**Final Exam CMPE-553 16.01.2023 (110 min, 100 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, 11 pages**

**Task 1 (11 points).** Using the key matrix $K=\left[\begin{matrix}2&1\\7&3\end{matrix}\right]$, encrypt the plaintext “I am” by Hill cipher. Invert the matrix $K$, check correctness of the inverted matrix $K^{-1}$, and use it decrypt back the ciphertext obtained. Use English alphabet extended by space ‘ ‘, with 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 | 26 |

Show your calculations, give explanations

Hints: C=KP mod n

P=K-1C mod n

 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

n=27

Plaintext P1=”I “=(8 26), P2=”am”=(0 12)

$C1=K\*P1 mod 27= \left[\begin{matrix}2&1\\7&3\end{matrix}\right]\left(\begin{array}{c}8\\-1\end{array}\right)mod27=\left(\begin{array}{c}16-1\\56-3\end{array}\right)mod27=\left(\begin{array}{c}15\\26\end{array}\right)$=”P “

$C2=K\*P2 mod 27= \left[\begin{matrix}2&1\\7&3\end{matrix}\right]\left(\begin{array}{c}0\\12\end{array}\right)mod27=\left(\begin{array}{c}0+12\\0+36\end{array}\right)mod27=\left(\begin{array}{c}12\\9\end{array}\right)$=”MJ“

C=”P MJ”

$$detK=6-7=-1;K^{-1}=\left[\begin{matrix}-3&1\\7&-2\end{matrix}\right]$$

$$K∙K^{-1}=\left[\begin{matrix}2&1\\7&3\end{matrix}\right]\left[\begin{matrix}-3&1\\7&-2\end{matrix}\right]=\left[\begin{matrix}-6+7&2-2\\-21+21&7-6\end{matrix}\right]=\left[\begin{matrix}1&0\\0&1\end{matrix}\right]$$

$P1^{'}=K^{-1}\*C1 mod 27= \left[\begin{matrix}-3&1\\7&-2\end{matrix}\right]\left(\begin{array}{c}15\\-1\end{array}\right)mod27=\left(\begin{array}{c}-45-1\\105+2\end{array}\right)mod27=\left(\begin{array}{c}-46\\107\end{array}\right)mod27=\left(\begin{array}{c}-19\\26\end{array}\right)mod27=\left(\begin{array}{c}8\\26\end{array}\right)$=”I “=P1

$P2'=K^{-1}\*C2 mod 27= \left[\begin{matrix}-3&1\\7&-2\end{matrix}\right]\left(\begin{array}{c}12\\9\end{array}\right)mod27=\left(\begin{array}{c}-36+9\\84-18\end{array}\right)mod27=\left(\begin{array}{c}-27\\66\end{array}\right)mod27=\left(\begin{array}{c}0\\12\end{array}\right)$=”AM“=P2

**Task 2 (11 points).** Decide on one possible variant of the first 12 bit values of the extended to 48 bits right half input R, if round key K=0xab5267cd129e, and outputs of S1, S2 are 0101 and 1010, respectively (see Fig. 3.9 below). Show intermediate calculations, explain you answer

Hints:

|  |
| --- |
|  |
|  |

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

101010 110101 001001 100111 110011 010001 001010 011110

Input to S-boxes is I(1:48)=ER(1:48) xor K(1:48), thus ER(1:48)=I(1:48) xor K(1:48)

Output 0101=5 is in row=0=00 and column=12=1100 from S1 can be obtained if its input is I(1:6)=011000. Thus, the first six expanded R values shall be ER(1:6)=I(1:6) xor K(1:6) = 011000 xor 101010 = 110010

Output 1010=10 is in row=0=00 and column=15=1111 from S2 can be obtained if its input is I(7:12)=011110. Thus, the second six expanded R values shall be ER(7:12)=I(7:12) xor K(7:12) = 011110 xor 110101 = 101011

Thus, ER(1:12)= 110010101011

**Task 3 (11 points).** Calculate result of the InvMixColumn transformation of the state array S (shown in the numerical example below at the right hand side) just for, S’(2,1) using (5.5), that shall be equal to {E7} (shown in the left hand side of the example). 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 |

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’ |  |

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

S’(2,1)=InvMixColumn(2,1:4)\*S(1:4,1)=({0D} {09} {0E} {0B})\*({40} {D4} {E4} {A5})={0d}\*{40}+{09}\*{d4}+{0e}\*{e4}+{0b}\*{a5}

{0d}\*{40}=(00001101)\*(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

|  |  |  |
| --- | --- | --- |
| Dividend | Divisor | Quotient |
| x^9+x^8+x^6xorx^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+xxorx^8+x^4+x^3+x+1= |  |  |
| x^6+x^5+x^3+x^2+1remainder |  |  |

{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 =0010 1110

|  |  |  |
| --- | --- | --- |
| Dividend | Divisor | Quotient |
| x^10+x^9+x^6+x^5+x^4+x^2xorx^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^3xorx^9+x^5+x^4+x^2+x= |  |  |
| x^5+x^3+x^2+xremainder |  |  |

{0e}\*{e4}=(0000 1110)\*(1110 0100)=(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

|  |  |  |
| --- | --- | --- |
| Dividend | Divisor | Quotient |
| x^10+x^8+x^6+x^5+x^4+x^3xorx^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^2xorx^8+x^4+x^3+x+1= |  |  |
| x^3+x^2+x+1remainder |  |  |

{0b}\*{a5}=(0000 1011)\*(1010 0101) = (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 =1010 1011

|  |  |  |
| --- | --- | --- |
| Dividend | Divisor | Quotient |
| x^10+ x^7+x^6 +x^2+x +1xorx^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 +1remainder |  |  |

Thus

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

0110 1101 +

0010 1110 +

0000 1111+

1010 1011=

1110 0111 =E7 as expected

**Task 4 (17 points)**. What is the 3rd word of AES 9-th round if the results of the following calculations considered in Lecture notes are known?

“For example, suppose that the round key for round 8 is

EA D2 73 21 B5 8D BA D2 31 2B F5 60 7F 8D 29 2F

Then the 1st four bytes (1st column) of the round key for round 9 are calculated as follows:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| I(decimal) | temp | After RotWord | After SubWord | Rcon(9) | After XORWith Rcon | W[i-4] | W[i]=temp XOR w[i-4] |
| 36 | 7f8d292f | 8d292f7f | 5da515d2 | 1b000000 | 46a515d2 | Ead27321 | Ac7766f3 |

“. 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;

 }

}

Round 9 key is in w[36;39], the 3rd word is w[38]

According to the code above, since 37 and 38 are not divisible by 4

W[38]=w[38-1] xor w[38-4]=w[37] xor w[34]= w[37] xor 31 2B F5 60

W[37]=w[37-1] xor w[37-4]=w[36] xor w[33] = B5 8D BA D2 xor Ac7766f3

Thus, w[37]=

1011 0101 1000 1101 1011 1010 1101 0010 +

1010 1100 0111 0111 0110 0110 1111 0011 =

0001 1001 1111 1010 1101 1100 0010 0001=19 fa dc 21

W[37] xor 31 2B F5 60 =

0001 1001 1111 1010 1101 1100 0010 0001 +

0011 0001 0010 1011 1111 0101 0110 0000 =

0010 1000 1101 0001 0010 1001 0100 0001 = 28 d1 29 41

**Task 5 (17 points)**. Using RSA, define keys, and digitally sign the message P=4, if N=77 and the 3-bit hash function to be used is h(x)=(x^2+1) mod 6. Validate the digital signature obtained. 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:

Digital signature: DS=E(KR, h(M)). Digital signature validation: D(PK, DS)==h(M’), where KR, KP, M, and M’ are private and public keys, original and received messages, respectively.

|  |  |
| --- | --- |
|  | 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=p\*q=77=7\*11=>p=7, q=11, fi(N)=6\*10=60, e=7,d=e^(-1) mod 60

A=(1,0,60) B=(0,1,7)

Q=floor(60/7)=8

T=A-q\*B=(1-8\*0,0-8\*1,60-8\*7) = (1,-8,4)

A=B=(0,1,7), B=T=(1,-8,4)

Q=floor(7/4)=1

T=A-q\*B=(0-1\*1,1-1\*(-8),7-1\*4) = (-1,9,3)

A=B=(1,-8,4), B=T=(-1,9,3)

Q=floor(4/3)=1

T=A-q\*B=(1-1\*(-1),-8-1\*9,4-1\*3) = (2,-17,1)

Since T3 as new B3 is 1, B2=-17 mod 60 =43 is 7^(-1) mod 60

Check it: 43\*7 mod 60= 301 mod 60 = 5\*60+1 mod 60 = 1

H(P)= (4^2+1) mod 6 =17 mod 6 =5

Let public key is KU=43 and private key is KR=7

Then DS(P) =5^7 mod 77

5^2=25

5^4=625 mod 77 = 9

DS(P) = 5^7=5^4\*5^2\*5 mod 77 = 9\*25\*5 mod 77 = -2\*3\*5 mod 77 =-30 mod 77 =47

To validate signature, it shall be decrypted with KU:

Dec(DS, KU) = 47^43 mod 77

47^2 mod 77 =53

47^4 mod 77 = 37

47^8 mod 77 = 60

47^16 mod 77 = 58

47^32 mod 77 =53

47^43 mod 77 =47^32\*47^8\*47^2\*47 mod 77 = 53\*60\*53\*47 mod 77 =37\*60\*47 mod 77 = -3\*30\*47 mod 77 =-13\*47mod 77 = -72 mod 77 =5=h(P)

Thus, the signature is valid.

**Task 6 (17 points)**. Use Diffie-Hellman key exchange protocol to define a common key, K, for two parties, A and B, if q=13. Show your calculations, give explanations. Secret keys shall be greater than 1!

Hints:



|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| X | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 2^x | 2 | 4 | 8 | 3 | 6 | 12 | 11 | 9 | 5 | 10 | 7 | 1 |

Thus, primitive root a=2

Xa=2,Ya= 2^2 mod 13 =4

Xb=3 Yb= 2^3 mod 13 = 8

K= Ya^Xb mod 13 = 4^3 mod 13 = 64 mod 13 = 12

K=Yb^Xa mod 13 = 8^2 mod 13 = 64 mod 13 = 12

**Task 7 (16 points)**. Assuming e=45, f=5, and g=17 are 6-bit numbers, calculate Ch(e,f,g) used in SHA-512. Show your calculations, give explanations

Hints:



e= 101 101,

f= 000 101,

g= 010 001

ch(e,f,g)=010 101= 21