Outline for October 10, 2022

Reading: *text*, §11.1–11.2, 12.1,12.4 **Assignments:** Homework 2, due October 21; Progress report, due Nov 4

1. Session and interchange keys
2. Key Exchange
   (a) Kerberos
   (b) Public key; man-in-the-middle attacks
   (c) The discrete log problem and Diffie-Hellman
3. Attacks
   (a) Precomputation
   (b) Misordered blocks
   (c) Statistical regularities
   (d) Type flaw
4. Networks and cryptography
   (a) Link vs.end-to-end encryption