**QUIZ1 CMSE-512 25.03.2024, 16.30 (90 min, 2 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 | 0.5 | 0.5 | 0.5 | 0.5 | 2 |

**Task 1. (0.5 points)** What is the data-oriented access control? What three models of data-oriented access control do you know? Give a particular example of each of them for three users and three objects.

Data-oriented control concerns granting/revoking users’ privileges on data access. Three models are access control matrix, access control lists, and capability lists.

1. Access control matrix:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Obj1 | Obj2 | Obj3 |
| User1 | wr | e |  |
| User2 | wre | r | E |
| User3 | R | wr | r |

1. Access control list:

ACL=>Obj1=>(U1 wr)=>(U2 wre)=>(U3 r)

Obj2=>(U1e)=>(U2 r)=>(U3 wr)

Obj3=>(U2 e)=>(U3 r)

1. Capability list:

CL->U1=>(Obj1 wr)=>(Obj2 e)

U2->(Obj1 wre)=>(Obj2 r)=>(Obj3 e)

U3=>(Obj1 r)=>(Obj2 wr)=>(Obj3 r)

**Task 2. (0.5 points)** What three strategies of password selection do you know? Explain the essence of each.

1. Passwords generated meet some rules, e.g. have at least 8 alpha-numeric symbols
2. Automatic password generation by a system
3. User chooses a password and a system checks its strength

**Task 3. (0.5 points)** Define an RSA private/public key pair for N=143 and check their correctness. Encrypt and decrypt *M=4* 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

N=143=p\*q=13\*11=>p=13, q=11. E\*d=1 mod fi(N); fi(p\*q)=(p-1)(q-1)=12\*10=120;

Let e=7, then d=e^(-1) mod 120

Find d by Extended Euclid Algorithm:

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

Q=floor(120/7)=floor(17+1/7)=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 it: e\*d=7\*103=721 = 6\*120+1 mod 120 =1

C=4^7 mod 143

4^2=16

4^4=16\*16 mod 143 = 256 mod 143 = 113

C= 4^7 = 4^4\*4^2\*4=113\*16\*4 mod 143 = -30\*16\*4 mod 143 =-120\*16 mod 143 = 23\*16 mod 143 = 23\*8\*2 mod 143 – 184\*2 mod 143 = 41\*2 mod 143 = 82

Decryption:

M’=C^103 mod 143=82^103 mod 143

103=64+32+4+2+1

82^103=82^64\*82^32\*82^4\*82^2\*82

82^2=82\*82=82\*2\*41=164\*41 mod 143 = 21\*41 mod 143 = 3\*7\*41 mod 143 = 3\*287 mod 143 = 3\*1=3

82^4=3\*3=9

82^8=9\*9=81

82^16=81\*81=81\*3\*27=243\*27 mod 143 = 100\*27 mod 143 = 2\*50\*3\*9 mod 143 = 2\*150\*9 mod 143 = 2\*7\*9 mod 143 = 126

82^32 = 126\*126 mod 143 = (-17)\*(-17) mod 143 = 289 mod 143 = 3

82^64 = 3\*3 = 9

82^103 = 9\*3\*9\*3\*82 mod 143 = 81\*9\*82 mod 143 = 243\*246 mod 143 = 100\*103 mod 143 = 50\*206 mod 143 = 50\*63 mod 143 = 25\*126 mod 143 = -25\*17 mod 143 = -250 -175 mod 143 = -107 -32 mod 143 = -139 mod 143 = 4 = M, thus, our decryption is correct.

**Task 4. (0.5 points)** What is the result of PC-1 if the DES master key in hexadecimal is k=0xabc3443215678cab. Explain your answer

**Hint**:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Permuted Choice 1 (PC-1) | |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  |  |  |  |  |  |  |  |  | |  | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | |  | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | |  | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | |  | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | |  | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | |  | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | |  | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | |  | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | |
| 57 49 41 33 25 17 9  1 58 50 42 34 26 18  10 2 59 51 43 35 27  19 11 3 60 52 44 36 |
| 63 55 47 39 31 23 15  7 62 54 46 38 30 22  14 6 61 53 45 37 29  21 13 5 28 20 12 4 |

k=0xabc3443215678cab in binary is

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

Result of PC-1 in binary is

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

Result of PC-1 in hexadecimal is 0xc326a91ab74c18