**QUIZ1 CMSE-512 10.05.2023, 16.30 (100 min, 2 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!

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| # | StId | Name Surname | Question | T1 | T2 | T3 | T4 | T5 | T6 | Total |
|  |  |  | Point | 0.3 | 0.3 | 0.4 | 0.4 | 0.3 | 0.3 | 2 |
| 1 | 22501468 | Hamidreza Rahimi |  | 0.2 | 0.2 | 0.3 | 0.35 | 0.1 | 0.1 | 1.25 |
| 2 | 22600290 | Nada Kollah |  | 0.2 | 0.2 | 0.4 | 0.4 | 0.3 | 0.25 | 1.75 |
| 3 | 20620220 | Mahmut Sevince |  | 0.2 | 0.2 | 0.4 | 0.05 | 0.05 | 0.1 | 1 |
| 4 | 22501703 | M. Nasser Barakat |  | 0.2 | 0.2 | 0.4 | 0.4 | 0.3 | 0.3 | 1.8 |
| 5 | 22500679 | Amin Safarzadeh |  | 0 | 0.05 | 0.15 | 0.4 | 0 | 0 | 0.6 |
| 6 | 22500558 | Malek Al Khatib |  | 0.3 | 0.3 | 0.4 | 0.4 | 0.3 | 0.15 | 1.85 |
| 7 | 21506656 | Farzaneh Nasirzadeh |  | 0.1 | 0.25 | 0.25 | 0.2 | 0.1 | 0.05 | 0.95 |

**Task 1. (0.3 points)** What is the “anonymity” security requirement? How it can be attacked?

The anonymity requirement assumes that the user network activity can’t be traced back to his/her identity. It can be attacked by the analysis of the user activities altogether that allows tracing back the packets sent by the user.

**Task 2. (0.3 points)** How the “salt” is used in the Crypt(3) function of the Unix password schema shown below:



The “salt” is used to define a permutation of the ciphertexts obtained in the course of iterative DES encryptions used by Crypt(3).

**Task 3. (0.4 points)** Define an RSA private/public key pair using numbers *p=7* and *q=19* 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=p\*q=7\*19=133, fi(N)=(p-1)\*(q-1)=6\*18=108

Let e=5, then d=e^(-1) mod 108, find it by EEA:

A=(1,0,108), B=(0,1,5)

Q=floor(108/5)=21

T=A-q\*B=(1-21\*0,0-21\*1,108-21\*5)=(1,-21,3)

A=(0,1,5), B=(1,-21,3)

Q=floor(5/3)=1

T=A-q\*B=(-1,22,2)

A=(1,-21,3), B=(-1,22,2)

Q=floor(3/2)=1

T=A-q\*B=(2,-43,1)

A=(-1,22,2), B=(2,-43,1)

B3=1=>B2=-43 mod 108=65=d

Check it: 5\*65=325=3\*108+1 mod 108 =1

Encryption: C=M^e mod N= 4^5 mod 133

4^2 mod 133 = 16

4^4 mod 133 = 256 mod 133 = 123

4^5 mod 133 = 123\*4 mod 133 = 246\*2 mod 133 = 113\*2 mod 133 = 226 mod 133 = 93

Decryption:M’=C^d mod N = 93^65 mod 133

93^2 mod 133 =4

93^4 mod 133 = 16

93^8 mod 133 =123

93^16 mod 133 = 123^2 mod 133 = 100

93^32 mod 133 = 100^2 mod 133 = 25

93^64 mod 133 = 25^2 mod 133 = 125\*5 mod 133 = -8\*5=-40 mod 133 =93

93^65 mod 133 = 93^64\*93 mod 133 = 93\*93 mod 133 = 4 = M, that is decryption is correct.

**Task 4. (0.4 points)** What is the result of PC-1 if the DES master key in hexadecimal is k=0x1122334455aabbe0. Explain your answer

**Hint**:

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

|  |
| --- |
| Permuted Choice 1 (PC-1) |
| 57 49 41 33 25 17 91 58 50 42 34 26 1810 2 59 51 43 35 2719 11 3 60 52 44 36 |
| 63 55 47 39 31 23 157 62 54 46 38 30 2214 6 61 53 45 37 2921 13 5 28 20 12 4 |

 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Row\col | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 2 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 3 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| 4 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| 5 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 6 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 7 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 |
| 8 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |

The key in binary as an 8x8 matrix |

Result of PC-1 as an 8x7 binary matrix:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Row\col | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 2 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| 3 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 4 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |
| 5 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| 6 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| 7 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |

Result in hexadecimal is 0xe098e656618605

**Task 5. (0.3 points)** Explain how 64-bit registers *a,b,c,d,e,f,g,h* are initialized in SHA-512. Why the initialization is required? What number is used to initialize the register *c*?

Hints:



The registers are initialized by taking the senior 64 bits of the fractional part of the square root of the first eight prime numbers. The initialization is required because there is no previous elementary hash function for the first one in the chain of them. To initialize c, the 3rd prime number is used that is 5.

**Task 6. (0.3 points)** Explain SSL protocol: Who are the actors in the protocol? Who initiates the protocol? Who generates a session key? How the session key is protected from eavesdropping?

**Hints:**

“Assume that a browser, C, connects to a server, S, that claims to represent a particular enterprise, E (for example, Macy’s). In this case, the protocol consists of the following steps:

1. S sends C a copy of its certificate signed by the CA – in the clear
2. C validates the certificate’s signature using the CA’s public key (included in its browser) and hence knows that the public key in the certificate belongs to the enterprise named in the certificate.
3. C generates and sends to S a session key encrypted with the public key in the certificate.”

The actors are: Client and Server. Client initiates the protocol. Client generates the session key. Session key is protected from eavesdropping by encryption with the Server’s public key.