Outline for October 7, 2022

Reading: *text*, §10.4–10.5, 11.1–11.2, 12.1 **Assignments:** Homework 1, due October 5; Project selection, due Oct 7

1. 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
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, then sign
   (c) El Gamal digital signatures
3. Session and interchange keys
4. Key Exchange
   (a) Needham-Schroeder and Kerberos
   (b) Public key; man-in-the-middle attacks
   (c) The discrete log problem and Diffie-Hellman
5. Attacks
   (a) Precomputation
   (b) Misordered blocks
   (c) Statistical regularities
   (d) Type flaw