# Outline for March 6, 2006

***Reading***: text, §14.6, 12.1–12.5

1. Greetings and felicitations!
   a. Puzzle of the day
2. Identity
   a. State and cookies
   b. Anonymous remailers: type 1 and type 2 (mixmaster)
3. Authentication:
   a. validating client (user) identity
   b. validating server (system) identity
   c. validating both (mutual authentication)
4. Basis: what you know/have/are, where you are
5. 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
6. Password Storage
   a. In the clear; Multics story
   b. Enciphered; key must be kept available
   c. Hashed; show UNIX versions, including salt