Outline for October 16, 2023

Reading: *text*, §10.5, 11.1–11.2, 12.1, 12.4

Assignments: Homework 2, due October 23; Background Research, due October 27

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