**Eastern Mediterranean University**

**Computer Engineering Department**

**CMSE-353 Security of Software Systems**

**Final Exam**

**Four A4 sheets of paper with your handwritings may be used for your help. Photocopies, printouts, etc. are not allowed! Calculators, telephones, and other electronic devices are not allowed**

**Duration: 130 Minutes January 12, 2024,**

**8.30**

**Std Id\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Std Name\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Instructor Alexander Chefranov**

**Totally 8 questions, 15 pages**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Task | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Total |
| Points | 7 | 8 | 9 | 9 | 17 | 17 | 17 | 16 | 100 |

[**Q1**](#Q1)[**Q2**](#Q2)[**Q3**](#Q3)[**Q4**](#Q4)[**Q5**](#Q5)[**Q6**](#Q6)[**Q7**](#Q7)[**Q8**](#Q8)

**Q1. (7 points).** What the Availability security requirement is? Explain its importance by an example

Availability requirement concerns a feature of the system to be available to authorized users in work hours according to an agreement between the system and the users. It is important for security, because if a system is not available when it is necessary controlling, e.g. a flying aircraft, it may fall down and crash together with its passengers.

[Q1](#Q1)

**Q2. (8 points).** Explain the difference between Access control lists and Capability lists by an example

Access control list (ACL) for each object specifies who and how can use it. Capability lists (CL) for each user specifies what objects and how he/she can use. For example, if we have two users, Hasan and Ahmet, and each of them can read file Data.txt, then ACL is Data.txt=>Hasan| Read => Ahmet|Read, whereas CL has two parts: Hasan=>Data.txt|Read and Ahmet=>Data.txt|Read

[Q1](#Q1)

**Q3. (9 points)**. Given DES 56-bit result of PC-1 in hexadecimal form as 0x12344321acddca, what is the result of Permuted choice 2 (PC-2) for **round 1** in binary and hexadecimal? Explain your answer.

# Hints:

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

|  |
| --- |
| Permuted Choice 2 (PC-2) |
| 14 17 11 24 1 5 3 28  15 6 21 10 23 19 12 4  26 8 16 7 27 20 13 2  41 52 31 37 47 55 30 40  51 45 33 48 44 49 39 56  34 53 46 42 50 36 29 32 |

|  |
| --- |
| Schedule of Left Shifts |
| Round number 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16  Bits rotated 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1 |

The given value 0x12344321acddca in binary is 0001 0010 0011 0100 0100 0011 0010 0001 1010 1100 1101 1101 1100 1010 that can be represented in the 8x7 matrix form as (left, below). It is round 1, hence 1 left circular shift is applied separately to the first 28 bits, and to the 2nd 28 bits (right, below)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 |  |  |  | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |  |  | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| 2 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |  |  | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 3 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |  |  | 3 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 4 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |  |  | 4 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| 5 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |  |  | 5 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 6 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |  |  | 6 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |
| 7 | 0 | 1 | 1 | 1 | 0 | 1 | 1 |  |  | 7 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |
| 8 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |  |  | 8 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |

Then the 48-bit result of PC-2 of the result of 1 left circular shift (below, left) in tabular form is shown below, right:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 |  |  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 |  | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |  | 2 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 3 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |  | 3 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 4 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |  | 4 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 |
| 5 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |  | 5 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| 6 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |  | 6 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
| 7 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |  |  |  |  |  |  |  |  |  |  |
| 8 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |  |  |  |  |  |  |  |  |  |  |

The result of PC-2 in hexadecimal form is 0x625882f95c85

[Q1](#Q1)

**Q4. (9 points).** Check that **InvMixColumn** transformation (5.5), see Hints, applied to the state array from the Lecture notes given below (in the right-hand side):

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

returns **S’(3,2)={D8} (in the left-hand side, indicated by an arrow).** Use arithmeticin GF(2^8) with irreducible polynomial m(x)=x^8+x^4+x^3+x+1. Show your calculations, give necessary explanations.

**Hints:**

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’ |  |

The value we are interested in is S’(3,2), hence, it is a product of row 3 and column 2:

These calculations shall be done in . First, calculate the products:

+

The product has the order of 10, hence, we reduce it:

|  |  |  |
| --- | --- | --- |
| Dividend | Divisor | Quotient |
| -  = |  |  |
|  |  |  |

Thus,

The product has the order of 9, hence, we reduce it:

|  |  |  |
| --- | --- | --- |
| Dividend | Divisor | Quotient |
| -  = |  |  |
|  |  |  |

Thus,

The product has the order of 8, hence, we reduce it:

|  |  |  |
| --- | --- | --- |
| Dividend | Divisor | Quotient |
| -  = |  |  |
|  |  |  |

Thus,

The product has the order of 10, hence, we reduce it:

|  |  |  |
| --- | --- | --- |
| Dividend | Divisor | Quotient |
| -  = |  |  |
| -  = |  |  |
|  |  |  |

Thus,

Now, add the products:

1001 0001

+

0000 0110

+

1111 0001

+

1011 1110

=

1101 1000 = d8, as it was expected.

[Q1](#Q1)

**Q5. (17 points).** Define keys, check their correctness, and digitally sign the message, M=4, using RSA and hash function h(x)=(3x+7) mod 11, if N=65. Use squaring, binary decomposition, and modulo reduction when encrypting (for example, 10^4 mod 13 is (10^2 mod 13)^2 mod 13 = (100 mod 13)^2 mod 13 = 9^2 mod 13= 81 mod 13= 3; 10^5 mod 13=(10^4 mod 13\*10) mod 13= 3\*10 mod 13 =30 mod 13 = 4). Show **your intermediate calculations**, give explanations

**Hints**:

# RSA algorithm

RSA (Rivest-Shamir-Adelman, 1978) algorithm is an asymmetric encryption algorithm. To design an encryption/decryption key pair, two large prime numbers, p and q, , are selected, and an integer, d, is chosen that is relatively prime to (p-1)(q-1) (d and (p-1)(q-1) have no common factors other than 1). Finally, an integer e is computed such that



One key is (e,N), and the other is (d,N), where N=p\*q, and is referred to as the modulus.

For example, we might select p=7, and q=13. Then N=91, and (p-1)(q-1)=72. We can choose d=5 (which is relatively prime to 72) and e=29, because e\*d=145 and



Then, one key is K1=(29,91) and the other is K2=(5,91). The message to be encrypted is broken into blocks such that each block, M, can be treated as an integer between 0 and (N-1). To encrypt M into the ciphertext block, B, we perform



To decrypt B, we perform



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

As far as asymmetric encryption is time consuming, some function, f, of M is computed – generally a hash – that produces a result that is considerably smaller than M itself. f(M) is also called a message digest of M. f(M) is encrypted with RC and referred to as a digital signature, which is transmitted along with M.

Thus, C sends two items, and M, to the receiver. The receiver decrypts the first item using PC and then compares the outcome with the result of applying f to the second item. If the two are the same, the receiver should be able to conclude that M could have been generated only by C.

N=65=p\*q=13\*5 => p=13, q=5

Fi(N)=(p-1)\*(q-1)=12\*4=48

Let e=5, then d=e^(-1) mod fi(N) = 5^(-1) mod 48

Use EEA to calculate d:

A=(1,0,48), B=(0,1,5)

Q=floor(A3/B3)=floor(48/5)=9

T=A-q\*B=(1-9\*0, 0-9\*1, 48-9\*5)=(1,-9,3)

A=B=(0,1,5), B=T=(1,-9,3)

Q=floor(A3/B3)=floor(5/3)=1

T=A-q\*B=(0-1\*0, 1-1\*(-9), 5-1\*3)=(-1,10,2)

A=B=(1,-9,3), B=T=(-1,10,2)

Q=floor(A3/B3)=floor(3/2)=1

T=A-q\*B=(1-1\*(-1), -9-1\*10, 3-1\*1)=(2,-19,1)

A=B=(-1,10,2), B=T=(2,-19,1)

B3=1=>b2=5^(-1) mod 48 = -19 mod 48 =29=d

Check its correctness: 5\*29 =145 mod 48 =3\*48+1 mod 48 =1, hence, it is correct.

Let e=5 is a public key, and d=29 is a private key. Digital signature is E\_d(h(M)).

H(M)=3\*4+7 mod 11 = 19 mod 11 = 8

E\_d(h(M))= 8^29 mod 65

29=16+8+4+1

8^2 = 64 mod 65 =-1 mod 65

8^4 = (-1)^2 mod 65 =1

8^8 = 1^2 mod 65 = 1

8^16 = 1^2 mod 65 = 1

Hence, 8^29 = 8^16\*8^8\*8^4\*8 mod 65 = 1\*1\*1\*8 mod 65 =8

Digital signature of M is 8.

[Q1](#Q1)

**Q6. (17 points).** For one round of SHA-512 calculate Ch(e,f,g), assuming that e=1110, f=0101, and g=1100 in binary are 4-bit entities. Show your calculations, give explanations, present results in decimal.

**Hints:**

|  |
| --- |
|  |

Applying bit-wise: Ch(e,f,g)=Ch(1110,0101,1100)=((1110)&(0101))+(not(1110)&(1100))=(0100)+((0001)&(0100))=(0100)+(0000)=(0100)

[**Q1**](#Q1)

**Q7. (17 points).** If h(x)=(7x+3) mod 19, what is the initial password pN for Lamport’s One-time password if p0=4, N=6. Show your calculations, give explanations.

Hints:

# Initialization Procedure

The client selects a password, , a number, , calculates

,

where

.

The client securely delivers to the server (, and the servers saves it into () tuple.

P6=h^6(p0)=h^6(4)

H(4)=7\*4+3 mod 19 = 31 mod 19 =12

H^2(4)=7\*12+3 mod 19 = 87 mod 19 = 11

H^3(4) = 7\*11+3 mod 19 = 80 mod 19 = 4

H^4(4) = 7\*4+3 mod 19 = 31 mod 19 =12

H^5(4) = 7\*12+3 mod = 87 mod 19 =11

H^6(4) = 7\*11 + 3 mod 19 = 80 mod 19 = 4

Hence, P6= 4.

[Q1](#Q1)

**Q8. (16 points).** Consider Fig. 5.8 from the Lecture notes below, p. 15, and answer 1-point questions below:

1. What is an IP address?

IP address is a unique computer node Internet identifier

1. How many bits does IP address use in IPv4 protocol?

32

1. Enlist all IP addresses used in Fig. 5.8.

192.168.1.1, 192.168.1.105, 192.168.1.106

1. What is a gateway?

A gateway is a node connected on one side to Internet, and on the other side to LAN

1. Is there a gateway in Fig. 5.8, and, if yes, what is its IP address?

Yes, there is a gateway, its address is 192.168.1.1

1. What is a MAC address?

MAC address is a node unique identifier used in LAN

1. How many bits does a MAC address use?

48

1. Enlist all MAC addresses used in Fig. 5.8.

00:11:22:33:44:01, 00:11:22:33:44:02, 00:11:22:33:44:03

1. What is ARP?

ARP is Address Resolution Protocol

1. What is the aim of ARP?

The aim of ARP is to relate Internet IP addresses to LAN MAC addresses

1. What is ARP cache?

ARP cache is a table of related pairs (IP, MAC)

1. What is the use of ARP cache?

ARP cache is used to relate IP and MAC addresses

1. What is poisoned ARP cache?

A poisoned ARP cache is a cache with invalid IP-MAC relations

1. How ARP cache can be poisoned?

ARP cache can be poisoned by sending fake ARP replies

1. Enlist all poisoned ARP caches in Fig. 5.8

ARP caches of Bob (left) and Alice (right)

1. Who and how poisoned ARP caches in Fig. 5.8

Eve poisoned caches of Bob and Alice sending ARP reply to Bob relating Alice’s IP address to Eve’s MAC address, and sending ARP reply to Alice relating Bob’s IP address to Eve’s MAC address

[Q1](#Q1)

