Outline for October 14, 2024

Reading: *text*, §11.2, 12.1, 12.4 **Due:** Homework 2, due October 23; Project progress report, due November 1

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