Outline for October 24, 2003

Reading: Chapters 10.2, 10.4, 10.6

Discussion Problem

Define spam. In particular, what distinguishes spam from unsolicited e-mail?

Outline for the Day

1. Key Exchange
   a. Needham-Schroeder and Kerberos
   b. Public key; man-in-the-middle attacks
2. Cryptographic Key Infrastructure
   a. Certificates (X.509, PGP)
   b. 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