

## Lecture 16: May 3, 2021

**Reading:** *text*, §8.3–8.4, 10.1–10.2.2

**Assignments:** Lab 2, due May 5, 2021  
Homework 3, due May 10, 2021 (Note new due date)

1. Originator-controlled access control
  - (a) Digital rights management
2. Role-based access control
3. Cryptography
  - (a) Codes vs. ciphers
  - (b) Attacks: ciphertext only, known plaintext, chosen plaintext
  - (c) Types: substitution, transposition
4. Symmetric Cryptography
  - (a) Monoalphabetic (simple substitution):  $f(a) = a + k \bmod n$
  - (b) Example: Caesar (shift) cipher with  $k = 3$ , RENAISSANCE  $\rightarrow$  UHQDLVVDQFH