Outline for February 22/25, 2002

Reading: §9.4, §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. Cryptographic Checksums
   a. Function $y = h(x)$: easy to compute y given x; computationally infeasible to compute x given y
   b. Variant: given x and y, computationally infeasible to find a second x' such that $y = h(x')$.
   c. Keyed *vs*. keyless
   d. MD5, HMAC
4. Key Exchange
   a. Needham-Schroeder and Kerberos
   b. Public key; man-in-the-middle attacks
5. Cryptographic Key Infrastructure
   a. Certificates (X.509, PGP)
   b. Certificate, key revocation
   c. Key Escrow
6. Digital Signatures