# Outline for November 27, 2006

***Reading***: §12.1–12.2.2

1. Greetings and felicitations!
   a. Puzzle of the day
   b. Office hours changed today to 4–5 PM
2. Basis: what you know/have/are, where you are
3. Passwords
   a. Problem: common passwords
   b. May be pass phrases: goal is to make search space as large as possible, distribution as uniform as possible
   c. Other ways to force good password selection: random, pronounceable, computer-aided selection
4. Password Storage
   a. In the clear; Multics story
   b. Enciphered; key must be kept available
   c. Hashed; show UNIX versions, including salt
5. Attacks
   a. Exhaustive search: password is 1 to 8 chars, say 96 possibles; it's about $7 \times 10^{16}$
   b. Inspired guessing: think of what people would like (see above)
   c. Random guessing: can't defend against it; bad login messages aid it
   d. Scavenging: passwords often typed where they might be recorded as login name, in other contexts, etc.
   e. Ask the user: very common with some public access services