Lecture 11: October 18, 2019

Reading: *text*, §8.4–8.5, 10.1–10.2

Assignments: Lab 1, due October 18, 2019
Homework 2, due October 21, 2019

1. Greetings and felicitations!
2. Puzzle of the Day
3. Role-based access control
4. Break-the-glass policies
5. Cryptography
   (a) Codes vs. ciphers
   (b) Attacks: ciphertext only, known plaintext, chosen plaintext
   (c) Types: substitution, transposition
6. Symmetric Cryptography
   (a) Monoalphabetic (simple substitution): $f(a) = a + k \bmod n$
   (b) Example: Caesar (shift) cipher with $k = 3$, `RENAISSANCE` $\rightarrow$ `UHQDLVVDQFH`