**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 6, 2024, 16.00**

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

**Instructor Alexander Chefranov**

**Totally 13 questions, 11 pages, 100 points**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Question** | **Q1** | **Q2** | **Q3** | **Q4** | **Q5** | **Q6** | **Q7** | **Q8** | **Q9** | **Q10** | **Q11** | **Q12** | **Q13** | **Total** |
| **Point** | **6** | **6** | **7** | **7** | **7** | **8** | **8** | **9** | **8** | **9** | **8** | **9** | **8** | **100** |
| **Grade** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**Before MT Exam questions Q1-Q5 (33 points):**

**Q1.** **(6 points).** What two tools are used to provide the confidentiality security requirement? Gizlilik güvenlik gereksinimini sağlamak için kullanılan iki araç nelerdir?

Encryption, access control

**Q2. (6 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 Smith has the label value=2. There are 6 documents labeled as follows: Bay Smith 'ın etiket değerinin = 2 olduğunu varsayalım. Aşağıdaki şekilde etiketlenmiş 6 belge vardır:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
| Document | Salary | Performance | Test results | Contractors | Losses | Income |
| Label value | 3 | 2 | 2 | 4 | 4 | 1 |
| Mr Smith can read okuyabilir (Y/N) | n | y | y | n | n | y |
| Mr Smith can write yazabilir(Y/N) | y | y | y | y | y | n |

For each document no=1..6, specify what document in the table above Mr Smith can read and what can write (by filling the last two rows). Give necessary explanations. 1..6 nolu her belge için yukarıdaki tabloda Mr Smith '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.”

**Q3. (7 points).** For RSA with N=95, define its public and private keys. Explain your answer, show intermediate calculations. N=95 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=95=p\*q=19\*5, => p=19, q=5; fi(N)=(p-1)\*(q-1)=18\*4=72

Let e=5, then d=e^(-1) mod 72 = 29, since e\*d=5\*29=145 = 2\*72+1 = 1 mod 72

Thus, e=5, d=29, N=95.

**Q4. (7 points).** If the right half, R1=0x1231ffcd, in hexadecimal, what is the value of the bit number 19 (nineteen) after R1 Expansion/Permutation in DES cipher? Explain your solution. Sağ yarı, R1=0x1231ffcd, onaltılık ise, 19 (on dokuz) 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=0x1231ffcd= 0001 0010 0011 0001 1111 1111 1100 1101. Bit 19 of the output is equal to the bit 12 of R1 according to E-table. Bit 12 of R1 is 1, hence, the bit number 19 is 1.

**Q5**. **(7 points)**  SSL protocol in Lecture notes is described as follows: “Assume that a browser, C, connects to a server, S, that claims to represent a particular enterprise, E (for example, Macy’s). In this case, the protocol consists of the following steps:

1. S sends C a copy of its certificate signed by the CA – in the clear
2. C validates the certificate’s signature using the CA’s public key (included in its browser) and hence knows that the public key in the certificate belongs to the enterprise named in the certificate.
3. C generates and sends to S a session key encrypted with the public key in the certificate.”

For SSL protocol, explain

1) (1 point) who has a public key;

S has a public key

2) (1 point) who generates a session key;

C generates a session key

3) (1 point) how the session key is delivered to the other party;

The session key is delivered to S encrypted with its public key

4) (2 points) is a session key delivery of SSL protocol confidential? Why do you think so?

The session key delivery is confidential because it is delivered encrypted with public key of S, and, hence, only S with its private key can correctly decrypt it.

5) (2 points) is a session key delivery of SSL protocol is protected from tampering with? Why do you think so? SSL protokolünün oturum anahtarı teslimatı kurcalanmaya karşı korunuyor mu? Neden böyle düşünüyorsun?

It is not protected from tampering with because neither digital signature, nor message authentication code is used for its protection.

**After MT Exam questions Q6-Q13 (67 points):**

**Q6. (8 points)** For $q=13$, give a particular numerical example of the Diffie-Hellman key exchange (see Fig. 6.2 below). Show details of your calculations of the shared key, K, by the both parties. q=13 için Diffie-Hellman anahtar değişiminin özel bir sayısal örneğini verin (bkz. aşağıdaki Şekil 6.2). Her iki tarafça paylaşılan anahtar K'ya ilişkin hesaplamalarınızın ayrıntılarını gösterin.

Hints:



Let a=2, XA=3, XB=4, YA=a^XA mod q = 2^3 mod 13 = 8; YB=a^XB mod q = 2^4 mod 13 16 mod 13 = 3. A receives YB and calculates KA=YB^XA mod q = 3^3 mod 13 =1, and B receives YA and calculates KB= YA^XB mod q = 8^4 mod 13 = 64\*64 mod 13 = 12\*12 mod 13 = 144 mod 13 =1. Thus the both parties arrive at the same key, K=KA=KB=1.

**Q7. (8 points)** What a certificate is (3 points) ? Who has issued, when, and to whom a certificate below (3 points) ? What encryption method is used by the subject (2 points)? Sertifika nedir (3 puan)? Aşağıdaki sertifikayı kim, ne zaman ve kime vermiştir (3 puan)? Konu tarafından hangi şifreleme yöntemi kullanılıyor (2 puan)?



A certificate is a document certifying that some subject has a particular public key value. Issuer: Sectigo RSA Domain Validation Secure Server CA. Issue date is not visible in the certificate. Issued to \*.emu.edu.tr. Encryption method of the subject is PKCS#1 RSA Encryption

**Q8. (9 points).** Explain how the initial value of the register *c* in SHA-512 is calculated (3 points). Calculate the first three hexadecimal digits (3C6) of *c (6 points).* SHA-512'deki *c* kaydının başlangıç değerinin nasıl hesaplandığını açıklayın (3 puan). *c* kaydındaki sayının ilk üç onaltılık basamağını (3C6) hesaplayın (6 puan).

**Hints**:





Initial values are taken from the first 64 bits of the fractional part of the square roots of the first eight prime numbers, which are 2,3,5,7,11,13,17, and 19. The third number used for c is 5. Sqrt(5)= 2.2360679774997896964091736687313, multiply its fractional part 0.2360679774997896964091736687313\*16=3.7770876399966351425467786997004. Its integer part, 3, is the 1st hexadecimal digit of c. Again multiply the fractional part of the result by 16: 0. 7770876399966351425467786997004\*16=12.433402239946162280748459195207. Its integer part, 12=C, is the 2nd digit of c. Again multiply the fractional part of the result by 16: 0.433402239946162280748459195207\*16=6.9344358391385964919753471233075. Its integer part, 6, is the 3rd hexadecimal digit of c.

**Q9. (8 points).** If A is using Protected2 from the figure below, explain how A can be authenticated by the server B. A, aşağıdaki figurden Protected2 kullanıyorsa, A'nın B sunucusu tarafından nasıl doğrulanabileceğini açıklayın



A sends to B: A, t1A,q1A, t2A, q2A, and Protected2. B authenticates A as follows: 1) B fetches A’s record from its database, where he finds passwA’ of A. Then B calculates temp1=f1(A, passwA’, t1A, q1A). Then B calculates temp2=f2(temp1, t2A, q2A). A is authenticated by B if temp2==protected2 holds.

**Q10. (9 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. }

RotWord performs a 1-byte circular left shift on a word. This means that an input word [b0, b1, b2, b3] is transformed into [b1, b2, b3, b0].”

What is the value of RotWord(Temp) calculated in Line 6 of the KeyExpansion code if key=0x342156780abcdef312456789fccdefaa for i=4. Show your calculations to get it, explain them. key=0x342156780abcdef312456789fccdefaa ve i=4 ise, KeyExpansion kodunun 6 satırında hesaplanan RotWord(Temp) değeri nedir? Almak için hesabını göster, açıkla.

According to line 3: w[0]= 0x34215678; w[1]=0x0abcdef3; w[2]= 0x12456789, and w[3]= 0xfccdefaa. Hence, according to line 5, temp=w[4-1]=w[3]= 0xfccdefaa, and RotWord(temp)= 0xcdefaafc

**Q11 (8 points)** Consider the ARP packet structure below. What is the use of the fields Operation (OPER) and Sender hardware address (SHA)? Aşağıdaki ARP paket yapısını göz önünde bulundurun. Operasyon (OPER) ve Gönderici donanım adresi (SHA) alanlarının kullanımı nedir?

|  |
| --- |
| **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) |

OPER specifies ARP protocol operation (request or reply). SHA is the MAC address of the sender.

**Q12. (9 points).** Check that P=(9, 7) belongs to E23(1,1). Show your calculations. Give necessary explanations. P=(9, 7)'ün E23(1,1)'e ait olduğunu kontrol edin. Hesaplamalarınızı gösterin. Gerekli açıklamaları yapın

Hints:

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

$$y^{2}=x^{3}+a∙x+b mod p$$



Calculate LHS: y^2 mod p = 7^2 mod 23 = 49 mod 23 =3. Calculate RHS: x^3 +1\*x+1 mod p = 9^3+9+1 mod 23 = 9\*3\*3\*9 +10 mod 23 = (27 mod 23)\*(27 mod 23) +10 mod 23 =4\*4+10 mod 23 = 26 mod 23 =3. Since LHS=RhS, the point meets the equation and belongs to E23(1,1).

**Q13. (8 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

An authenticator consists of C’s name together with a current timestamp, TS, encrypted with Ksess,C&S:



and is meant to be used only once. S can decrypt the authenticator by using Ksess,C&S (which it determines by decrypting the ticket). “

Explain what for and how Authenticator is used in the protocol. Authenticator'ın protokolde ne için ve nasıl kullanıldığını açıklayın.

Authenticator is used to 1) check that the holder of the ticket is actually requesting the service (name in the ticket encrypted by KDS shall be the same as in the authenticator encrypted by the session key received in the ticket) 2) check that it is not a replay by comparing timestamp TS versus already used by C timestamps. The authenticator is decrypted by KsessC&S, and C is extracted and compared versus C in the ticket. TS is also extracted, compared versus the timestamps used previously. If it is for the first time, it is accepted, and posted in the databese of the passwords used. Otherwise, the uses is rejected.