**Eastern Mediterranean University**

**Computer Engineering Department**

**CMSE-456/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 25, 2025, 10.30**

**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 “[China Has an Army of Robots on Its Side in the Tariff War](https://www.nytimes.com/2025/04/23/business/china-tariffs-robots-automation.html)”, 2) encrypt “Artificial intelligence”, and 3) decrypt it back. Explain your solution. 1)Yalnızca İngilizce alfabedeki harflerin yerine "[China Has an Army of Robots on Its Side in the Tariff War](https://www.nytimes.com/2025/04/23/business/china-tariffs-robots-automation.html)" ifadesini kullanan basit bir ikame şifresi için aşağıdaki ikame tablosunu doldurun, 2) " Artificial intelligence "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 | c | h | i | n | a | s | r | m | y | o | f | b | t | d | e | w | g | j | k | l | p | q | u | v | x | z |

Encryption, use substitution table top-to-bottom:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext | a | r | t | i | f | i | c | i | a | l | i | n | t | e | l | l | i | g | e | n | c | e |
| Cipherttext | c | j | l | y | s | y | i | y | c | b | y | d | l | a | b | b | y | r | a | d | i | a |

Decryption, use substitution table bottom-to-top:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Cipherttext | c | j | l | y | s | y | i | y | c | b | y | d | l | a | b | b | y | r | a | d | i | a |
| Plaintext | a | r | t | i | f | i | c | i | a | l | i | n | t | e | l | l | i | g | e | n | c | e |

**Q2. (20 points).** What is the difference between the access control lists and capability lists? How are they related to the access control matrix? What is object? What is subject?

Erişim kontrol listeleri ile yetenek listeleri arasındaki fark nedir? Erişim kontrol matrisiyle nasıl ilişkilidirler? Nesne nedir? Özne nedir?

ACL shows for each object what subjects have access to that object, but CL shows for each subject what objects are accessible to it. ACL is the column view of the acsess control matrix (ACM), and CL is the row view of ACM. Objects are files, documents, devices, other assets of a computer system, whereas subject are processes working with these assets

**Q3. (20 points).** What is the result of DES cipher Permuted Choice 2 in hexadecimal if its input is 0xabcdef9a567798 in hexadecimal? Explain your solution. Girişi onaltılık sayı sisteminde 0xabcdef9a567798 ise DES şifresinin Permuted Choice 2'sinin onaltılık sayı sisteminde sonucu nedir? Çözümünüzü açıklayınız.

**Hint**:

|  |
| --- |
| Permuted Choice 2 (PC-2) |
| 14 17 11 24 1 5 3 2815 6 21 10 23 19 12 426 8 16 7 27 20 13 241 52 31 37 47 55 30 4051 45 33 48 44 49 39 5634 53 46 42 50 36 29 32 |

0xabcdef9a567798 in hexadecimal in binary is

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

 There result of PC2 in binary is

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | 1 (14) | 1 (17) | 0 (11) | 1 (24) | 1 (1) | 1 (5) | 1 (3) | 1 (28) |
| 2 | 0 (15) | 0 (6) | 1 (21) | 1 (10) | 1 (23) | 1 (19) | 0 (12) | 0 (4) |
| 3 | 0 (26) | 1 (8) | 1 (16) | 1 (7) | 0 (27) | 0 (20) | 1 (13) | 0 (2) |
| 4 | 0 (41) | 1 (52) | 1 (31) | 0 (37) | 1 (47) | 0 (55) | 0 (30) | 0 (40) |
| 5 | 0 (51) | 0 (45) | 0 (33) | 1 (48) | 1 (44) | 1 (49) | 1 (39) | 0 (56) |
| 6 | 1 (34) | 1 (53) | 1 (46) | 1 (42) | 0 (50) | 1 (36) | 1 (29) | 0 (32) |

Binary output is

1101 1111 0011 1100 0111 0010 0110 1000 0001 1110 1111 0110

Hexadecimal output is 0xdf3c72681ef6

**Q4. (20 points).** For RSA, define the private/public keys pair, encrypt $M=8$, and decrypt it back if $N=143$. 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, $M=8$'yi şifreleyin ve $N=143$ 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:**

N=143 = p\*q => p=11, q=13

Fi(N) = (p-1)(q-1) = 10\*12 = 120

Let e= 7, d = e^(-1) mod 120, find it by EEA

1. A = (1,0,120), B= (0,1,7)

Q= floor(120/7) = 17

T = A-q\*B = (1-17\*0, 0-17\*1, 120-17\*7) = (1, -17, 1)

A = B = (0,1, 7)

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

B3 = 1 => B2 = -17 mod 120 = 103 =d

Check that e\*d mod 120 =1: 7\*103 = 721 mod 120 = 6\*120+ 1 mod 120 =1, OK

 E = 7, d = 103

1. Encrypt M = 8:

C = M^e mod N = 8^7 mod 143

7 = 4 + 2 + 1

Find squares:

8^2 = 64 mod 143 = 64

8^4 = 64^2 mod 143 = 64\*2\*32 mod 143 = 128\*32 mod 143 = -15\*32 mod 143 = -120\*4 mod 143 = 23\*4 mod 143 = 92

C = 8^4\*8^2\*8 mod 143 = 92\*64\*8 mod 143 = 92\*128\*4 mod 143 = -92\*15\*4 mod 143 = 51\*15\*4 mod 143 = 153\*20 mod 143 = 10\*20 mod 143 = 200 mod 143 = 57

1. Decrypt C = 57 by M’ = C^d mod N = 57^103 mod 143

103 = 64 + 32 + 4 + 2 +1

Find squares:

57^2 = 19\*3\*19\*3 mod 143 = 19\*9\*19 mod 143 = 171\*19 mod 143 = 28\*19 mod 143 = 4\*7\*19 mod 143 = 4\*133 mod 143 = -40

57^4 = 40\*40 mod 143 = 160\*10 mod 143 = 17\*10 mod 143 = 170 mod 143 = 27

57^8 = 27\*27 mod 143 = 27\*9\*3 mod 143 = 243\*3mod 143 =100\*3 mod 143 = 50\*3\*2 mod 143 = 150\*2 mod 143 = 7\*2 mod 143 = 14

57^16 = 14\*14 mod 143 = 196 mod 143 = 53

57^32 = 53\*53 mod 143 = 2809 mod 143 = 92

57^64 = 92\*92 mod 143 = 92\*2\*46 mod 143 = 184\*46 mod 143 = 41\*46 mod 143 = 1886 mod 143 = 27

M’ = 57^103 mod 143 = 57^64\*57^32\*57^4\*57^2\*57 mod 143 = 27\*92\*27\*(-40)\*57 mod 143 = 14\*92\*(-40)\*57 mod 143 = 7\*2\*92\*(-40)\*57 mod 143 = 7\*184\*(-40)\*57 mod 143 = 7\*41\*4\*(-10)\*57 mod 143 = 7\*164\*(-10)\*57 mod 143 = 7\*21\*(-10)\*57 = 147\*(-10)\*57 mod 143 = 4\*(-10)\*19\*3 mod 143 = -4\*190\*3 mod 143 = -4\* 47\*3 = 4\*(-141) mod 143 = 4\*2 mod 143 = 8 = M, hence, decryption is correct

**Q5. (20 points).** Given SHA-512 round function inputs as

a = 6A09E667F3BCC908 e = 510E527FADE682D1

b = BB67AE8584CAA73B f = 9B05688C2B3E6C1F

c = 3C6EF372FE94F82B g = 1F83D9ABFB41BD6B

d = A54FF53A5F1D36F1 h = 5BE0CD19137E2179,

what are the output values of g and h in binary number system?

Verilen SHA-512 yuvarlama fonksiyonu girişleri şu şekildedir:

a = 6A09E667F3BCC908 e = 510E527FADE682D1

b = BB67AE8584CAA73B f = 9B05688C2B3E6C1F

c = 3C6EF372FE94F82B g = 1F83D9ABFB41BD6B

d = A54FF53A5F1D36F1 h = 5BE0CD19137E2179,

g ve h'nin ikili sayı sistemi olarak çıkış değerleri nelerdir?

Hints:



According to the code above:

h = 1F83D9ABFB41BD6B =

0001 1111 1000 0011 1101 1001 1010 1011 1111 1011 0100 0001 1011 1101 0110 1011// h = g

g = 9B05688C2B3E6C1F =

1001 1011 0000 0101 0110 1000 1000 1100 0010 1011 0011 1110 0110 1100 0001 1111// g = f