Lecture 12: April 24, 2026

Reading: *text*, §10.4.1–10.5, 11.1–11.2 **Due:** Homework 2, due April 24, 2026

1. Greetings and felicitations!
2. Cryptographic Checksums
   (a) Keyed vs. keyless
3. Digital Signatures
   (a) Judge can confirm, to the limits of technology, that claimed signer did sign message
   (b) RSA digital signatures: sign, then encipher, then sign
4. Session and interchange keys
   (a) Normally public key cryptosystems used as key interchange system to exchange secret keys (cheap)
   (b) Then use secret key system (too expensive to use public key cryptosystem for this)
5. Key Exchange
   (a) Needham-Schroeder and Kerberos