CIS3360: Security in Computing (online session, Spring 2012)

Homework 2: Chapter 8

(assigned 02/06, due on webcourse by 3AM 02/16, i.e., late night in 02/15)

Question 1 to 4 should be submitted to Assignment 2.1

1. **(12 points) Knowledge-based Question:**
   a. What are the differences between public/symmetric key cryptography? The advantage and disadvantage of each?
   b. For English alphabet based texts regardless of upper or lower case (i.e., assuming each letter has only 26 possible value), if the length of the key using Vigenere Cipher is 4, how many possible encryption keys exist? (hint: we all know that Caesar cipher has 26 possible encryption keys)
   c. What is the usage of a cryptographic hash function? Can two documents have the same hash value?

2. **(8 points) Determine whether a statement is True or False. If a statement is false, you must explain why.**
   a. Digital signature of a message m is H(m), where H() represent a cryptographic hash function such as MD5 or SHA-1.
   b. Cesar cipher is a kind of substitution cipher, while Vigenere cipher is a kind of transposition cipher.

3. **(18 points)** Cipher Generation:
   a. What are the substitutions for the (decimal) numbers 12, 7, and 2 using the S-box from lecture notes Ch08-CryptoConcepts.ppt, Page 17? (The S-box is also shown in the textbook as Figure 8.3)
   b. What is the encryption of the following string "THELAZYFOX" using the Caesar cipher shown in Page 14 in lecture notes Ch08-CryptoConcepts.ppt?
   c. What is the Hill cipher key matrix **K** that can realize the following permutation:

      π: (1,2,3,4,5) → (3,5,1,4,2)

4. **(10 points)** Birthday Attack: Suppose in our class we have 25 students, what is the probability that we have two students having the same day as their birthday? (hint: the problem is explained in lecture notes Ch08-CryptoConcepts.ppt, Page 66)

Question 5 to 7 should be submitted to Assignment 2.2

5. **(20 points)** Modular power computation:
    a. Compute 7^{16} mod 11 using modular power algorithm shown on lecture notes Ch08-CryptoConcepts.ppt, Page 57. Show your computation steps.
    b. Compute 7^{120} mod 143 using modular power algorithm shown on lecture notes Ch08-CryptoConcepts.ppt, Page 57. Show your computation steps.

6. **(20 points)** Euclid's GCD Algorithm: Show the steps of applying the Euclid GCD algorithm to compute the following GCDs. You can show the steps by providing the similar computation table shown on lecture notes Ch08-CryptoConcepts.ppt, Page 47.
    a. GCD(412,200)
    b. GCD(510,412)

7. **(12 points)** Assume that User M (denoted as M) wants to send a message P to User N (denoted as N), and they know each other's public key (K_N^+, K_M^+) beforehand. Please show/explain how User M sends the message P to User N and how User N processes the message in order to guarantee of both properties: (1) the message is confidential between M and N; and (2) User N is sure that the message is sent by User M. Assume that the message P must be encrypted by using symmetric key encryption, i.e., you cannot directly use public key to encrypt the entire message.