**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: 120 Minutes Dk April Nısan 4, 2024, 14.30**

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

**Instructor Alexander Chefranov**

**Totally Toplam: 5 questions soru, 7 pages sayfa, 100 points puan**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Question/Soru** | **Q1** | **Q2** | **Q3** | **Q4** | **Q5** | **Total/Toplam** |
| **Point/Puan** | **20** | **20** | **20** | **20** | **20** | **100** |
| **Grade/Not** |  |  |  |  |  |  |

# Q1. (20 points). 1) Fill in a substitution table below for a simple substitution cipher for English alphabet letters only using a key phrase “Biden Outraged After Israel’s Military Claims Aid Convoy Attack Was a Mistake”, 2) encrypt “Exam is today”, and 3) decrypt it back. Explain your solution. 1) Yalnızca İngilizce alfabedeki harflerin yerine " Biden Outraged After Israel’s Military Claims Aid Convoy Attack Was a Mistake " ifadesini kullanan basit bir ikame şifresi için aşağıdaki ikame tablosunu doldurun, 2) "Exam is today"ı şifreleyin ve 3) şifreyi geri çözün. Çözümünüzü açıklayın.

# Substitution table ikame tablosu

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| 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 | B | I | D | E | N | O | U | T | R | A | G | F | S | L | M | Y | C | V | K | W | H | J | P | Q | X | Z |

Encrypt by substitution of the letters found in the top row of the substitution table by the letter just beneath them:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| E | X | A | M | I | S | T | O | D | A | Y |
| N | Q | B | S | R | K | W | M | E | B | X |

Ciphertext is: NQBSRKWMEBX

Decryption is made similarly but substituting symbols of the bottom row by respective letters just above them:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| N | Q | B | S | R | K | W | M | E | B | X |
| E | X | A | M | I | S | T | O | D | A | Y |

**Q2. (20 points).** What two rules define the mandatory access control (MAC) model? What is the rational for each of them? Zorunlu erişim kontrolü (ZEK) modelini hangi iki kural tanımlar? Her birinin mantığı nedir?

The first rule: “no read-up”, the second rule: “no write-down”

The rational for the first rule comes from military where people with not sufficient, low secrecy level shall not get access to the higher secrecy level documents. The rational for the 2nd rule is to counter Trojan horse attack, when a malicious program is invoked by a valid high-level secrecy user and can read high-secrecy documents and write them into low-level documents later might be accessed by an attacker having low-secrecy level.

**Q3. (20 points).** For RSA, define the private/public keys pair, encrypt M=7, and decrypt it back if $p,q\in \{27,28,29,30,31\}$. Use binary decomposition of an exponent, squaring, and immediate modulo reduction when getting a number greater than $N$ Explain your answer, show intermediate calculations. RSA için, özel/genel anahtar çiftini tanımlayın, M=7'yi şifreleyin ve p,q∈{27,28,29,30,31} ise şifresini tekrar çözün. N'den büyük bir sayı elde ederken üssün ikili ayrıştırmasını, karesini almayı ve anında modülo azaltmayı 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

e=29, d=5, e\*d=145 mod 72 =1

C=M^e mod N = 5^29 mod 91

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

Decryption:

M=C^d mod N = 31^5 mod 91

31^2 mod 91 = 51

31^4 mod 91 = 51\*51 mod 91 = 53

31^5 mod 91 = 31^4\*31 mod 91 = 53\*31 mod 91 = 5

Solution:

P=29, q=31, N=p\*q= 899, fi(N)=28\*30=840

E=11, d=11^(-1) mod 840

Use EEA:

1. A=(1,0,840), B=(0,1,11)

Q=floor(840/11)=76

T=A-q\*B=(1-76\*0, 0-76\*1, 840-76\*11)=(1,-76, 4)

1. A=B=(0,1,11), B=(1,-76,4)

Q=floor(11/4)=2

T=A-q\*B=(0-2\*1, 1-2\*(-76), 11-2\*4)=(-2,153,3)

1. A=B=(1,-76,4), B=(-2,153,3)

Q=floor(4/3)=1

T=A-q\*B=(1-1\*(-2), -76-1\*153, 4-1\*3)= (3,-229,1)

1. A=B=(1,-76,4), B=T=(3,-229,1)

B3=1=>B2=-229 mod 840 = 611=11^(-1) mod 840=d

Check: e\*d=11\*611 = 6721 = 840\*8+1 mod 840 =1

Thus, e=11, d=611

C=M^e mod N = 7^11 mod 899 = 7^8\*7^2\*7 mod 899

7^2 mod 899 = 49

7^4 mod 899 = 49\*49 mod 899 = 603

7^8 mod 899 = 603\*603 mod 899 = 413

C=7^11 mod 899 = 7^8\*7^2\*7 mod 899 = 413\*49\*7 mod 899 = 459\*7 mod 899 = 516

611= 512+64+32+2+1

M’=C^d mod N = 516^611 mod 899 = 516^512\*516^64\*516^32\*516^2\*516 mod 899

516^2 mod 899 = 516\*516 mod 899 = 152

516^4 mod 899 = 152\*152 mod 899 = 629

516^8 mod 899 = 629\*629 mod 899 = 81

516^16 mod 899 = 81\*81 mod 899 = 268

516^32 mod 899 = 268\*268 mod 899 = 803

516^64 mod 899 = 803\*803 mod 899 = 226

516^128 mod 899 = 226\*226 mod 899 = 732

516^256 mod 899 = 732\*732 mod 899 = 20

516^512 mod 899 = 20\*20 mod 899 = 400

M’=516^512\*516^64\*516^32\*516^2\*516 mod 899 = 400\*226\*803\*152\*516 mod 899 = 500\*803\*152\*516 mod 899 = 546\*152\*516 mod 899 = 284\*516 mod 899 = 7=M

**Q4. (20 points).** What is the result of DES cipher Expansion/Permutation of the right half, R1=0xabcdef9a, in hexadecimal? Explain your solution. Sağ yarının (R1=0xabcdef9a) DES şifresi Genişletme/Permütasyonunun onaltılık sayı cinsinden sonucu 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=0xabcdef9a=

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |

Result in binary:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 0 | 1 | 0 | 1 | 0 | 1 |
| 0 | 1 | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 1 | 1 |
| 1 | 1 | 0 | 1 | 0 | 1 |

Result in hexadecimal: 0x557e5bf5fcf5

**Q5. (20 points).** In the conditions of the question Q3, calculate RSA digital signature of the message “Exam is today” if the hash function used is $h(x)=\sum\_{i=1}^{n}code\left(x\_{i}\right) mod 17$ where $n$ is the number of characters in the message $x$, and $code()$ is defined by the substitution table of the question Q1, e.g. $code(“e”)=4$. Explain your solution. Soru 3'ün koşullarında, kullanılan karma işlevi $h(x)=\sum\_{i=1}^{n}code\left(x\_{i}\right) mod 17$ ise, "Exam is today" mesajının RSA dijital imzasını hesaplayın; burada n, x mesajındaki karakter sayısıdır ve code(), Q1 sorusunun ikame tablosu tarafından tanımlanır, ör. $code(“e”)=4$. Çözümünüzü açıklayın.

H(“Exam is today”)=4+23+0+12+8+18+19+14+3+0+24 mod 17 = 4+6+3+1+2+7 mod 17 = 23 mod 17 = 6 = 125 mod 17

Digital signature is DS=RSA(Private\_key, h(message))= h(message)^Private\_key mod N

In the settings of Q3, there are two keys: 11 and 611, and N=899. Let Private\_key=11, public\_key=611. Then DS=6^11 mod 899 = 6^8\*6^2\*6 mod 899

6^2 mod 899 = 36

6^4 mod 899 = 36\*36 mod 899 = 397

6^8 mod 899 = 397\*397 mod 899 = 284

DS=6^11 mod 899 = 6^8\*6^2\*6 mod 899 = 284\*36\*6 mod 899 = 335\*6 mod 899 = 212.