**Eastern Mediterranean University**

**Computer Engineering Department**

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

**Final Exam Son Sınavı**

**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 Süre: 150 Minutes June 25, 2025, 12.30**

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

**Instructor Alexander Chefranov**

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Before MT Exam questions** | | | | | **After MT Exam questios** | | | | | |  |
| **Questions** | **Q1** | **Q2** | **Q3** | **Q4** | **Q5** | **Q6** | **Q7** | **Q8** | **Q9** | **Q10** | **Q11** | **Total** |
| **Point** | **3** | **5** | **7** | **12** | **6** | **12** | **14** | **8** | **10** | **15** | **8** | **100** |
| **Grade** |  |  |  |  |  |  |  |  |  |  |  |  |

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

**Q1.** **(3 points).** What two tools are used to provide the integrity security requirement? Bütünlük güvenliği gereksinimini sağlamak için hangi iki araç kullanılır?

1. Backups
2. checksums

**Q2. (5 points).** What two rules does Mandatory access control (MAC) model use? What are the reasons to use each of them? Zorunlu erişim denetimi (MAC) modeli hangi iki kuralı kullanır? Her birini kullanmanın nedenleri nelerdir?

**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.”

“BLP modeli askeri çok seviyeli güvenlik paradigmasından türetilmiştir (Çok gizli, Gizli, Gizli, Sınıflandırılmamış)

Her belgenin 4 güvenlik seviyesinden 1'i ve her kullanıcının da 4'ten 1'i olmak üzere "izni" vardır.

Belirli bir seviyedeki bir belgeye yalnızca aynı veya daha yüksek izne sahip kullanıcılar erişebilir, "okuma yok" kuralı.

Bir kullanıcı yalnızca kendi veya daha yüksek güvenlik seviyesindeki belgelere yazabilir, "yazma yok" kuralı, '\*' özelliği.”

1. No read-up reasoned by not allowing not enough qualified people to read secret documents
2. No write-down reasoned by necessity to counter Trojan horse attacks

**Q3. (7 points).** DES cipher right half input to round 1 is R0=0x32456**7**FD, in hexadecimal. In which positions will its bits represented by **7** be found after R1 Expansion/Permutation? Give your answer filling an answer table below. Explain your solution. DES şifresi 1. tur için sağ yarım girdi R0=0x324567FD, onaltılık olarak. 7 ile temsil edilen bitleri R1 Genişleme/Permutasyon sonrasında hangi pozisyonlarda bulunacaktır? Cevabınızı aşağıdaki cevap tablosunu doldurarak verin. Çözümünüzü açıklayın.

**Hints**:

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

**Answer table for positions of 7 from R1**

|  |  |  |
| --- | --- | --- |
| Bit # | Bit value | Position(s) after Expansion/Permutation |
| 0 (LSB) | 1 | 35, 37 |
| 1 | 1 | 34 |
| 2 | 1 | 33 |
| 3 (MSB) | 0 | 30, 32 |

7 =0111 in binary, they occupy bits number 21,22,23, and 24. Bit 21 (0) goes to positions 30 and 32. Bit 22 (1) goes to position 33. Bits number 23 (1) goes to position 34. And bit number 24 (1) goes ti positions 41 and 43.

**Q4. (12 points).** For RSA with N=133, define its public and private keys and encrypr the plaintext M=4. Explain your answer, show intermediate calculations. N=133 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=133=p\*q=7\*19=>p=7, q=19, fi(N)=6\*18=108

Let e=5, the d=5^(-1) mod 108

Use EEA:

1. A=(1,0,108), B=(0,1,5)

Q=floir(108/5)=21

T=A-q\*B=(1-21\*0,0-21\*1, 108-21\*5) = (1,-21, 3)

1. A=B=(0,1,5), B=T=(1,-21,3)

Q=floor(5/3) =1

T=A-Q\*B=(0-1\*1, 1+1\*21, 5-1\*3) = (0,22, 2)

1. A=B=((1,-21,3), B=T=(0,22,2)

Q=floor(3/2)=1

T=A-q\*B = (1-1\*0, -21-1\*22, 3-1\*2)=(1,-43, 1)

1. A=B=(0,22,2), B=T=(1,-43,1)

B3=1=>B2=-43 mod 108 = 65 =d=5^(-1) mod 108

Check it:5\*65 mod 108 =325 mod 108 = 3\*108+1 mod 108 =1, hence, d=65

Encrypt C=M^e mod N = 4^5 mod 133

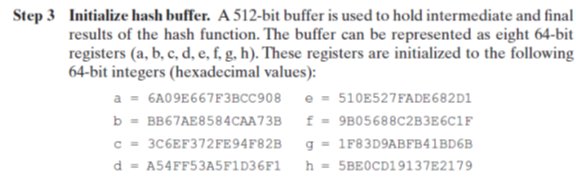
4^2 = 16

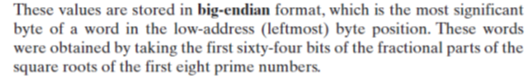
4^4 = 16\*16 mod 133 = 256 mod 133 = 123

C = 4^4\*4 = 123\*4 mod 133 = 246\*2 mod 133 = 113\*2 mod 133 = 226 mod 133 = 93

**Q5. (6 points).** Explain how the initial value of the register *d* in SHA-512 is calculated (2 points). Calculate the first three hexadecimal digits (A54) of *d (4 points).* SHA-512'deki d kaydının başlangıç değerinin nasıl hesaplandığını açıklayın (2 puan). *d* kaydındaki sayının ilk üç onaltılık basamağını (A54) hesaplayın (4 puan).

**Hints**:





Initial register values are calculated as the first 64 bits of the fractional part of the square root of the first 8 prime numbers: 2,3,5,7,11,13,17, and 19. Register d is initialized using 7:

Sqrt(7)= 2,6457513110645905905016157536393 with fractional part 0,6457513110645905905016157536393. Convert it to hexadecimal by successive multiplication by 16 and writing out their integer parts as hexadecimal digits:

0,6457513110645905905016157536393\*16 = 10,332020977033449448025852058228

Hence, the first digit is 10 = A

0,332020977033449448025852058228\*16 = 5,3123356325351911684136329316507

Hence, the second digit is 5

0,3123356325351911684136329316507\*16 = 4,9973701205630586946181269064107

Hence, the 4rd digit is 4 as expected.

**After MT Exam questions Q6-Q11 (67 points):**

**Q6. (12 points)** For , 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=17 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=2, XB=3, then YA=2^2 mod 17 = 4, YB=2^3 mod 17 = 8

Then K calculated by A is K=YB^XA mod q = 8^2 mod 17 = 64 mod 17 = 13

K calculated by B is K=YA^XB mod q = 4^3 mod 17 = 64 mod 17 = 13.

**Q7. (14 points)** Consider the following materials from the Lecture Notes: Ders Notlarından aşağıdaki materyalleri inceleyin:

“**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 RotWord(Temp) calculated in Line 6 of the KeyExpansion code if w[4..7]={0x11112222, 0x33334444, 0x55556666, 0x77778888} for i=8. Show your calculations to get it, explain them. w[4..7]={0x11112222, 0x33334444, 0x55556666, 0x77778888} ve i=8 ise, KeyExpansion kodunun 6 satırında hesaplanan RotWord(Temp) değeri nedir? O almak için hesabını göster, açıkla.

**Hints:** “1. 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].

1. SubWord performs a byte substitution on each byte of its input word, using the S-box (Table 5.4a)
2. The result of steps 1 and 2 is XORed with a round constant, Rcon[j]

The round constant is a word in which the three rightmost bytes are always 0. Thus the effect of an XOR of a word with Rcon is to only perform an XOR on the leftmost byte of the word. The round constant is different for each round and is defined as Rcon[j]=(RC[j],0,0,0), with RC[1]=1, RC[j]=2RC[j-1] and with multiplication defined over the field GF(28). The values of RC[j] in hexadecimal are 1. RotWord, bir kelime üzerinde 1 baytlık dairesel sola kaydırma gerçekleştirir. Bu, [b0, b1, b2, b3] giriş kelimesinin [b1, b2, b3, b0]'a dönüştürüldüğü anlamına gelir.

2. SubWord, S-box'ı kullanarak giriş kelimesinin her baytında bir bayt ikamesi gerçekleştirir (Tablo 5.4a)

3. 1. ve 2. adımların sonucu, bir yuvarlama sabiti olan Rcon[j] ile XOR'lanır

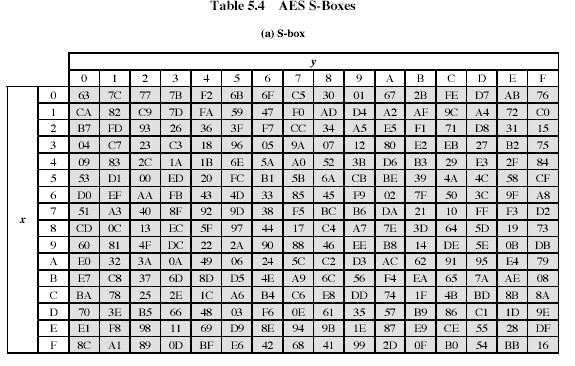
Yuvarlama sabiti, en sağdaki üç baytın her zaman 0 olduğu bir kelimedir. Bu nedenle, bir kelimenin Rcon ile XOR'lanmasının etkisi, yalnızca kelimenin en soldaki baytında bir XOR gerçekleştirmektir. Yuvarlama sabiti her tur için farklıdır ve Rcon[j]=(RC[j],0,0,0) olarak tanımlanır; burada RC[1]=1, RC[j]=2 RC[j-1] ve çarpma, GF(28) alanı üzerinde tanımlanır. RC[j] değerleri onaltılık sayı sisteminde şöyledir:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| J | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| RC[j] | 01 | 02 | 04 | 08 | 10 | 20 | 40 | 80 | 1b | 36 |

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: Örneğin, 8. tur için tur anahtarının şu olduğunu varsayalım: EA D2 73 21 B5 8D BA D2 31 2B F5 60 7F 8D 29 2F. Daha sonra 9. tur için tur anahtarının ilk dört baytı (1. sütun) aşağıdaki gibi hesaplanır:

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

**“**

****

Temp = w[7] = 0x77778888

Since i=8 and 8 mod 4 =0, calculate RotWord(temp) = RotWord(0x77778888) =0x77888877.

Then calculate SubWord(0x77888877) =F5C4C4F5. Rcon[i/4]=Rcon[2] = 02000000

Calculate SubWord(0x77888877) xor Rcon[2]= F5C4C4F5 xor 02000000 = F7C4C4F5

Calculate 5 xor 2 = 0101 xor 0010 = 0111. All the rest digits in F5C4C4F5 are preserved,

Thus , temp = F7C4C4F5, and w[8] = w[4] xor temp = 0x11112222 xor F7C4C4F5, or in binary

0001 0001 0001 0001 0010 0010 0010 0010

Xor

1111 0111 1100 0100 1100 0100 1111 0101

=

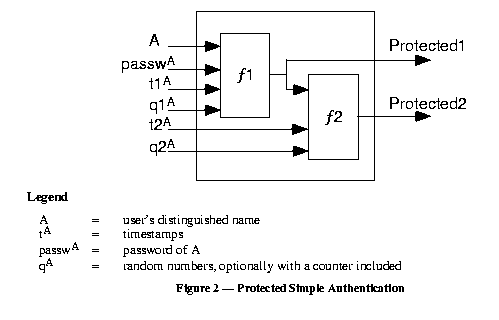
1110 0110 1101 0101 1110 0110 1101 0111 = 0xE6D5E6D7 = w[8]

**Q8 (8 points)** Consider the ARP packet structure below. What is the use of the fields Sender protocol address (SPA) and Target hardware address (THA)? How many bytes are allocated for SPA? How many bytes are allocated for THA? Aşağıdaki ARP paket yapısını göz önünde bulundurun. Gönderen protokol adresi (SPA) ve Hedef donanım adresi (THA) alanlarının kullanımı nedir? SPA için kaç bayt ayrılmıştır? THA için kaç bayt ayrılmıştır?

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

SPA has IP address of a sender in 4 bytes. THA has MAC address of a receiver in 6 bytes.

**Q9. (10 points).** Explain why the use of Protected2 in the figure below protects A’s password. What the password is protected from? How exactly is it protected? Aşağıdaki şekilde Protected2 kullanımının A'nın şifresini neden koruduğunu açıklayın. Şifre neye karşı korunuyor? Tam olarak nasıl korunuyor?



The use of Prtotected2 protects the password because it does not travel in clear. The password is protected from reading. It is protected by two times hashing first, with the user name A, timestamp t1 and nonce q1. Then this hash is again hashed with the timestamp t2 and nonce q2.

**Q10. (15 points).** Check that P=(6, 4) belongs to E23(1,1). Show your calculations. Give necessary explanations. P=(6, 4)'ün E23(1,1)'e ait olduğunu kontrol edin. Hesaplamalarınızı gösterin. Gerekli açıklamaları yapın

**Hints**:

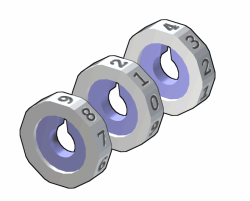
Elliptic curve, *Ep(a,b)*, equation is



Calculate LHS of E23(1,1): 4^2 = 16 mod 23 = 16

Calculate RHS of E23(1,1): 6^3+6+1 mod 23 = 36\*6+7 mod 23 = 13\*6 +7 mod 23 = 26\*3+7 mod 23 = 3\*3+7 mod 23 = 16, that is equal to the LHS. Hence, P(6,4) actually belongs E23(1,1).

**Q11. (8 points).** Explain how a letter lock below works. Aşağıdaki harf kilidinin nasıl çalıştığını açıklayın



A particular combination of letters at top position of the disks allows the key passing all the disks on opening a lock. Knowledge of the combination allows opening the lock easily. But trials will takeon average too much time to find the right combination making difficult its breaking.