**QUIZ1 CMPE-552 21.11.2016 (75 min, 2 points)**

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

**One sheet of paper with your handwritings may be used. Photocopies, printouts, telephones, caclulators, etc, are not allowed**

Instructor Alexander Chefranov

**Totally 3 questions, 4 pages**

Good Luck!

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | Total |
|  |  |  |  |

**Task 1. (0.6 points)** What replay attack is? Explain how it is conducted. What might be the aim of the replay attack?

Replay attack is conducted by intercepting valid network messages and repeating them by an opponent. A replay attack may aim masquerading, i.e. impersonating some person by some other person by e.g. the use of intercepted password

**Task 2. (0.7 points)** Define an RSA private/public key pair using numbers *p* and *q* from [5,10]. Encrypt and decrypt *M=21* 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

p=5, q=7, N=35, fi(N)=(p-1)(q-1)=24; e=7, gcd(24,7)=gcd(7,3)=gcd(3,1)=gcd(1,0)=1 => 24 and 7 are relatively prime. D=e-1mod24

A=(1,0,24), B=(0,1,7), Q=3, T=A-QB=(1,-3,3)

A=(0,1,7), B=(1,-3,3), Q=2, T=A-QB=(-2,7,1) =>d=7

Check: 7\*7=49mod24=1

C=M7=217mod35=212\*214\*21=21

212=441mod35=35\*12+21=21

214=212=21mod35

P=C7=217=21mod35

**Task 3. (0.7 points)** Consider Steps 1, 2 of the Kerberos protocol:

1. C sends to KDS a message, M1 (in the clear), requesting a ticket to be used to authenticate C to S. M1 contains the names of the intended communicants (C,S).
2. When KDS receives M1, the following takes place:

(a) KDS (randomly) constructs a session key, Ksess,C&S

(b) KDS sends to C a message, M2, containing two items:

(i) [Ksess,C&S, S, LT]

(ii)  [Ksess,C&S, C, LT] – the actual ticket,

where LT is the lifetime (the time interval) over which the ticket is valid.

Answer the following questions:

1. Why in Kerberos protocol, a client, C, can decrypt part (i) of the message obtained in the Step 2, and cannot decrypt part (ii)?

C can decrypt part(i) because it is encrypted with the key KC,KDS shared by C and KDS

C cannot decrypt part (ii) because it is encrypted by a key KS,KDS not known to C

1. What information is kept in these parts, (i) and (ii)?

In part (i): Ksess,C&S, server name S, and lifetime LT

In part (ii): Ksess,C&S, client name C, and lifetime LT

1. What for part (i) is used by C?

Part (i) is used by C to get the session key, Ksess, C&S, and encrypt by it a request to S

1. What for part (ii) is used by C?

Part (ii) is used by C to transmit it to the server S as a ticket for a service request