**QUIZ CMPE-553 10.01.2023 (110 min, 3 points)**

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

**Mobiles are not allowed. Calculators are allowed. Five cheat sheets with your own handwritings can be used. Good Luck!**

Instructor Alexander Chefranov

**7 questions, 13 pages**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Task** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **Total** |
| **Max Point** | **0.3** | **0.3** | **0.4** | **0.5** | **0.5** | **0.5** | **0.5** | **3** |
| **Grade** |  |  |  |  |  |  |  |  |

**Task 1. (0.3 points)** Encrypt the plaintext “plain” by Hill cipher, and decrypt back the ciphertext obtained. The key matrix is $K=\left[\begin{matrix}1&3\\2&5\end{matrix}\right]$. 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 your calculations, give explanations

Hints: 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

Encryption: P1=(P L)=(15 11), $C1=\left(\begin{array}{c}1\\2\end{array} \begin{array}{c}3\\5\end{array}\right)\left(\begin{array}{c}15\\11\end{array}\right) mod 26=\left(\begin{array}{c}15+33\\30+55\end{array}\right)=\left(\begin{array}{c}48\\85\end{array}\right)mod26=\left(\begin{array}{c}22\\7\end{array}\right)$=

(W H)

P2=(A I)=(0 8), $C2=\left(\begin{array}{c}1\\2\end{array} \begin{array}{c}3\\5\end{array}\right)\left(\begin{array}{c}0\\8\end{array}\right) mod 26=\left(\begin{array}{c}0+24\\0+40\end{array}\right)mod26=\left(\begin{array}{c}24\\14\end{array}\right)$=(Y O)

Since the last block is not full, pad it by X

P3=(N X)=(13 23), $C3=\left(\begin{array}{c}1\\2\end{array} \begin{array}{c}3\\5\end{array}\right)\left(\begin{array}{c}13\\23\end{array}\right) mod 26=\left(\begin{array}{c}13+69\\26+115\end{array}\right)mod26=\left(\begin{array}{c}82\\141\end{array}\right)mod26=\left(\begin{array}{c}4\\11\end{array}\right)$=(E L)

Thus, ciphertext C=(C1C2C3)=(WHYOEL)

Decryption: Inverse matrix $detK=5-6=-1; K^{-1}=-\left(\begin{matrix}5&-3\\-2&1\end{matrix}\right)=\left(\begin{matrix}-5&3\\2&-1\end{matrix}\right)$. Check it: $K^{-1}∙K=\left(\begin{matrix}-5&3\\2&-1\end{matrix}\right)\left(\begin{matrix}1&3\\2&5\end{matrix}\right)=\left(\begin{matrix}-5+6&-15+15\\2-2&6-1\end{matrix}\right)=\left(\begin{matrix}1&0\\0&1\end{matrix}\right)$

$P1’=K^{-1}∙C1=\left(\begin{matrix}-5&3\\2&-1\end{matrix}\right)\left(\begin{array}{c}22\\7\end{array}\right)mod26=\left(\begin{array}{c}-110+21\\44-7\end{array}\right)mod26=\left(\begin{array}{c}-89\\37\end{array}\right)mod26=\left(\begin{array}{c}-11\\11\end{array}\right)mod26=\left(\begin{array}{c}15\\11\end{array}\right)$=(P L)=P1

$P2’=K^{-1}∙C2=\left(\begin{matrix}-5&3\\2&-1\end{matrix}\right)\left(\begin{array}{c}24\\14\end{array}\right)mod26=\left(\begin{array}{c}-120+42\\48-14\end{array}\right)mod26=\left(\begin{array}{c}-78\\34\end{array}\right)mod26=\left(\begin{array}{c}0\\8\end{array}\right)mod26$=(A I)=P2

$P3’=K^{-1}∙C3=\left(\begin{matrix}-5&3\\2&-1\end{matrix}\right)\left(\begin{array}{c}4\\11\end{array}\right)mod26=\left(\begin{array}{c}-20+33\\8-11\end{array}\right)mod26=\left(\begin{array}{c}13\\-3\end{array}\right)mod26=\left(\begin{array}{c}13\\23\end{array}\right)$=(N X)=P3

Thus, plaintext revealed is P’=(PLAINX).

**Task 2. (0.3 points)** Calculate a value of S-box S4 output if the result of XOR inside the function F (see Fig. 3.9 below) is 0x5267129abcde~~ff~~. Show intermediate calculations, explain you answer

Hints:

|  |
| --- |
|  |
|  |

0x5267129abcde=0101 0010 0110 0111 0001 0010 1001 1010 1011 1100 1101 1110=

010100 100110 011100 010010 100110 101011 110011 011110

Input to S4 is 010010, end bits are 00=0, middle bits are 1001 =9, hence S4 output is on the cross of row 0 and column 9, that is 2=0010.

**Task 3. (0.4 points)** Calculate result of MixColumn transformation of the ~~he~~ state array S just for, S’(2,2), in the numerical example below that shall be equal to {3A}. Show your calculations, give explanations

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 .

S22’=({01} {01} {02} {03})\*({4d} {90} {4a} {d8})={4d}+{90}+{02}\*{4a}+{03}\*{d8}

{02}\*{4a}=(0000 0010)\*(0100 1010) = x\*(x^6+x^3+x)=x^7+x^4+x^2=(1001 0100)={94}

{03}\*{d8}=(0000 0011)\*(1101 1000)=(x+1)\*(x^7+x^6+x^4+x^3)= x^8+x^7+x^5+x^4+ x^7+x^6+x^4+x^3= x^8+x^6+x^5+x^3 mod x^8+x^4+x^3+x+1= x^6+x^5+x^4+x+1=(0111 0011)={73}

{4d}+{90}+{02}\*{4a}+{03}\*{d8}={4d}+{90}+{94}+{73}=

=0100 1101+

 1001 0000+

 1001 0100+

 0111 0011=0011 1010 = {3a} as expected.

**Task 4 (0.5 points)**. Given AES master key as 0x0123456789abcdef0011223344556677, what is w[2] of the expanded key? Show your calculations, give explanations

Hint:

KeyExpansion(byte key[16], word w[44]){

 Word temp;

 For(i=0;i<4;i++) w[i]=(key[4\*i], key[4\*i+1], key[4\*i+2], key[4\*i+3]);

 For(i=4;i<44;i++){

 Temp=w[i-1];

 If(I mod 4 = 0) temp = SubWord(RotWord(temp)) XOR Rcon[i/4];

 W[i]=w[i-4] XOR temp;

 }

}

Word w[2]= (key[4\*2], key[4\*2+1], key[4\*2+2], key[4\*2+3])=0x00112233

**Task 5 (0.5 points)**. Using RSA, define keys, and encrypt and decrypt back the message M=3, if N=33. When encrypting/decrypting, use squaring with modulo reduction: (M^(2n)) mod N = ((M^n mod N)^2) mod N, and exponent binary decomposition, e.g,, M^23=M^16\*M^4\*M^2\*M, Show your calculations, give explanations

Hints:



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

N=33=p\*q=3\*11, fi(N)=2\*10=20, e=3, e^(-1) mod 20 = 7, actually, 3\*7 mod 20=1

Encryption: C=M^e mod N = 3^3 mod 33 = 27

Decryption: M’=C^7 mod 33 = 27^7 mod 33

27^2 mod 33= (-6)^2 mod 33 = 36 mod 33 =3

27^4 mod 33 = 3^2 mod 33 = 9

27^7 mod 33 = (27^4 mod 33\*27^2 mod 33 \* 27) mod 33 = (9\*3\*27) mod 33= 27^2 mod 33 = 3= M, thus, decryption is correct.

**Task 6 (0.5 points)**. Use Diffie-Hellman key exchange protocol to define a common key, K, for two parties, A and B, if q=11. Show your calculations, give explanations

Hints:



Take $α=2$:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| X | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| $α^{x}modq$  | 2 | 4 | 8 | 5 | 10 | 9 | 7 | 3 | 6 | 1 |

Since all numbers from 1 to 10 are obtained by exponentiation, $α$ is a primitive root.

Let Xa=2, Xb=3, then Ya=2^Xa mod 11 = 4, Yb=2^Xb mod 11 = 8

K=Ya^Xb mod 11 = 4^3 mod 11 = 64 mod 11 = 9

K=Yb^Xa mod 11 = 8^2 mod 11 = 64 mod 11 = 9

**Task 7 (0.5 points)**. Assuming a=10,b=17, and c=20 are 5-bit numbers, calculate Maj(a.b,c) used in SHA-512. Show your calculations, give explanations

Hints:



A=01010, b=10001, c=10100

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| a | 0 | 1 | 0 | 1 | 0 |
| b | 1 | 0 | 0 | 0 | 1 |
| c | 1 | 0 | 1 | 0 | 0 |
| Maj(a,b,c) | 1 | 0 | 0 | 0 | 0 |

Thus, Maj(a,b,c)=100002=16.