**Nova Southeastern University**

**College of Computing and Engineering**

**ISEC 620 Applied Cryptography**

**Fall 2020**

**(August 17 – December 6, 2020)**

Written Assignment #3

Date: November 1, 2020

Instructor: Dr. Junping Sun

* List ways in which secret keys can be distributed to two communicating parties. (10 points)

The first way is a key can be chosen by party A and then delivered physically to party B.

The second way is a third party can be chosen by party A and physically delivered to party B.

The third way is if A and B have both previously used a key, One will then transmit the new key to the other and encrypt it using the previous key.

The fourth way is if a third-party connection from both parties A and B is encrypted. The third party could then deliver a key to parties A and B via its encrypted links.

* What is the difference between a session key and a master key? (5 points)

The difference between a session key and a master key is how it persists.

A session key will be destroyed once the session is terminated; its purpose is to encrypt traffic while in session. A master key will persist to exist even after the session is terminated. It is used between entities to distribute more session keys.

* What is a key distribution center? (5 points)

A Key Distribution Center oversees which systems get to communicate with each other. Also known as a KDC, it will grant a one-time session key for a connection between two parties. Once two parties have been granted permission to talk to each other from the KDC will they be able to establish a secure encrypted connection.

* What are two different uses of public-key cryptography related to key distribution? (5 points)

Public-key cryptography is related to key distribution in the first way by Public Key Encryption. The public key is used to encrypt the message and can only be decrypted with the private key. This establishes confidentiality between two parties by creating an encrypted tunnel blocked from the outside world. The other relation is digital signatures. This is when a message is signed with the private key and can be verified with the public key. This establishes integrity between two parties by proving that the sender is the true creator of the message.

* List four general categories of schemes for the distribution of public keys. (5 points)

-Public Announcement.

This is when parties broadcast their public keys to each other and everyone. This is not secure because any party can forge a public key until the parties are notified of the forged public key.

-Public Available Directory.

This is when a central entity keys records of the public keys between parties.

Both parties A and B will have their public keys stored in a central key authority.

Parties will have to register their public keys to the key authority by secure means and can change them at will. This is thought of as safer than public announcement, but if the private key of the authority is compromised then an attacker could pass public keys for all parties.

-Public Key Authority.

Similar to Public Available Directory above but with tighter control of the distribution of public keys. A request is sent to the authority with a timestamp, the authority returns a message that was encrypted with its private keys so the originator can verify its integrity by using the authorities public key for verification. That encrypted message to the originator from the authority contains the recipient B's public key that can be used to encrypt messages to recipient B. Sender A will then Cache recipient B's public key with an identifier and a nonce value and then proceed to send a message. B will decrypt A's message with B's private key and then send a request to the key authority in the same fashion to obtain the public key for A.

-Public Key Certificates.

In this distribution of public keys both A and B apply to a trusted third party to hold their public keys. These keys are stored in certificates that are digitally signed by the certificate authority. That way the integrity of the certificate can be established.

Recipients are able to encrypt messages back and forth using certificates to obtain each others public keys to encrypt messages.

* What are the essential ingredients of a public-key directory? (10 points)

A Public key directory has a few essential ingredients.

-The first being that an authority should maintain a directory with a name and public key for each

participant.

-Each party needs to register a public key with the authority. The registration needs to be done securely

in person or among other means.

-A party may update their public key within the authority.

-Periodically the authority publishes the entire directory or updates to the directory.

-Parties should be able to access the directory electronically.

7. What are the requirements for the use of a public-key certificate scheme? (10 points)

The public-key certificate scheme has two requirements. The first being that a party can read a certificate and be able to tell the name and public key of the certificate’s owner. The party should also be able to verify the certificates integrity by proving it originated from the authority and the currency of the certificate.

8. What is the purpose of the X.509 standard? (5 points)

The purpose of the X.509 standard is agreeing on the formatting of certificates. They contain an identity and a public key for the party. After the certificate is validated by an authority the public key within the certificate can encrypt messages to the certificates party.

9. What is the chain of certificates? (5 points)

A chain of certificates is a list of certificates and record of how they are connected from the client to the server certificate, to the intermediary certificate, to the Root Certificate Authority. This is done to verify integrity all the way back to the Root Certificate Authority. Each certificate is verified by the public key of the last one. This is done all the way down the chain until reaching the end. The last ticket in the chain is called a trust anchor.

10. How is an X.509 certificate revoked? (5 points)

Revoked Certificates are sent to a Certificate Revocation List called a CRL.

The CRL is signed by the Certificate Authority to verify its identity. When a certificate is no longer valid due to time or any other constraint it will be added to the CRL.

11. Find the prime factorization of 7007. Also describe and show how you find it in step by step. (10 points)

7007

/ \

Step 1. 7 1001

/ \

Step 2. 7 143

/ \

Step 3. 11 13

The above factors a 7007 into multiple prime numbers.

This leaves us with **7,7,11, and 13.**

This can be checked by ((7\*2)\*11\*13) = 7007.

12. Please give the definition of Euler’s Totient function correctly and clearly as well as concisely. (5 points)

Euler’s Totient Function is designed to count the positive integers up to a given integer *n* and that are relatively prime to *n*.The symbol for this function in the Greek Letter Phi and is represented as *ϕ(n).*

When *n* is a prime number, the *ϕ(n)* will always equal *n-1.*

For example, the number 10 would have a *ϕ(4).* This is because its number coprime to *n* are 1,3,7,9.

2,5,6,8 are not options because 2 \*5 =10 so they are not prime, and 2 is a factor of 6, and 8. Leaving behind the only prime numbers of n 1,3,7,and 9.

13. Determine the value (41) and (231). (Note: (*n*) is Euler’s Totient function) (20 points)

*ϕ(41)=40.*

Since the number *n* = 41 and is prime. The *ϕ(n)* will equal *n-1.* In this case it is 40.

*ϕ(231)=120.*

Step 1 - *ϕ(231) = ((ϕ(3) \* ϕ(77)).*

*Since ϕ(3) is prime, ϕ(3) = 2.*

*Step 2 - ϕ(77) = (ϕ(7)) \* ϕ(11)).*

*Since ϕ(7) and ϕ(11) are prime, ϕ(7) = 6 and ϕ(11) = 10.*

*Step 3 – Multiply all, (2 \* 6 \* 10) = 120.*

14. What is the difference between an index and a discrete logarithm? (5 point

In Public Key Infrastructure discrete logarithms base their security on that assumption that their chosen groups don’t have an efficient solution and are hard to obtain by basing groups.

The discrete in discrete logarithm refers to that work is performed in discrete groups that aren’t real numbers but are cyclic groups of generators. In an index the exponent is an integer which is a real number. The key difference with discrete using non real numbers and index using real ones.

15. Describe in general terms an efficient procedure (step by step) for picking a prime number. (15 points)

Picking a prime number goes as follows:

Step 1: Pick an odd integer *a* at random as best as possible using a good random number generator.

Step 2: Pick an integer *b* so that *b<a* at random.

Step 3: Perform probabilistic primality tests.

IF (*a* fails on first test)

Go back to Step 1.

IF (*a* pass enough tests.) // Test are determined on how well you want it to perform.

Accept A as prime number.//Fin.

Else

Go back to step 2.

16. What are the principal elements of a public-key cryptosystem? (10 points)

First element: Choosing logic to make asymmetric keys.

Second element: Choosing logic to encrypt message with recipient’s public key.

Third element: Choosing logic to decrypt message with recipient’s private key.

Fourth element: A way to publish the public keys.

Fifth element: A way to authenticate that the public key belongs to its creator.

17. What are the roles of the public and private key? (10 points)

Public and Private keys are generated asymmetric key pairs that play very different roles.

The sender will use the receiver’s public key to encrypt messages to be sent to said receiver, that receiver of the encrypted message will decrypt it using their own private key because it was encrypted using their public key. So, in this case public keys are for encryption while private keys are for decryption. Also, private keys are used for creating digital signatures while public keys are used to authenticate the sender is who they say they are by means of those digital signatures on encrypted messages.

18. Perform encryption/decryption for the following given conditions by using RSA algorithm in Figure 9.6 of the textbook. (25 points)

*p* = 3; *q* =11; *e* = 7; *M* = 5;

Public Key: {*7, 33*}

Private Key: {*3,33*}

Encryption : C = Me mod n = 57 mod 33 = *14*

Decryption : M = Cd mod n = 143  mod 33 = *5*

Since n = p \* q.

Let **n = 33**. (3\*11)

Since *ϕ(n)*= (p-1) \* (q-1)

Let *ϕ(n)*= (2 \* 10) => ***ϕ(n)* = 20.**

By using the backward substitution of GCD algorithm we need to compute *d = e-1 mod ϕ(n)*

From *GCD(ϕ(n), e),*

Let *GCD(20,7) = 1,*

Hence *d \* e mod ϕ(n) = 1,*

*So* that, *7d mod 20 = 1,*

***Leaving d=3.***

*Public key pu = (e,n)*

*Private key pr = (d,n)*

*So that*

***Pu = (7,33)***

***Pr = (3,33)***