Outline for February 25/March 1, 2002

Reading: §10.2, §10.4.2-10.4.3, §10.5.1-10.5.1.1, §10.5.2, §10.6 except §10.6.2.2

1. Greetings and Felicitations
2. Puzzle of the day
3. Key Exchange
   a. Needham-Schroeder and Kerberos
   b. Public key; man-in-the-middle attacks
4. Cryptographic Key Infrastructure
   a. Certificates (X.509, PGP)
   b. Certificate, key revocation
   c. Key Escrow
5. Digital Signatures