Name:

# Computer Security: Homework 4

Due September 27, 2010 on compass. Shortened late hand in period to October 1, 2010 to ensure adequate time to post answers before exam.

1. Alice and Bob use RSA to exchange data. Alice's public key is ($e_A$, $n_A$). Bob's public key is ($e_B$, $n_B$). Their private keys are $d_A$ and $d_B$ respectively.
   a) Show the computations that Alice would perform to send Bob the message, m, such that only Bob could read the message.

   b) Bob want's to send Alice a message, m, that only she can read. He also wants her to be assured that Bob created the message. Show the computations that Bob would perform to create such an encrypted message.

   c) What is the mathematical relationship between Alice's public and private key?

   d) The computationally efficient solution of what hard problem will eliminate the strength of the RSA algorithm? Why?

2. Alice and Bob need to communicate securely. They only have symmetric key algorithms like AES available to them. They each have an interchange key ($K_a$ and $K_b$), and they need to develop a session key negotiation protocol.

a. They start with a straightforward algorithm that assumes each participant has the other's interchange key. The initiator picks a session key and encrypts it with its peer's interchange key. E.g., Alice picks session key $K_{ab}$ and sends $\{K_{ab}\}K_b$ to Bob. What kind of attack could Eve launch on this scenario?

b. Needham-Schroeder is a key exchange algorithm that involves a trusted third party. What is a benefit of using a trusted third party as opposed to the direct approach described in part a?

c. What is the purpose of the last exchange of messages between Alice and Bob in the Needham-Schroeder protocol?

Name:

3. Work with Gnu Privacy Guard (GPG). You can access GPG from http://gnupg.org. I have used this on Linux and installed it via yum on my personal system. I am running it on my Windows system via cygwin. It is already be installed on the University Linux systems. Type "man gpg" to check if it is installed on your system. Once you get your GPG system operational perform the following tasks:
   a. Create a key pair and submit your exported public key. Export your key in the armored ASCII format.
   b. Sign the class public key posted at http://www.cs.illinois.edu/class/fa10/cs461/assignments/cs461-pub.asc with your key. Submit the exported signed key. Again export in ASCII using the armored format.
   c. Select an ascii file. Encrypt it with the class key and sign it with your key. Submit the signed and encrypted file.

4. Alice is writing a secure network messaging library. Confidentiality of the data is less of a concern than integrity. The message will be sent unencrypted.
   a. She is considering using HMAC-SHA or MD5. Which algorithm should she use? Give a reason for the preference.
   b. If Alice is worried about Eve launching a birthday attack, what order of number of hash tests would Eve have to perform to find a pair of messages that breaks the hash? (for the algorithm chosen in step a)
   c. How does the crypto-hash protect the sender and receiver from changes made by a malicious intermediary?