**Midterm Exam CMPE-552 25.11.2021, 16.30 (100 min, 30 points)**

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

**One sheet of paper with your notes and a calculator may be used. Electronic devices are not allowed**

Instructor Alexander Chefranov

**Totally 4 questions, 6 pages**

Good Luck!

**Task 1. (7.5 points)** What masquerade attack is? What security requirements might be violated in the result of masquerade attack? How masquerade attack is conducted? Explain your answers

In masquerade attack, an intruder impersonates a valid user to get access to the victim system. In the result of masquerade attack intruder gets access to a system violating authentication, on getting access he can get read access to secret documents violating confidentiality, modify data violating integrity, and data modification can cause violating availability (valid password changed to a new one not known to the legitimate user). A masquerade attack can be conducted by stealing password of a legitimate user.

**Task 2. (7.5 points)**  Let N=p\*q=221. Define an RSA private/public key pair 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=221=p\*q=13\*17=> p=13, q=17

Fi(N)=(p-1)\*(q-1)=12\*16=192

Let e=5, then e^(-1) mod fi(N)= 5^(-1) mod 192 =b=?

A=(A1,A2,A3)=(1,0,192), B=(b1,b2,b3)=(0,1,5)

Q=floor(192/5)=38

T=(t1,t2,t3)A-q\*B=(1-38\*0, 0-38\*1, 192-38\*5)=(-38,0,2)

A=B=(0,1,5), B=T=(1,-38,2)

Q=floor(5/2)=2

T=A-q\*B=(0-2\*1, 1-2\*(-38), 5-2\*2)=(-2, 77, 1)

A=B=(1,-38,2), B=T=(-2, 77, 1)

B3==1 yes => b2=77=d=5^(-1) mod 192

Check it by multiplication: 5\*77 mod 192 = 385 mod 192 =( 2\*192+1) mod 192 = 1

Then C=M^e mod N= 6^5 mod 221 = 216\*36 mod 221 = -5\*36 mod 221 =- 180 mod 221 = 41

Decryption: M’=C^d mod N = 41^77 mod 221 =

41^2 mod 221 = 134

41^4 mod 221 = 55

41^8 mod 221 = 152

41^16 mod 221 =120

41^32 mod 221 =35

41^64 mod 221 = 120

M\=41^77 = 41^(64+8+4+1) mod 221= 31^64\*31^8\*31^4\*31 mod 221= 1\*118\*183\*31 mod 221 = 157\*31 mod 221 = 5=M, hence, decryption is correct

**Task 3. (7.5 points)** Assuming 8-bit registers used in MD5 a=2, b=3, c=1, d=2 s=3, X[k]=2, T[i]=3, what is new c value after the first two steps of the 1st round of such MD5 modification? Show you calculations, explain your answer

Hints:

Each round consists of a sequence of 16 steps operating on the buffer ABCD. Each step is of the form



Where

*a,b,c,d* – the four words of the buffer, in a specified order that varies across steps

*g* – one of the primitive functions F,G,H,I

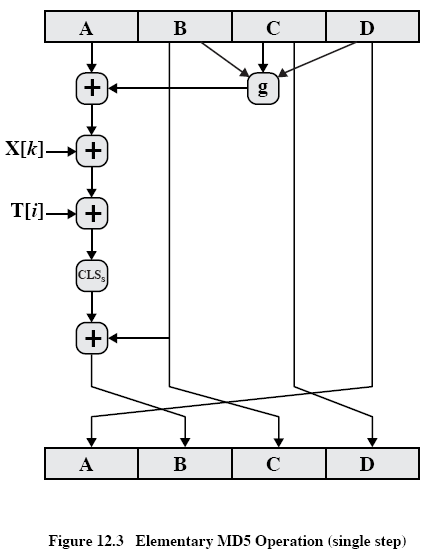
*<<<s* – circular left shift (rotation) of the 32-bit argument by *s* bits

*X[k] – M[q**16+k] – k*-th 32-bit word in the *q*-th 512-bit of the message

*T[i]* – the *i*-th 32-bit word in matrix *T*

+ - addition modulo 

Figure 12.3 illustrates the step operation



F(b,c,d)=

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Bit# | b | c | d | F(b,c,d) |
| 0 | 1 | 1 | 0 | 1 |
| 1 | 1 | 0 | 1 | 0 |
| 2 | 0 | 0 | 0 | 0 |

F(b,cd)=1

a+F(b,c,d)=2+1=3

a+F(b,c,d)+X[k]=3+2=5

a+F(b,c,d)+X[k]+T[i]=5+3=8=00001000

a1=(a+F(b,c,d)+X[k]+T[i])<<<s= 8<<<3=64

After the 1st step shifting of registers is made: b1=a1=64, c1=b=3, d1=c=1, a1=d=2

After the 2nd step, new a1 will be calculated on the base of the original d, and again shifting of registers is made so that c2=b1=64

Answer: register c after the 2nd step of the 1st round is 64.

**Task 4. (7.5 points)** Propose a way of ~~invocation~~ invoking of a parasitic virus living in an executable file so that it is activated without human participation.

A parasitic virus living in exe-file can be invoked automatically if placed into start-up folder