Outline for November 17, 2006

Reading: §9.4, 10.1–10.2

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