# Outline for November 20, 2006

***Reading***: §10.2, 10.4.2

1. Greetings and felicitations!
   a. Puzzle of the day
2. Key Exchange
   a. Needham-Schroeder and Kerberos
   b. Public key; man-in-the-middle attacks
3. Cryptographic Key Infrastructure
   a. Certificates (X.509, PGP)