Lecture 12 Outline

April 27, 2018

Reading: §8.3–8.5, 10.1–10.2

Assignments: Homework 3, due on May 9, 2018 at 11:59pm
Lab 2, due on May 7, 2018 at 11:59pm

1. Greetings and felicitations!
2. Originator-controlled access control
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`