPE-553 14.11.2024 (90 min, 30 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, 6 pages**

**Task 1. (10 points)** Encrypt the plaintext “text” by the Hill cipher **(5 points)** and decrypt it back **(5 points)** for the key matrix $K=\left(\begin{matrix}1&1\\2&3\end{matrix}\right)$ 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

From (2):



















Thus, we get



and



Solution:

“text”=(19 4 23 19) $=(P\_{1} P\_{2})$;

$C\_{1}=KP\_{1}=\left(\begin{matrix}1&1\\2&3\end{matrix}\right)\left(\begin{matrix}19\\4\end{matrix}\right) mod 26=\left(\begin{matrix}19+4\\38+12\end{matrix}\right) mod 26=\left(\begin{matrix}23\\50\end{matrix}\right) mod 26=\left(\begin{matrix}23\\24\end{matrix}\right)="xy"$

$$C\_{2}=KP\_{2}=\left(\begin{matrix}1&1\\2&3\end{matrix}\right)\left(\begin{matrix}23\\19\end{matrix}\right) mod 26=\left(\begin{matrix}23+19\\46+57\end{matrix}\right) mod 26=\left(\begin{matrix}42\\103\end{matrix}\right) mod 26=\left(\begin{matrix}16\\25\end{matrix}\right)="qz"$$

C=”xyqz”

$detK=1\*3-1\*2=1$, 

, $K\_{12}^{-1}=\left(-1\right)^{1+2}D\_{21}=-1 $, $K\_{21}^{-1}=\left(-1\right)^{2+1}D\_{12}=-2 $, $K\_{22}^{-1}=\left(-1\right)^{2+2}D\_{22}=1 $, hence $K^{-1}=\left(\begin{matrix}3&-1\\-2&1\end{matrix}\right)$. Check correctness of $K^{-1}$:

$$K^{-1}\*K mod 26=\left(\begin{matrix}3&-1\\-2&1\end{matrix}\right)\left(\begin{matrix}1&1\\2&3\end{matrix}\right) mod 26=$$

$$ \left(\begin{matrix}3\*1-1\*2&3\*1-1\*3\\-2\*1+1\*2&-2\*1+1\*3\end{matrix}\right) mod 26= \left(\begin{matrix}1&0\\0&1\end{matrix}\right) mod 26= \left(\begin{matrix}1&0\\0&1\end{matrix}\right)$$

Since a unity matrix is obtained, our calculation of $K^{-1}$ is correct.

Decryption: $P^{'}=K^{-1}C mod 26$, $P\_{1}^{'}=K^{-1}C\_{1}mod 26=\left(\begin{matrix}3&-1\\-2&1\end{matrix}\right)\left(\begin{matrix}23\\24\end{matrix}\right) mod 26= \left(\begin{matrix}3\*23-1\*24\\-2\*23+1\*24\end{matrix}\right) mod 26= \left(\begin{matrix}69-24\\-46+24\end{matrix}\right) mod 26= \left(\begin{matrix}45\\-22\end{matrix}\right) mod 26=\left(\begin{matrix}19\\4\end{matrix}\right)="te"=P\_{1}$

$$P\_{2}^{'}=K^{-1}C\_{2}mod 26=\left(\begin{matrix}3&-1\\-2&1\end{matrix}\right)\left(\begin{matrix}16\\25\end{matrix}\right) mod 26= \left(\begin{matrix}3\*16-1\*25\\-2\*16+1\*25\end{matrix}\right) mod 26= \left(\begin{matrix}48-25\\-32+25\end{matrix}\right) mod 26= \left(\begin{matrix}23\\-7\end{matrix}\right) mod 26=\left(\begin{matrix}23\\19\end{matrix}\right)="xt"=P\_{2}$$

Thus, $P^{'}="text"=P$. Hence, decryption is made correctly.

**Task 2. (10 points)** Assuming that the 48-bit round key K1 is 0x1CDEFF1CDEFF, and R0=0x12345678, 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 |

The first 6 bits of Expansion/Permutation(R0) according to E table are R0(32,1,2,3,4,5)=000010. Then:

$$K\_{1}\left(1:6\right)=000111$$

$$⊕$$

$$R\_{0}\left(32,1,2,3,4,5\right)=000010$$

$$= 000101$$

The first 6 bits used as input to S1 are 000100, they define row 01=1, and column 0010=2. The output of S1(1,2) is 7 that is “0111” in binary.

**Task 3. (10 points)** Given the AES 128-bit plaintext P=0x123456789abcdef0123456789abcdef0

and the 128-bit round key

w[0,3]=0x23456789abcdef0123456789abcdef01,

calculate the first 16 bits of the results of the following transformations:

1. **(5 points)** Add round key (first 16 bits):

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 |

1. **(5 points)** Substitute bytes (first 16 bits):

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |

Show details of your calculations, explain your answer

Hints:







Solution:

1. Apply add round key to P(1:16):

P(1:16)+w[0,3](1:16)=0x1234+0x2345=

0001 0010 0011 0100 +

0010 0011 0100 0101 =

0011 0001 0111 0001

1. Apply Substitute byte to P(1:16)=0x1234

S(0x12)=0x93 = 1001 0011; S(0x34)=0x18 = 0001 1000