Outline for March 1, 2006

Reading: text, §10.4.2, 10.6, 11.1, 11.3

1. Greetings and felicitations!
   a. Puzzle of the day
2. Cryptographic Key Infrastructure
   a. Certificates (X.509, PGP)
   b. Certificate, key revocation
3. Digital Signatures
   a. udge can confirm, to the limits of technology, that claimed signer did sign message
   b. RSA digital signatures: sign, then encipher
4. Types of attacks
   a. Forward searches
   b. Misordered blocks
   c. Statistical regularities (repetitions)
5. Networks and ciphers
   a. Where to put the encryption
   b. Link vs. end-to-end