**Eastern Mediterranean University**

**Computer Engineering Department**

**CMPE-455 Security of Computer Systems and Networks**

 **Final Exam**

**Five A4 sheets of handwritten paper may be used for your help. Photocopies, printouts, etc. are not allowed! Calculators are allowed, other electronic devices are not allowed. Yardımınız için beş A4 yaprak el yazısı kağıt kullanılabilir. Fotokopi, çıktı vb. izin verilmez! Hesap makinelerine izin verilir, diğer elektronik cihazlara izin verilmez**

**Duration: 150 Minutes June 19, 2023**

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

**Instructor Alexander Chefranov**

**Totally 11 questions, 10 pages, 100 points**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Question** |  |  |  |  |  |  |  |  |  |  |  | **Total** |
| **Point** | **5** | **5** | **5** | **6** | **6** | **6** | **14** | **14** | **13** | **13** | **13** | **100** |

**Before MT Exam questions Q1-Q6 (33 points):**

**Q1.** **(5 points).** What are the two tools used to provide the availability security requirement? Kullanılabilirlik güvenlik gereksinimini sağlamak için kullanılan iki araç nelerdir?

Physical protection, redundancy

**Q2. (5 points).** Consider Bell-LaPadula model with 5 security levels: 5 güvenlik düzeyine sahip Bell-LaPadula modelini düşünün:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Label | Unclassified | Confidential | Secret | Top Secret | Top2 Secret |
| Value | 0 | 1 | 2 | 3 | 4 |

Suppose, Mr Brown has label value=3. There are 5 documents labeled as follows: Bay Brown'ın etiket değerinin = 3 olduğunu varsayalım. Aşağıdaki şekilde etiketlenmiş 5 belge vardır:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
| Document | Salary | Performance | Test results | Contractors | Losses |
| Label value | 2 | 3 | 3 | 4 | 2 |
| Mr Brown can read (Y/N) | y | y | y | n | y |
| Mr Brown can write (Y/N) | n | y | y | y | n |

For each document no=1..5, specify what document in the table above can Mr Brown read and what can write (by filling the last two rows). Give necessary explanations. 1..5 nolu her belge için yukarıdaki tabloda Mr Brown'ın hangi belgeyi okuyabildiğini ve ne yazabileceğini (son iki satırı doldurarak) belirtiniz. Gerekli açıklamaları yapın.

Hints: From Lecture notes:

“BLP model is derived from the military multilevel security paradigm (Top secret, Secret, Confidential, Unclassified)

Each document has 1 out of 4 security levels, and each user has “clearance”, also 1 out of 4.

A document of a certain level can be accessed only by users with the same or higher clearance level, “no read-up” rule.

A user can write only in the documents of his or higher level of security, “no write down” rule, ‘\*’ property.”

Mr Brown can read documents of the not higher and write into the documents of not lower level.

**Q3. (5 points).** For RSA with N=77, define its public and private keys. Explain your answer, show intermediate calculations. N=77 ile RSA için genel ve özel anahtarları bulun. Cevabınızı açıklayın, ara hesaplamaları gösterin

**Hints**:

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).

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) //T=A-Q\*B
6. (A1,A2,A3):= (B1,B2,B3)
7. (B1,B2,B3):= (T1,T2,T3)
8. goto 2

N=77=p\*q=11\*7, fi(N)=(p-1)\*(q-1)=10\*6=60. Let e=7, then d=e^(-1) mod 60. Find it by EEA:

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

Q=floor(A3/B3)=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(A3/B3)=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(A3/B3)=floor(4/3)=1

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

A=B=(-1,9,3)

B=T=(2,-17,1)

B3=1=> B2=-17=7^(-1) mod 60; -17 mod 60= 43 => d=43. Check it: 7\*43 =301 mod 60 =1, it is correct. Hence, e=7 is the public key, and d=43 is the private key.

**Q4. (6 points).** If the right half, R1=0xabcd1221, in hexadecimal, what is the value of the bit number 12 after R1 Expansion/Permutation in DES cipher? Explain your solution. Sağ yarı, R1=0x abcd1221, onaltılık ise, 12 numaralı bitin DES şifresindeki Genişletme/Permütasyonundan sonraki değeri nedir? Çözümünüzü açıklayın

**Hint**:

|  |
| --- |
| 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 |

R1=0xabcd1221= 1010 1011 1100 1101 0001 0010 0010 0001. According to E, bit 12 is the original bit 9 of R1 which is 1 (shown in yellow).

**Q5. (6 points).** Explain how the initial value of the register *b* in SHA-512 is calculated. Calculate the first three hexadecimal digits (BB6) of *b.* SHA-512'deki b kaydının başlangıç değerinin nasıl hesaplandığını açıklayın. *b* kaydındaki sayının ilk üç onaltılık basamağını (BB6) hesaplayın.

**Hints**:





For b initialization the prime 3 is used. Its square root fractional part 64 bits are used. Its square root is 1.7320508075688772935274463415059 with the fractional part 0.7320508075688772935274463415059. Multiplying it by 16 and taking the integer part of it, we get the 1st hexadecimal digit: b=11: 11.712812921102036696439141464094.

Taking the fractional part 0.712812921102036696439141464094 and again multiplying by 16 and taking its integer aprt, we get the 2nd hexadecimal digit b=11: 11.405006737632587143026263425503; Similar, for the 3rd digit, multiply 0.405006737632587143026263425503 by 16 getting 6: 6.4801078021213942884202148080532, as it was expected.

**Q6. (6 points).** If A is using Protected1 from the figure below, explain how A can be authenticated by the server B. A, aşağıdaki figurden Protected1 kullanıyorsa, A'nın B sunucusu tarafından nasıl doğrulanabileceğini açıklayın



To be authenticated, A provides Protected1 together with A, passwA, t1A, q1A. The server, B, fetches A’s password from its database, and using the data provided, recalculates Protected1’ according to Fig. 2. If Protected1==Protected1’, A is authenticated.

**After MT Exam questions Q7-Q11 (67 points):**

**Q7. (14 points)** Consider the following materials from the Lecture Notes:

“**AES Key Expansion**

The AES key expansion algorithm takes as input a 4-word (16-byte) key and produces a linear array of 44 words (156 bytes). The following pseudo code describes the expansion:

1. KeyExpansion(byte key[16], word w[44]){
2. Word temp;
3. For(i=0;i<4;i++) w[i]=(key[4\*i], key[4\*i+1], key[4\*i+2], key[4\*i+3]);
4. For(i=4;i<44;i++){
5. Temp=w[i-1];
6. If(I mod 4 = 0) temp = SubWord(RotWord(temp)) XOR Rcon[i/4];
7. W[i]=w[i-4] XOR temp;
8. }
9. }”

What is the value of Temp calculated in Line 5 of the KeyExpansion code if key=0x123456789abcdef123456789abcdef. Show your calculations to get it, explain them. key=0x123456789abcdef123456789abcdef ise, KeyExpansion kodunun 5. Satırında hesaplanan Temp değeri nedir? Almak için hesabını göster, açıkla.

According to the code, w[0]= 0x12345678, w[1]=0x9abcdef1, w[2]=0x23456789, w[3]=0xabcdef; temp=w[4-1]=w[3]= 0xabcdef;

**Q8 (14 points)** Consider the ARP packet structure below. What data is used as the Sender hardware address and Sender protocol address? Aşağıdaki ARP paket yapısını göz önünde bulundurun. Gönderici donanım adresi ve Gönderici protokol adresi olarak ne veri kullanılır?

|  |
| --- |
| **Internet Protocol (IPv4) over Ethernet ARP packet** |
| **Octet offset** | **0** | **1** |
| **0** | Hardware type (HTYPE) |
| **2** | Protocol type (PTYPE) |
| **4** | Hardware address length (HLEN) | Protocol address length (PLEN) |
| **6** | Operation (OPER) |
| **8** | Sender hardware address (SHA) (first 2 bytes) |
| **10** | (next 2 bytes) |
| **12** | (last 2 bytes) |
| **14** | Sender protocol address (SPA) (first 2 bytes) |
| **16** | (last 2 bytes) |
| **18** | Target hardware address (THA) (first 2 bytes) |
| **20** | (next 2 bytes) |
| **22** | (last 2 bytes) |
| **24** | Target protocol address (TPA) (first 2 bytes) |
| **26** | (last 2 bytes) |

Sender hardware address is the MAC address of the sender. Sender protocol address is the IP address of the sender.

**Q9. (13 points).** Consider Kerberos protocol from the Lecture notes:

# “



Figure 26.4. Sequence of messages used to authenticate a client in symmetric encryption

# Protocol

1. C sends to KDS a message, M1 (in the clear), requesting a ticket to be used to authenticate C to S. M1 contains the names of the intended communicants (C,S).
2. When KDS receives M1, the following takes place:

(a) KDS (randomly) constructs a session key, Ksess,C&S

(b) KDS sends to C a message, M2, containing two items:

 (i) [Ksess,C&S, S, LT]

 (ii)  [Ksess,C&S, C, LT] – the actual ticket,

 where LT is the lifetime (the time interval) over which the ticket is valid.

1. When C receives M2, it performs the following steps:
	1. C recovers Ksess,C&S from the first item using  (it cannot decrypt the ticket)
	2. C saves the ticket until it is ready to request some service “

Explain how Ticket is used in the protocol. Biletin protokolde nasıl kullanıldığını açıklayın.

Tick is used in the protocol to get a service by the client C from the server S. It contains th session key, the client’s name, and the life-time. The service decrypts the ticket using a key shared between TGS and S, gets the session key, gets the client’s name, and the life-time. If the ticket has not expired, the client requesting service is the same as in the ticket, and the request is not replayed (by checking Authenticator), then S provides the service to C.

**Q10. (13 points)** Explain who is authenticated and how in the Figure 2.10 below. Aşağıdaki Şekil 2.10'da kimin kimliğinin nasıl doğrulandığını açıklayın



The cellphone is authenticated by the base-station. The cellphone sends its ID to the station, gets back a challenge, and returns it encrypted with a pre-shared secret key K. The cellphone is authenticated if the result of the decryption is equal to the nonce R sent to the cellphone initially.

**Q11. (13 points).** Check that P=(12, 4) belongs to E23(1,1). Show your calculations. Give necessary explanations. P=(12, 4)'ün E23(1,1)'e ait olduğunu kontrol edin. Hesaplamalarınızı gösterin. Gerekli açıklamaları yapın

Hints:

Elliptic curve, *Ep(a,b)*, equation is

$$y^{2}=x^{3}+a∙x+b mod p$$



For the points (x,y)=(12,4) from E23(a=1,b=1) the above equation shall hold. Calculate 4^2=16 mod 23 = 16; x^3+x+1 = 12^3+12+1 = (12\*6\*2\*12 mod 23 + 13) mod 23 =(72 mod 23\*24 mod 23+13) mod 23= (3\*1+13) mod 23 = 16, i.e. the equality holds, and (12,4) is actually an element of E23(1,1).