Outline for February 27, 2006

Reading: text, §9.4, 10.1–10.2, 10.4.2, 10.6, 11.1, 11.3

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