Midterm Exam **COS 432, Fall 2003**

All questions have equal weight. Use your time wisely; read all of the questions first and then think about how to allocate your time.

You may use your own lecture notes, copies of other people's lecture notes, and any summaries you have made of those notes. You may not use any other materials.

Note that some or all of these problems have more than one correct answer. You must give a single answer; and you will get full credit if your answer is one of the correct ones. Don't be too worried if you can think of alternative answers that seem just as good as the answer you gave.

Please do your work in an exam book.

Undergraduates: Before turning in your exam, please hand-write and sign the Honor Code pledge, "I pledge my honor that I have not violated the Honor Code during this examination."

(Graduate students: No need to sign anything. You are bound automatically by university regulations.)

---

1. A SecurID token is a small device, about the size and shape of a credit card, that some organizations use to authenticate users who are logging in to a server. Each user carries a SecurID token. There is a small window on the front of the SecurID token; the window displays a six-digit number. Every thirty seconds, the number changes in an apparently unpredictable way. When a user wants to log on to the server, the user must type in the number that currently appears on his SecurID token. The server verifies that the user has entered the correct number, before allowing the user to log in.

   Assume that each SecurID token has an internal clock that is perfectly synchronized with the server's clock.

   Give a plausible explanation for how this system uses cryptography. How does the SecurID generate the numbers it displays? How does the server check whether the entered number is correct?

2. A garage door opener system consists of two components: an opener, which is bolted to the ceiling inside a house's garage; and a remote, which the owner keeps in her car. When the owner presses a button on the remote, this causes the remote to send a sequence of bits (about 200 bits in all) by radio to the opener; and if the opener likes the bit stream it receives, it opens the garage door.

   If the remote sends the same bit-sequence every time, the system is subject to replay attacks – an adversary can record the bit-sequence sent by the remote, and can re-send that sequence later (perhaps after the owner has left) to gain entry. *A new system has been designed to prevent replay attacks.*

   Give a plausible explanation for how this new system uses cryptography. What kinds of key(s) are used, and where are they stored? How does the remote generate the bit sequence to send each time? How does the opener decide whether to accept the bit sequence it has received?

   (Hint: bear in mind that the protocol uses a single message, in which the remote sends a message of about 200 bits in size to the opener. The remote does not, and cannot, receive messages.)

3. Many hotels use magnetic-stripe cards as door keys. The key has a magnetic stripe that easily readable and writable. When you check in to the hotel, the desk clerk uses a machine to write something onto the stripe of the card that will serve as your key. When you get to your room, you insert the card into a magnetic-stripe reader that is part of the door lock. If the door lock likes what it reads on your card, it opens the door. Your key continues to work for the duration of your scheduled stay; but after your scheduled checkout date, it will no longer open the door.

   The door locks are not connected to anything, so they cannot communicate in real time with any other component of the system.

   Give a plausible explanation for how this system uses cryptography. What kinds of keys are used, and where are they stored? How does the writer at the front desk generate the information it writes onto the keycard? How does the lock use the information on the keycard to decide whether to allow access to the room?