**MT Exam CMSE-512 02.04.2024, 16.30 (90 min, 30 points)**

St. Name, Surname\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ St.Id#\_\_\_\_\_\_\_\_\_\_\_\_\_

**Three A4-sized sheets of paper with your handwritten notes may be used. Calculators are allowed. Other electronic devices are not allowed**

Instructor Alexander Chefranov

**Totally 4 questions, 5 pages**

Good Luck!

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Task | T1 | T2 | T3 | T4 | Total |
| Point | 7.5 | 7.5 | 7.5 | 7.5 | 30 |

**Task 1. (7.5 points)** What is the user-oriented access control? What three methods of user authentication do you know?

The user-oriented access control is the control of the authenticity of a user. Authentication methods: 1) by user name and password; 2) two-factor by user name, password, and verification code sent to the registered telephone that is to be entered by the user; 3) by biometrics (fingerprints, iris, face, etc.)

**Task 2. (7.5 points)** What three strategies of password breaking do you know? Explain the essence of each.

1. Brute force attack: try to enumerate all possible passwords
2. Dictionary attack: try words from a dictionary
3. Steal password, e.g. by looking over shoulder when the password is entered

**Task 3. (7.5 points)** Define an RSA private/public key pair for some and check their correctness. Encrypt and decrypt *M=5* with RSA using the keys. Show your calculations, give necessary explanations.

Hints: Two large prime numbers, *p* and *q*, , are selected, and an integer, *d*, is chosen that is relatively prime to *(p-1)(q-1)*. Finally, an integer e is computed such that

, N=pq, C=MemodN, M=CdmodN

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)
6. (A1,A2,A3):= (B1,B2,B3)
7. (B1,B2,B3):= (T1,T2,T3)
8. goto 2

p=17, q=19, N=p\*q=323, fi(N)=16\*18=288

Let e=5, then d=5^(-1) mod 288. Use EEA to find it:

1. A=(1,0,288), B=(0,1,5)

Q=floor(A3/B3)=floor(288/5)=floor(57+3/5)=57

T=A-q\*B=(1-57\*0, 0-57\*1, 288-57\*5)=(1,-57,3)

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

B=T=(1,-57,3)

Q=floor(A3/B3)=floor(5/3)=floor(1+2/3)=1

T=A-q\*B=(0-1\*1, 1-1\*(-57), 5-1\*3)=(-1,58,2)

1. A=B=(1,-57,3)

B=(-1,58,2)

Q=floor(A3/B3)=floor(3/1)=floor(1+1/2)=1

T=A-q\*B=(1-1\*(-1), -57-1\*58, 3-1\*2)=(2,--115,1)

1. A=B=(-1,58,2)

B=(2,--115,1)

B3=1 =>B2=-115 mod 288 = 173 = 5^(-1) mod 288

Check it: 173\*5=865=3\*288+1 mod 288 = 1

d=173

Encryption:

C=5^5 mod 323 = 5^4\*5 mod 323

5^2 = 25 mod 323= 25

5^4 = 25\*25 mod323 = 625 mod 323 =302

C= 302\*5 mod 323 = 1510 mod 323 = 4\*323+218 mod 323 =218

Decryption: M’=218^173 mod 323

173=128+32+8+4+1

Hence, 218^173 mod 323 = 218^128\*218^32\*218^8\*218^4\*218 mod 323

218^2 mod 323 =105\*105=105\*3\*35 =315\*35 mod 323 = -8\*35 mod 323 = -280 mod 323 = 43

218^ 4 mod 323 = 43\*43 mod 323= 234

218^8 mod 323 = 234\*234 mod 323 = 89\*89 mod 323 = 169

218^16 mod 323 = 169\*169 mod 323 = 154\*154 mod 323 = 154\*2\*77 mod 323 = 308\*77 mod 323 = -15\*77 mod 323 =-3\*5\*77 mod 323 = -3\*385 mod 323 =-3\*62 mod 323 = -186 mod 323 = 137

218^32 mod 323 = 137\*137 mod 323 = 35

218^64 mod 323 = 35\*35 mod 323 = 1225 mod 323 = 256

218^128 mod 323 = 256\*256 mod 323 = 67\*67 mod 323 = 290

Hence, M’=218^128\*218^32\*218^8\*218^4\*218 mod 323=

290\*35\*169\*234\*218 mod 323 =

-33\*35\*169\*234\*2\*109 mod 323 = -3\*11\*35\*169\*468\*109 mod 323 = -3\*385\*169\*145\*109 mod 323 =-62\*169\*145\*3\*109 mod 323 =-62\*169\*145\*327 mod 323 =-62\*169\*145\*4 mod 323 =-62\*169\*580 mod 323 =

-62\*169\*257 mod 323 =-31\*2\*169\*257 mod 323 =-31\*338\*257 mod 323 =-31\*15\*257 mod 323 =-465\*257 mod 323 = -142\*257 mod 323 = 142\*66 mod 323 = 142\*3\*22 mod 323 = 426\*22 mod 323 = 103\*22 mod 323 = 103\*2\*11 mod 323 = 206\*11 mod 323 = - 117\*11 mod 323 = -318 mod 323 = 5 =M

**Task 4. (7.5 points)** What is the result of DES Expansion/Permutation of R0=0x1921abbf in hexadecimal? Explain your answer

**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 |

In binary:

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

Result of E/P:

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

Result in hexadecimal: 0x8f2903d57dfe