Nova Southeastern University
College of Computing and Engineering

Assignment 3
ISEC 660 Advanced Network Security
Winter 2021
Due date: 3/14/2021
Total Points: 100

Notes:
1. Please include your name in EVERY document you submit.
2. Please sign and submit the "Certification of Authorship" form (located in Canvas) along with your solutions.

Section I. Reading

Chapters 2, 8, 9, 20, 21, 22, 23

Section II. Questions (70 points, all questions are equally weighted)

Q1. Suppose someone suggests the following way to confirm that the two of you are both in possession of the same secret key. You create a random bit string the length of the key, XOR it with the key, and send the result over the channel. Your partner XORs the incoming block with the key (which should be the same as your key) and sends it back. You check, and if what you receive is your original random string, you have verified that your partner has the same secret key, yet neither of you has ever transmitted the key. Is there a flaw in this scheme? Please use examples(s) to justify your answer.

Q2. Consider the RSA algorithm with $p=7$ and $q=13$. Follow the conventions shown in Section 21.4.
2.1 What are n and $\emptyset(n)$?
2.2 Let e be 3. Is this an acceptable choice for e? If the answer is *yes*, then justify. If the answer is *no*, suggest an alternative value for e.
2.3 Find d such that $de=1 \pmod z$ and $d<72$.
d. What are public key and private key in this question?

Q3. Cryptography (Main Reference: Chapter 21)

Review Section 21.5 of the textbook on the Diffie-Hellman algorithm. Following the textbook convention, with $q = 71$ and $\alpha = 7$, suppose user A and B choose private keys $X_A = 5$ and $X_B = 12$, respectively.

3.1 Calculate A's and B's public keys, Y_A and Y_B. Show the process.
3.2 Following the results from step a, calculate the shared symmetric key K.

Q4. Firewall (Main Reference: Chapter 9)

Table 9.5 of the textbook shows a sample of a packet filter firewall rule set for an imaginary network of IP address that range from 192.168.1.0 to 192.168.1.254. Describe the effect of each firewall rule.

Q5. List four functions supported by S/MIME.

Q6. What are the two ways of providing authentications in IPsec?

Q7. What are the principal elements of a Kerberos system? Why the system is designed with different servers?

Section III. Practical assignment (30 points)

See the instructions in the "Wireshark_SSL.pdf" file for details on how experiment on SSL using Wireshark. Answer the questions listed in the file based on your experience with Wireshark. Please include necessary screenshots in your submission.

Note that there are two options to capture the network traffic, either by capturing the live traffic, or by downloading the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the *ssl-etherealtrace-1* packet trace.

For additional information about the SSL/TLS protocol, please refer to Chapter 22 of the textbook and the following URLs.

https://www.geeksforgeeks.org/secure-socket-layer-ssl/

https://en.wikipedia.org/wiki/Transport_Layer_Security