Lecture 16: October 30, 2019

Reading: *text*, §12.1, 12.3–12.4, 12.5.3, [5]

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. Cipher problems
   (a) Precomputation
   (b) Misordered blocks
   (c) Statistical regularities
   (d) Type flaw attacks
4. Networks and ciphers
   (a) Where to put the encryption
   (b) Link vs. end-to-end
5. TLS and SSL
   (a) Session, connection
   (b) Cryptographic mechanisms
   (c) Lower layer: TLS record protocol