**MT Exam CMSE-512 15.05.2023, 18.30, CMPE-128 (100 min, 30 points)**

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

**ThreeA4-sized sheets of paper with your handwritten notes may be used. Calculators are allowed. Other electronic devices are not allowed**

Instructor Alexander Chefranov

**Totally 6 questions, 6 pages**

Good Luck!

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | T1 | T2 | T3 | T4 | ~~T5~~ | T6 | Total | Ultimate out of |
| Point | 5 | 5 | 5 | 5 | ~~5~~ | 5 | 25 | 30 |

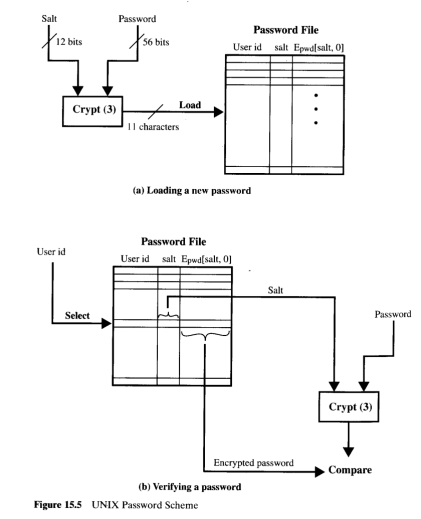
**Task 5 hint was not provided in full, hence, it is cancelled**

**Task 1. (5 points)** What is the “integrity” security requirement? How it can be attacked?

Integrity requirement is that only authorized users can alter system data. It can be attacked by getting unauthorized access and altering the data.

**Task 2. (5 points)** What data structure is used for the password keeping in Linux? Explain each field of the structure. How a password entered is verified?

**Hint**:



The data structure used according to the figure above is: User\_id, salt, Epwd[salt,0]. User\_id specifies a user, salt is a 12-bit string used to modify the original password provided by a user, Epwd[salt,0] is the result of encryption of the zero-valued data-block using the user’s pwd as a key and salt for its modification. A password entered is verified by comparing Epwd[salt,0] kept in the password file versus respective recalculated value using the salt from the password file and password entered.

**Task 3. (5 points)** Define an RSA private/public key pair using numbers *p=5* and *q=17* and check their correctness. Encrypt and decrypt *M=6* 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=p\*q=5\*17=85, fi(N)=(p-1)\*(q-1)=4\*16=64. Let d=3, then e=d^(-1) mod 64

Use EEA:

A=(1,0,64), B=(0,1,3)

Q=floor(64/3)=21

T=A-q\*B=(1-21\*0,0-21\*1, 64-21\*3)=(1,-21, 1)

A=(0,1,3), B=(1,-21,1)

New B3= 1, hence, 3^(-1) mod 64=B2=-21 mod 64 = 43. Check it: 43\*3=129=1 mod 64

Thus, e=43

Encryption:

C=M^e mod N= 6^19 mod 85 =>

6^2 mod 85 = 36

6^4 mod 85 = 36^2 mod 85 = 21

6^8 mod 85 = 21^2 mod 85 = 16

6^16 mod 85 = 16^2 mod 85 = 1

6^32 mod 85 = 1^2 mod 85 = 1

C= 6^43 mod 85 = 6^32\*6^8\*6^2\*6 mod 85 = 1\*16\*36\*6 mod 85 =96\*36 mod 85 = 11\*36 mod 85 = 198\*2 mod 85 = 28\*2 mod 85 = 56

Decryption:

M’=C^d mod N = 56^3 mod 85=>

56^2 mod 85 = 112\*28 mod 85 = 27\*28 mod 85 = 9\*84 mod 85 =9\*(-1) mod 85 = -9 mod 85 = 76

M’=C^2\*C mod N = 76\*56 mod 85 = -9\*56 mod 85 =-3\*168 mod 85 =-3\*(-2)mod 85 =6 = M, hence, decryption is correct.

**Task 4. (5 points)** What is the output of the S-box S2 if the result of the addition of the E output with the round key is 0x123456789abc. Explain your answer

**Hints**:

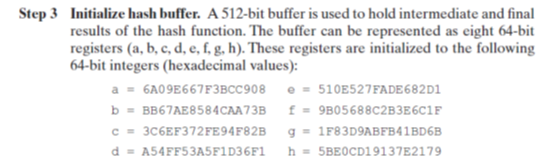




The result of addition in binary is 0x123456789abc = 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100. The input to S2 is the 2nd group of six bits: 10 0011. The two end bits, 11, define the row number 3, and the four middle bits, 0001, define the column number 1, on the cross of which we find 8, that is 1000 in binary, the output of S2.

**~~Task 5. (5 points)~~** ~~Prove by direct calculation that the first three hexadecimal digits of the initial value of the SHA-512 register~~ *~~a~~* ~~are actually ‘6A0’. Show results of your calculations, give necessary explanations.~~

**Hints**:



**Task 6. (5 points)** Explain PayPal protocol: Who are the actors of the protocol? Who initiates the protocol? How money is transferred? How sensitive credit card information is protected from disclosing?

The actors are Monery\_sender, Money\_receiver, and PayPal server. The protocol is initiated by Money\_sender willing to transfer money. Money is transferred by telling PayPal amount and e-mail of the receiver; actual transfer is made by PayPal. Sensitive credit card information is not transferred in the transactions as it is stored by PayPal in the registration process, and the customers are identified by their e-mail addresses.