Lecture 10: April 20, 2026

Reading: *text*, §8.4, 10.1–10.2.2 **Due:** Homework 2, due April 24, 2026

1. Greetings and felicitations!
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`
   (c) Polyalphabetic: Vigenère, $f_i(a) = a + k_i \bmod n$
   (d) Cryptanalysis: first do index of coincidence to see if it is monoalphabetic or polyalphabetic, then Kasiski method.
   (e) Problem: eliminate periodicity of key
   (f) Perfect secrecy: when the probability of computing the plaintext message is the same whether or not you have the ciphertext; only cipher with perfect secrecy: one-time pads; C = `AZPR`; is that `DOIT` or `DONT`?