**Eastern Mediterranean University**

**Computer Engineering Department**

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

**Midterm Exam**

**Three 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 üç A4 yaprak el yazısı kağıt kullanılabilir. Fotokopi, çıktı vb. izin verilmez! Hesap makinelerine izin verilir, diğer elektronik cihazlara izin verilmez**

**Duration Süre: 110 Minutes Dk April Nısan 26, 2023, 12.30**

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

**Instructor Alexander Chefranov**

**Totally Toplam: 7 questions soru, 10 pages sayfa, 100 points puan**

# Q1. (15 points). 1) Fill in a substitution table below for a simple substitution cipher for English alphabet letters only using a key phrase “Pierre discusses weeks with an artificial intelligence and ends his life", 2) encrypt “Pierre”, and 3) decrypt it back. Explain your solution.

# Aşağıdaki yerine koyma tablosunu sadece İngilizce alfabe harflerini kullanarak tamamlayınız. Aşağıdaki anahtar ifadeyi kullanın: “Pierre discusses weeks with an artificial intelligence and ends his life"; 2) “Pierre”i şifreleyin ve 3) geri şifresini çözün

# Substitution table ikame tablosu

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext letter | 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 |
| Ciphertext letter | p | i | e | r | d | s | c | u | w | k | t | h | a | n | f | l | g | b | j | m | o | q | v | x | y | z |

Fill in the substitution table by successive non-repeating letters from the key phrase followed by the rest letters in alphabetical order. Then encrypt by substituting each plaitext letter by respective ciphertext letter from the table:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Plaintext | P | i | e | r | r | e |
| Ciphertext | l | w | d | b | b | d |
| Decrypted text | p | i | e | r | r | e |

For decryption, each ciphertext letter found in the bottom row of the table is replaced by the letter above it in the top row

**Q2. (14 points).** What are the three differences between Access control matrix model and Bell-LaPadula model? Give necessary explanations. Erişim denetimi matris modeli ile Bell-LaPadula modeli arasındaki üç fark nedir? Gerekli açıklamaları yapın

1. BLP model uses clearance levels, ACM model does not use them
2. ACM model for each pair (subject, object) specifies all access rights of the subject with respect to the object; BLP model has not such pairs
3. BLP model uses two rules (“no read-up”, “no write-down”) to decide on the access of a subject to an object; ACM model does use these rules.

**Q3. (15 points).** Use RSA to encrypt M=3 if N=91. Explain your answer, show intermediate calculations. N=91 ise M=3'ü şifrelemek için RSA kullanın. 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). 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) //T=A-Q\*B
6. (A1,A2,A3):= (B1,B2,B3)
7. (B1,B2,B3):= (T1,T2,T3)
8. goto 2

Use squaring for exponentiation and a\*b mod N = ((a mod N)\*(bmod N)) mod N

5^2 mod 91 =25

5^4 mod 91 = 25^2 mod 91 = 125\*5 mod 91 = 34\*5 mod 91 = 170 mod 91 = 79

5^8 mod 91 = 79\*79 mod 91 = (-12)\*(-12) mod 91 = 144 mod 91 = 53

5^16 mod 91 = 53\*53 mod 91 = 79

5^29 mod 91 = 5^16\*5^8\*5^4\*5 mod 91 = 79\*53\*79\*5 mod 91 = 53\*53\*5 mod 91 = 79\*5 mod 91 = 395 mod 91= 4\*91+31 mod 91 = 31 = C

N=p\*q=91=>p=13, q=7, fi(N)=(p-1)\*(q-1)=12\*6=72

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

Use EEA to calculate d:

A=(1,0,72), B=(0,1,5)

Q=floor(72/5)=14

T=A-q\*B=(1-14\*0,0-14\*1,72-14\*5)=(1,-14,2)

A=(0,1,5), B=T=(1,-14,2)

Q=floor(5/2)=2

T=A-q\*B=(0-2\*1,1-2\*(-14),5-2\*2)=(-2,29,1)

A=(1,-14,2), B=T=(-2,29,1)

Since B3=1, 5^(-1) mod 72 = B2= 29, as shown above.

Encryption: C=M^e mod N = 3^5 mod 91

3^2 mod 91 =9

3^4 mod 91 = 81 = -10 mod 91

3^5 mod 91 = 3^4\*3 mod 91 = -10\*3 mod 91 = -30 mod 91 = 61

**Q4. (14 points).** If the right half, R1=0x12345678, in hexadecimal, what is the value of the bit number 27 after its Expansion/Permutation in DES cipher? Explain your solution. Sağ yarı, R1=0x12345678, onaltılık ise, 27 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 |

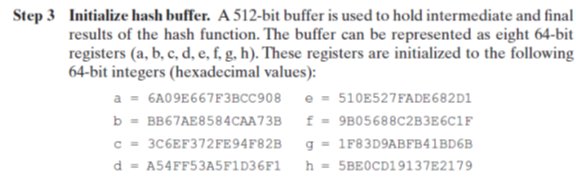
R1 in binary is

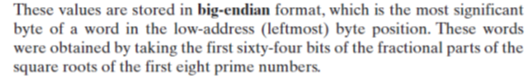
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| 3 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |
| 4 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |

Bit 18 of R1 is in the position 27 according to E-table. Bit 18 is 1 (shown by yellow)

**Q5. (14 points).** Explain how the initial value of the register *a* in SHA-512 is calculated. Calculate the first three hexadecimal digits (6A0) of *a.* SHA-512'deki a regıster başlangıç değerinin nasıl hesaplandığını açıklayın. Bir sayının ilk üç onaltılık basamağını (6A0) hesaplayın.

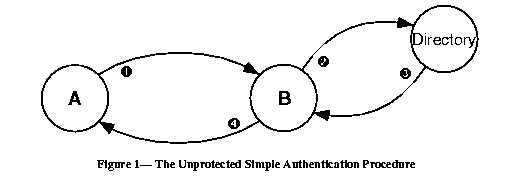
**Hints**:





Initial value of a is calculated as the first 64 bits of the fractional part of the square root of 2. Square root of 2 is 1.4142135623730950488016887242097. Its fractional part is 0.4142135623730950488016887242097. The first hexadecimal digit is obtained by multiplication by 16 and taking the integer part of the result: 6.6274169979695207808270195873552 that is 6. Then, take fractional part of the result and multiply again by 16: 10.038671967512332493232313397683. Its integer part 10=A, is the 2nd hexadecimal digit. Again, take the fractional part of the result and multiply by 16: 0.61875148019731989171701436292333. Its integer part is 0, the 3rd hexadecimal digit.

**Q6. (14 points).** Explain the meaning of A, B, Directory, and of the actions represented by the numbers 1..4 in the figure below from the Lecture notes: Ders notlarından aşağıdaki resimde, A, B, İndeks ve 1..4 sayılarıyla temsil edilen eylemlerin anlamını açıklayın:



A: client; B: server; Directory: database with user names and passwords;

1: client asks the service of B providing its user name and password

2: server checks its database for the user’s record, fetches its password

3: database returns whether user name and password provided match the kept ones

4: server accepts or rejects the client based on the result received from its database

# Q7. (14 points). How AES S-box works? What is the result in decimal of theS-box transformation of the decimal value 12310? Give necessary explanations. AES S-box nasıl çalışır? Ondalık 123'ün S-kutusu dönüşümünün ondalık sonuç nedir? Gerekli açıklamaları yapın.

# Hints:

# 

AES S-box replaces a byte represented by two hexadecimal digits, xy, by substituting it by the entry of S-box located in row x and column y. 12310=7\*16+11=7B16. On the cross of row 7 and column B, is 2116=2\*16+1=3310.