**MT Exam CMSE-512 30.04.2025, 16.30 (100 min, 100 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 5 questions, 6 pages**

Good Luck!

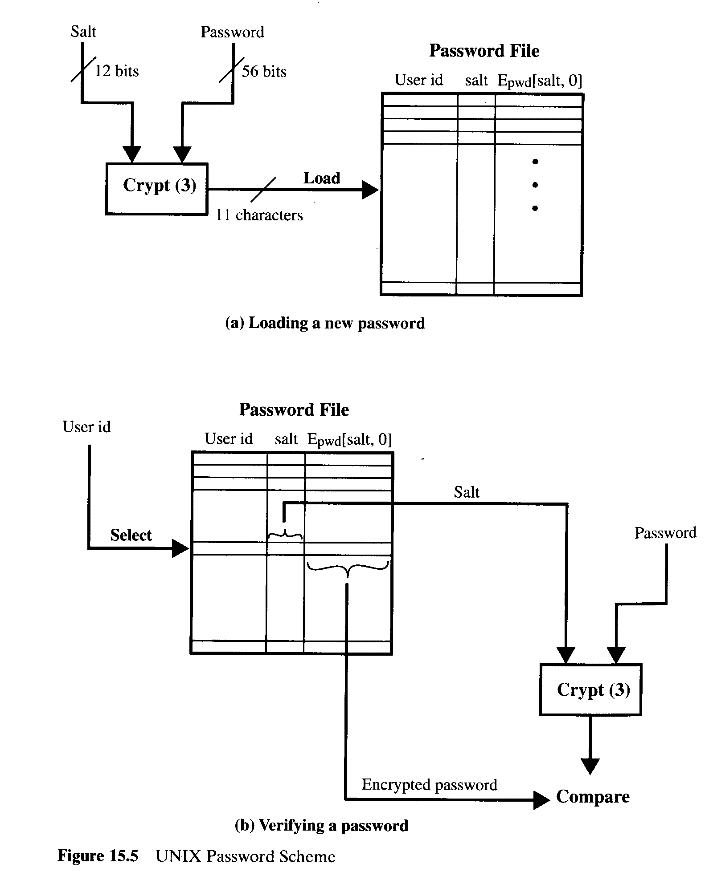
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Name Surname | T1 | T2 | T3 | T4 | T5 | Total |
| Point | 20 | 20 | 20 | 20 | 20 | 100 |
| Grade |  |  |  |  |  |  |

**Task 1. (20 points)** What is the data-oriented access control? What are the three models of data-oriented access control? Explain briefly each of them.

Data-oriented access control is the control of authorizations of the valid users of a system. Three models are access control matrix (ACM), access control list (ACL), and capability list (CL). ACM is a static matrix rows of which are labelled by subjects (users, active processes), and columns by passive objects (files, documents, other resources). On the cross of a row labelled by U and column labelled by R, access rights of U with respect to R are specified. ACL is a column view linked list implementation of ACM where for each object respective subjects with their privileges are specified. CL is a row view linked list implementation of ACM where for each subject respective accessible objects are specified together with the access rights to them.

**Task 2. (20 points)**  How DES algorithm is used in UNIX for the password protection by encryption with “salt”? What is encrypted? What encryption key is used? How the encrypted password is used for a user authentication?

Hints:



DES algorithm is used to generate “encrypted” password by 25 consecutive encryptions of 64-bit block of zeros using the password as an encryption key. The “salt” is used to permute outputs of each of the encryption before feeding them as inputs to the encryption step. A user is authenticated by re-generating the “encrypted” password together with the “salt” and comparing it versus the “encrypted” password of the user from the password file.

**Task 3. (20 points)** Define an RSA private/public key pair for some and check their correctness. Encrypt and decrypt *M=9* with RSA using the keys. Show details of 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.

In calculations use binary decomposition of an exponent (e.g. 23 = 16+4+2+1), successive squaring to get exponents of power of 2 (e.g. 2^16 =( ((2^2)^2)^2)^2, and immediate modulo reduction: a\*b mod N = ((a mod N)\*(b mod N)) mod N.

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=187 = p\*q => p=11, q=17, fi(N) = (p-1)\*(q-1) = 10\*16 = 160

Let e = 7, then d = e^(-1) mod fi(N). Use EEA to find d:

1. A = (1,0,160), B = (0,1, 7)

Q= floor(160/7) = 22

T = A – q\*B = (1-22\*0, 0 – 22\*1, 160 – 22\*7) = (1,-22, 6)

A = B = (0,1,7), B = (1, -22, 6)

1. Q = floor(7/6) =1

T = A – q\*B = (0 – 1\*1, 1 – 1\*(-22), 7 – 1\*6) = (-1,23, 1)

B3= 1 => d = B2 = 23

Check it: e\*d = 7\*23 = 161 mod 160 = 1, it’s OK

Encryption: C = M^e mod N = 9^7 mod 187. Use binary decomposition and successive squaring to find C: 7 = 4 + 2 +1

9^2 = 81 mod 187 = 81

9^4 = 81\*81 mod 187 = 81\*3\*27 mod 187 = 243\*27 mod 187 = 56\*27 mod 187 = 56\*3\*9 mod 187 = 168\*9 mod 187 = -19\*9 mod 187 = - 171 mod 187 = 16

9^7 mod 187 = 9^4\*9\*2\*9 mod 187 = 16\*81\*9 mod 187 = 16\*243\*3 mod 187 = 16\*56\*3 mod 187 = 16\*168 mod 187 = -16\*19 mod 187 = -2\*152 mod 187 = 2\*35 mod 187 = 70

Decryption: M’ = C^d mod N = 70^23 mod 187

23 = 16 + 4 +2 +1

70^2 = 70\*70 mod 187 = 70\*2\*35 mod 187 = 140\*35 mod 187 = -47\*35 mod 187 = -47\*5\*7 mod 187 = -235\*7 mod 187 = -48\*7 mod 187 = -2\*24\*7 mod 187 = -2\*168 mod 187 = 2\*19 mod 187 = 38

70^4 = 38\*38 mod 187 = 361\*4 mod 187 = 174\*4 mod 187 = -13\*4 mod 187 = -52

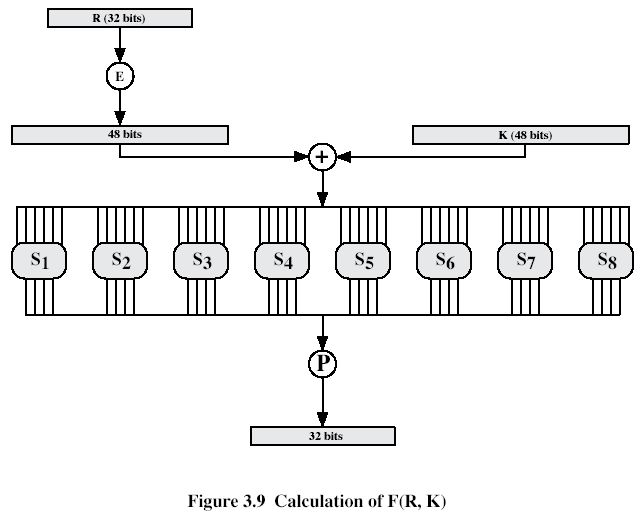
70^8 = 52\*52 mod 187 = 52\*4\*13 mod 187 = 208\*13 mod 187 = 21\*13 mod 187 = 273 mod 187 = 86

70^16 = 86\*86 mod 187 = 86\*2\*43 mod 187 = 172\*43 mod 187 = -15\*43 mod 187 = -3\*5\*43 mod 187 = -3\*215 mod 187 = -3\*28 = -84

70^23 = 70^16\*70^4\*70^2\*70 mod 187 = 84\*52\*38\*70 mod 187 = 168\*26\*38\*70 mod 187 = -19\*26\*38\*70 mod 187 = -19\*26\*19\*2\*70 mod 187 = -19\*26\*19\*140 mod 187 = 19\*26\*19\*47 mod 187 = 361\*26\*47 mod 187 = 174\*26\*47 mod 187 = -13\*26\*47 mod 187 = -13\*13\*2\*47 mod 187 = -169\*94 mod 187 = 18\*94 mod 187 = 9\*2\*94 mod 187 = 9\*188 mod 187 = 9\*1 mod 187 = 9 = M, thus, decryption is correct

**Task 4. (20 points)** What is the output of the S-box S3 in binary if the 48-bit input to S-boxes is R0=0x921abcbd01fa in hexadecimal? Explain your answer

**Hint**:



S-box S3:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10 | 0 | 9 | 14 | 6 | 3 | 15 | 5 | 1 | 13 | 12 | 7 | 11 | 4 | 2 | 8 |
| 13 | 7 | 0 | 9 | 3 | 4 | 6 | 10 | 2 | 8 | 5 | 14 | 12 | 11 | 15 | 1 |
| 13 | 6 | 4 | 9 | 8 | 15 | 3 | 0 | 11 | 1 | 2 | 12 | 5 | 10 | 14 | 7 |
| 1 | 10 | 13 | 0 | 6 | 9 | 8 | 7 | 4 | 15 | 14 | 3 | 11 | 5 | 2 | 12 |

|  |  |  |
| --- | --- | --- |
| 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 |

R0=0x921abcbd01fa = 1001 0010 0001 1010 1011 1100 1011 1101 0000 0001 1111 1010

Each box gets 6 bits:

100100 100001 101010 111100 101111 010000 000111 111010

Box S3 gets 101010 = 1 0101 0. Two end bits, 10, define the row number, 2, and the 4 middle bits, 0101, define the column number, 5. On the cross of row 2 and column in S3 we find 15 that is 1111 in binary.

**Task 5. (20 points)**

For x = 0x123455 in hexadecimal calculate



where



Provide details of your calculations, give explanations

x = 0x123455 = 0001 0010 0011 0100 0101 0101

ROTR1(x) = 1000 1001 0001 1010 0010 1010

ROTR8(x) = 0101 0101 0001 0010 0011 0100

SHR7(x) = 0000 0000 0010 0100 0110 1000

1101 1100 0010 1100 0111 0110 = 0xdc2c76