**QUIZ CMPE-552 13.01.2017 (90 min, 100 points)**

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

**Calculators are allowed. Two A4 sheets of paper with your handwritings may be used for your help (printouts, photocopies, etc. are not allowed). Electronic devices are not allowed.**

Instructor Alexander Chefranov

**Task 1. (20 points)** Assume N=35. Define a redundancy predicate for checking validity of a serial number, and generate a valid serial number. Check its validity. Using RSA, define a bank’s private and public keys, blind the serial number, get blinded token (signed by the bank blinded serial number), un-blind it (signed by the bank serial number), and get back the serial number. Show your calculations.

If N=35, then N=p\*q=7\*5, p=7, q=5, ed=1modfi(N); fi(N)=(p-1)(q-1)=6\*4=24

E=5, gcd(e, fi(N))=gcd(5,24)=1

D=e: ed=25mod24=1. Let public key, P=e=5, and private key, R=d=5

Redundancy predicate p(n)=(n mod 5==3). Let n=18 then p(18)=(18mod5==3)=TRUE, hence, n=18 is a valid serial number

For blinding, select u=6, gcd(u,N)=gcd(6,35)=1, u-1mod35=6

B(n)=RSAP(u)\*nmodN=65\*18mod35=6\*18mod35=108mod35=3

The bank encrypts B(n) with its private key, R,

S=RSAR(b(n))=35mod35=33

The client un-blinds blinded serial:

Token=u-1\*SmodN=6\*33mod35=198mod35=23

Serial number, n, is obtained by decrypting Token with the public key, P,

n’=RSAP(Token)=235mod35=18=n

We see, n’=n

**Task 2. (20 points)** What encryption method and what key are used in the XML code below:

<PaymentInfo xmlns = “<http://...>”>

 <Name> Hasan Eren </Name>

 <EncryptedData Type =

“

[http://www.w3.org/2001/04/xmlenc#Element”](http://www.w3.org/2001/04/xmlenc#Element\”  )

xmlns=”[http://www.w3.org/2001/04/xmlenc#](http://www.w3.org/2001/04/xmlenc)”/>

<EncryptionMethod Algorithm =

“[http://www.w3.org/2001/04/xmlenc#aes-ctr”/](http://www.w3.org/2001/04/xmlenc#aes-ctr)>

 <ds:KeyInfo xmlns:ds =

“[http://www.w3.org/2000/09/xmldsig#](http://www.w3.org/2000/09/xmldsig)“>

 <ds:KeyName> Secret1 </ds:KeyName>

 </ds:KeyInfo>

 <CipherData>

 <CipherValue>Zx23XAbc4..</CipherValue>

 </CipherData>

 </EncryptedData>

</PaymentInfo>

Give necessary explanations.

The cipher used is AES in Counter mode as it is specified in the EncryptionMethod element’s attribute, Algorithm. The key used is define in the element Ds:KeyName as Secret1 which specifies name of the key, not the key value.

**Task 3. (20 points)** What for certificates are used? How they are validated? How to certificates can be validated by two communicating parties in the case when they have certificates from two different certificate authorities? What means are provided in X.509 to support such mutual certificate validation?

Certificates are used to make known in a trusted way a public key of a subject. Certificates are validated by checking signature of the certificate authority, validity period, and absence of the certificate in the certificate revocation lists issued by the certificate authority.

To validate certificate issued by another certificate authority, public key of which is not known in a trusted way, it is necessary to build a certificate path starting from a certificate authority, public key of which is known in a trusted, to the certificate under the question.

X.509 provides a hierarchical directory where certificate authorities exchanged by certificates are represented together with subjects to whom the certificates authorities issued certificates.

**Task 4. (20 points)** What for the function f2 is used in simple protected authentication procedures illustrated by Fig. 2 below? How this authentication procedure counters replay attacks? Give necessary explanations



The function f2 is used for creation of the authenticator, Protected2. It uses three inputs, one of them is an output of f1.

The authentication procedure counters replay attacks by the use of time-stamps, t, and nonces, q, that they are created again for each new authentication.

**Task 5. (20 points)** Consider Lamport’s One-time password scheme below.

# Initialization Procedure

The client selects a password, , a number, , calculates

,

where

.

The client securely delivers to the server (, and the servers saves it into () tuple.

# Authentication Procedure

When the client, C, requests authentication by the server, S, the following proceeds:

1. C -> S: C\_ID //client sends his ID

2. S -> C: Counter(C\_ID) //server responds by respective Counter value

3. C -> S: C\_ID, 

4. S: If  then {

 S authenticates C, and sets ()=()

 }

 Else C is not authenticated

Assume that the client, A, specified N=5, p0=1, h(x)=(7\*x+1)2mod11. Show

1. Initial record of A
2. Record of A after the first successful authentication

Give necessary explanations

pwd5=H5(p0)= H4(h(p0))= H4(h(1))= H3(h(9))= H2(h(4))= H(h(5))=h(9)=4

h(1)=(7\*1+1)2mod11=64mod11=9

h2(1)=h(h(1))=h(9)=(7\*9+1)2mod11=642mod11=92mod11=4

h3(1)=h(h2(1))=h(4)=(7\*4+1)2mod11=292mod11=72mod11=5

h4(1)=h(h3(1))=h(5)=(7\*5+1)2mod11=32mod11=9

h5(1)=h(h4(1))=h(9)=(7\*9+1)2mod11=642mod11=81mod11=4

Initial record is (N, pwdN,ID)=(5,4,A)

In the first authentication, A responds by pwd4=h4(p0)= h4(1)=9

User A is authenticated by checking h(pwd4)=h(9)=4==pwd5? Yes

The next record, hence, is (N-1, pwdN-1, A)=(4,9,A)