**CMPE 209 Network Security**

**Homework #3**

**Due: 4/10/2023, 11:59 p.m.**

[Question 1] (10 points) Please explain the differences between secret key cryptography and public key cryptography.

[Question 2] (10 points) What is a message authentication code? List three approaches to message authentication and explain it clearly for each step (Hint: Please refer to Figure 2.5).

[Question 3] (10 points) What properties must a hash function have to be useful for message authentication? Please explain each of the properties clearly. (Hint: You need to list the desirable hash function property)

[Question 4] (10 points) Please show how to find a pair of a private key and a public key in RSA. You must explain each step to drive the key pair. And then, find a private key (d) in RSA given with two large primes p = 11 and q=3. The public key in RSA is e=3.

[Question 5] (10 points) How can public-key encryption be used to distribute a secret key? (Hint: you can use a private key (PR) and a public key(PU) to distribute a secret key. You can assume that there are two persons (Alice and Bob) who want to share a secret key for communications.)

(reference answer) Several different approaches are possible, involving the private key(s)

of one or both parties. One approach is the Diffie-Hellman key exchange.

Another approach is for the sender to encrypt a secret key with the

recipient's public key.

[Question 6] (20 points) A and B want to establish a secure communication channel between them. They do not care about the confidentiality of the messages being transmitted, but they do want to ensure the integrity and authenticity of the messages. Answer the following questions by drawing diagrams that show the procedures of sending and receiving messages. Assume A and B share a common key K to utilize symmetric encryption.

(1) (5 points) How can they achieve their goal only with symmetric cryptography?

(2) (5 points) How can they achieve their goal only with a hash function (e.g., MD5)?

(3) (5 points) Can they get a non-repudiation service by using the symmetric cryptography? If yes, how? If no, why?

(4) (5 points) Please identify a particular way to provide the non-repudiation service for A and B. If needed, you can set up some assumptions.

[Question 7] [100 points] SEED labs.

Please conduct the lab assignment from SEED labs. Please refer the SEED labs on Canvas and submit your report based on the highlighted part. You need to follow the instructions for each lab and show your work by taking screenshots with your explanation for each lab.

(1) (30 points) Secret-Key Encryption Lab(Please do Task 1, Task 2, and Task 3).

<https://seedsecuritylabs.org/Labs_20.04/Files/Crypto_Encryption/Crypto_Encryption.pdf>

(2) (30 points) RSA Encryption and Signature Lab. (Please do Task1, Task2, Task3, and Task4).

<https://seedsecuritylabs.org/Labs_20.04/Crypto/Crypto_RSA/>

(3)(20 points) Pseudo Random Number Generation Lab (Please do Task 1 and Task 3).

<https://seedsecuritylabs.org/Labs_20.04/Files/Crypto_Random_Number/Crypto_Random_Number.pdf>

(4) (20 points) MD5 Collision Attack Lab. (Please do only Task 1).

<https://seedsecuritylabs.org/Labs_20.04/Files/Crypto_MD5_Collision/Crypto_MD5_Collision.pdf>

FYI) Instructions for Setup: <https://github.com/seed-labs/seed-labs/blob/master/manuals/vm/seedvm-manual.md>

[Question 8] Please include the SDN Mininet lab. The point for this questions will be added to your homework #2 score. If you already submitted it, you don’t need to submit it again.