Lecture 14: April 29, 2026

Reading: *text*, §11.4, 12.14 **Due:** Homework 3, due May 11, 2026

1. Greetings and felicitations!
2. Cryptographic Key Infrastructure
   (a) Merkle trees
   (b) Certificate chains
   (c) Certificate, key revocation
3. Attacks
   (a) Precomputation
   (b) Misordered blocks
   (c) Statistical regularities
   (d) Type flaw