Lecture 14: October 25, 2019

Reading: *text*, §11.1–11.2, 11.4, 12–12.3, [5]

Assignments: Lab 2, due November 6, 2019
Homework 3, due November 8, 2019

1. Greetings and felicitations!
2. Puzzle of the Day
3. Key Exchange
   (a) Needham-Schroeder and Kerberos
   (b) The discrete log problem and Diffie-Hellman
   (c) Public key; man-in-the-middle attacks
4. Key Generation
   (a) Cryptographically random numbers
   (b) Cryptographically pseudorandom numbers
   (c) Strong mixing function
5. Cryptographic Key Infrastructure
   (a) Certificates (X.509, PGP)
   (b) Certificate, key revocation
6. Cipher problems
   (a) Precomputation
   (b) Misordered blocks
   (c) Statistical regularities
   (d) Type flaw attacks
7. Networks and ciphers
   (a) Where to put the encryption
   (b) Link vs. end-to-end