# CSC650 SECURE NETWORKED SYSTEMS

## Homework 2

**Due: 7:00PM, Tuesday, 03/15/2016**

1. Bob has been told to design a message authentication code to prevent messages from being modified by an intruder. Bob decides to use the hash result of a message as the message authentication code without using any key. Does this solve the problem and why? If it does not solve the problem, what is the right way to construct the message authentication code? (10 Points)

2. For RSA key generation, given $p = 23$, $q = 17$, and $e = 5$, calculate $d$. Give the process of calculation. (10 Points)

3. Explain how to protect data integrity when Alice wants to send a message to Bob by using secret key cryptography. (e.g., what should Alice send to Bob and how does Bob verify whether the message has been modified or not during transmission). What if they want to use public key cryptography? (10 Points)

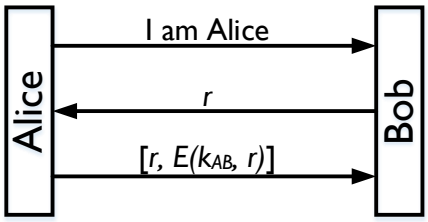
4. Can the message authentication code preserve non-repudiation? What about digital signatures? Why? (10 Points)

5. Consider Diffie-Hellman protocol.
   a. What is the Diffie-Hellman protocol used for? (5 Points)
   b. Given $p = 13$, $g = 4$, $SA = 3$, and $SB = 5$. Compute $T_A$, $T_B$, and the shared key $k$ using Diffie-Hellman protocol. (10 Points)
   c. Why is Diffie-Hellman protocol vulnerable to the Man-in-The-Middle attack? (5 Points)

6. Suppose Fred sees your RSA digital signatures on messages $m_1$and $m_2$ (i.e. he knows $m_1^d \ mod \ n$ and $m_2^d \ mod \ n$). Then, he is able to forge the signatures on messages $m_1^2$ mod $n$, message $m_2^2$ mod $n$, and message $m_1.m_2$ mod $n$. How does he do that? (15 Points)

7. What are the two principles to protect authentication again the reflection attack? (10 Points)

8. Suppose we use the following authentication protocol for the server Bob to authenticate a user Alice. Alice initiates contact with Bob. Suppose we wish Bob to be a stateless server, and therefore it is inconvenient to require him to remember the challenge he sent to Alice. Hence, Alice is required to send the challenge back to Bob, along with the encrypted challenge. So the protocol is:




Is this protocol secure? (We do not consider database reading attack here.) (10 Points)