Outline for November 22, 2006

Reading: §10.6; 11.4.1; 12.1

1. Greetings and felicitations!
   a. Puzzle of the day
2. Cryptographic Key Infrastructure
   a. Certificate, key revocation
3. Digital Signatures
   a. Judge can confirm, to the limits of technology, that claimed signer did sign message
   b. RSA digital signatures: sign, then encipher
4. PEM, PGP
   a. Goals: confidentiality, authentication, integrity, non-repudiation (maybe)
   b. Design goals: drop in (not change), works with any RFC 821-conformant MTA and any UA, and exchange messages without prior interaction
   c. Use of Data Exchange Key, Interchange Key
   d. Review of how to do confidentiality, authentication, integrity with public key IKs
   e. Details: canonicalization, security services, printable encoding (PEM)
   f. PGP v. PEM
5. Authentication
   a. validating client (user) identity
   b. validating server (system) identity
   c. validating both (mutual authentication)