**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 encyrpt 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 to to encrypt traffic while in session. A master key will persist to exsist even after the session is terminated.It is used between entiteis to distribute more session keys.

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

-A Key Distribution Center is in charge of which systems get to communicate with each other. Also know 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 eachother from the KDC will they be able to establish a secure encrytped connection.

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



[**https://quizlet.com/37144672/is-672-chapter-04-flash-cards/**](https://quizlet.com/37144672/is-672-chapter-04-flash-cards/)

[**https://thisismyclassnotes.blogspot.com/2015/06/key-distribution-and-user-authentication.html#:~:text=List%20ways%20in%20which%20secret,there%20are%20the%20following%20options%3A HYPERLINK "https://thisismyclassnotes.blogspot.com/2015/06/key-distribution-and-user-authentication.html#:~:text=List%20ways%20in%20which%20secret,there%20are%20the%20following%20options%3A&text=A%20key%20could%20be%20selected%20by%20A%20and%20physically%20delivered%20to%20B.&text=A%20third%20party%20could%20select,it%20to%20A%20and%20B"& HYPERLINK "https://thisismyclassnotes.blogspot.com/2015/06/key-distribution-and-user-authentication.html#:~:text=List%20ways%20in%20which%20secret,there%20are%20the%20following%20options%3A&text=A%20key%20could%20be%20selected%20by%20A%20and%20physically%20delivered%20to%20B.&text=A%20third%20party%20could%20select,it%20to%20A%20and%20B"text=A%20key%20could%20be%20selected%20by%20A%20and%20physically%20delivered%20to%20B. HYPERLINK "https://thisismyclassnotes.blogspot.com/2015/06/key-distribution-and-user-authentication.html#:~:text=List%20ways%20in%20which%20secret,there%20are%20the%20following%20options%3A&text=A%20key%20could%20be%20selected%20by%20A%20and%20physically%20delivered%20to%20B.&text=A%20third%20party%20could%20select,it%20to%20A%20and%20B"& HYPERLINK "https://thisismyclassnotes.blogspot.com/2015/06/key-distribution-and-user-authentication.html#:~:text=List%20ways%20in%20which%20secret,there%20are%20the%20following%20options%3A&text=A%20key%20could%20be%20selected%20by%20A%20and%20physically%20delivered%20to%20B.&text=A%20third%20party%20could%20select,it%20to%20A%20and%20B"text=A%20third%20party%20could%20select,it%20to%20A%20and%20B**](https://thisismyclassnotes.blogspot.com/2015/06/key-distribution-and-user-authentication.html#:~:text=List%20ways%20in%20which%20secret,there%20are%20the%20following%20options%3A&text=A%20key%20could%20be%20selected%20by%20A%20and%20physically%20delivered%20to%20B.&text=A%20third%20party%20could%20select,it%20to%20A%20and%20B)**.**

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



[**http://www.brainkart.com/article/Distribution-of-Public-Keys\_8469/**](http://www.brainkart.com/article/Distribution-of-Public-Keys_8469/)

[**http://www.darshan.ac.in/Upload/DIET/Documents/CE/IS\_Public%20Key%20Cryptography\_06012015\_043459AM.pdf**](http://www.darshan.ac.in/Upload/DIET/Documents/CE/IS_Public%20Key%20Cryptography_06012015_043459AM.pdf)

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

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



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

Formatting certificates.

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

[**https://www.venafi.com/blog/how-do-certificate-chains-work**](https://www.venafi.com/blog/how-do-certificate-chains-work)

[**https://sites.google.com/site/ddmwsst/digital-certificates**](https://sites.google.com/site/ddmwsst/digital-certificates)

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



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

<https://www.integers.co/questions-answers/what-is-the-prime-factorization-of-the-number-7007.html>

<https://www.2dtx.com/prime/prime7007.html>

<https://factorization.info/prime-factors/0/prime-factors-of-7007.html>

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

<https://www.doc.ic.ac.uk/~mrh/330tutor/ch05s02.html>

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

<https://www.chegg.com/homework-help/questions-and-answers/determine-value-phi-41-231--note-n-euler-s-totient-function-q41824102>

<https://www.dcode.fr/euler-totient>

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

<https://www.chegg.com/homework-help/questions-and-answers/difference-index-discrete-logarithm-please-give-detailed-answer-q24508789>

<https://crypto.stackexchange.com/questions/33958/what-is-the-difference-between-discrete-logarithm-and-logarithm>

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

<https://quizlet.com/170284728/review-questions-public-key-cryptography-flash-cards/>

<https://www.chegg.com/homework-help/questions-and-answers/describe-general-terms-efficient-procedure-step-step-picking-prime-number-q2262297>

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

<https://quizlet.com/170284728/review-questions-public-key-cryptography-flash-cards/>

<https://brainly.in/question/13932907>

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

[https://comodosslstore.com/blog/public-key-and-private-key-pair-how-it-works.html#:~:text=Public%20Key%20and%20Private%20Key%20pair%20is%20the%20core%20component,carrying%20out%20encryption%20and%20decryption. HYPERLINK "https://comodosslstore.com/blog/public-key-and-private-key-pair-how-it-works.html#:~:text=Public%20Key%20and%20Private%20Key%20pair%20is%20the%20core%20component,carrying%20out%20encryption%20and%20decryption.&text=This%20key%20pair%20is%20used,Bitcoin%20and%20other%20such%20cryptocurrencies"& HYPERLINK "https://comodosslstore.com/blog/public-key-and-private-key-pair-how-it-works.html#:~:text=Public%20Key%20and%20Private%20Key%20pair%20is%20the%20core%20component,carrying%20out%20encryption%20and%20decryption.&text=This%20key%20pair%20is%20used,Bitcoin%20and%20other%20such%20cryptocurrencies"text=This%20key%20pair%20is%20used,Bitcoin%20and%20other%20such%20cryptocurrencies](https://comodosslstore.com/blog/public-key-and-private-key-pair-how-it-works.html#:~:text=Public%20Key%20and%20Private%20Key%20pair%20is%20the%20core%20component,carrying%20out%20encryption%20and%20decryption.&text=This%20key%20pair%20is%20used,Bitcoin%20and%20other%20such%20cryptocurrencies).

<https://www.quora.com/What-are-the-roles-of-public-and-private-keys>

<https://www.chegg.com/homework-help/roles-public-private-key-chapter-9-problem-2rq-solution-9780134444635-exc>

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;

<https://www.chegg.com/homework-help/questions-and-answers/perform-encryption-decryption-using-rsa-algorithm-following--p-3-q-11-e-7-m-5-b-p-5-q-11-e-q3302878>

<https://github.com/dfarrell07/rsa_walkthrough/blob/master/solutions>

<https://www.coursehero.com/file/24098901/Week-5-Homeworkdocx/>