Lecture 20: May 12, 2021

Reading: *text*, §11.2–11.4 **Assignments:** None yet; stay tuned

1. Key Exchange
   (a) Public key; man-in-the-middle attacks
   (b) The discrete log problem and Diffie-Hellman
2. Key Generation
   (a) Cryptographically random numbers
   (b) Cryptographically pseudorandom numbers
   (c) Strong mixing function
3. Cryptographic Key Infrastructure
   (a) Certificates
   (b) Merkle trees
   (c) Certificate chains
   (d) Certificate, key revocation