Outline for February 5, 2016

Reading: *text*, §10 in text

Assignments due: Homework 2, due February 5
Project progress report, due February 8

1. Key exchange
   a. Needham-Schroeder and Kerberos
   b. Public key; man-in-the-middle attacks
2. Key Generation
   a. Cryptographically random numbers
   b. Cryptographically pseudorandom numbers
   c. Strong mixing function
3. Cryptographic Key Infrastructure
   a. Certificates (X.509, PGP)