Lecture 15: October 28, 2019

Reading: *text*, §11.3–11.4, 12.1

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

1. Greetings and felicitations!
   (a) Sample midterm and study guide now on Canvas
2. Puzzle of the Day
3. Key generation
   (a) Cryptographically random numbers
   (b) Cryptographically pseudorandom numbers
   (c) Strong mixing function
4. Cryptographic key infrastructure
   (a) Certificates (X.509, PGP)
   (b) Certificate, key revocation
5. Cipher problems
   (a) Precomputation
   (b) Misordered blocks
   (c) Statistical regularities
   (d) Type flaw attacks