Lecture 15: May 1, 2026

Reading: *text*, §12.4, 12.5.3, 13 **Due:** Homework 3, due May 11, 2026

1. Greetings and felicitations!
2. Attacks
   (a) Precomputation
   (b) Misordered blocks
   (c) Statistical regularities
   (d) Type flaw
3. Networks and cryptography
   (a) Link vs.end-to-end encryption
4. TLS security