Lecture 22 Outline

Reading: *text*, §10.6, 11.3, 11.4.1 **Assignments due:** Homework 4, due May 23, 2011

1. Greetings and Felicitations!
   a. Homework #4 now on SmartSite
2. Digital Signatures
   a. Judge can confirm, to the limits of technology, that claimed signer did sign message
   b. RSA digital signatures: sign, then encipher
3. Networks and ciphers
   a. Where to put the encryption
   b. Link vs. end-to-end
4. PEM, PGP
   a. Goals: confidentiality, authentication, integrity, non-repudiation (maybe)
   b. Design goals: drop in (not change), works with any RFC 821-conforment 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