

Lecture 19: May 10, 2021

Reading: *text*, §10.4, 11.1–11.2

Assignments: Homework 3, due May 10, 2021 (Note new due date)

1. 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
2. Session and interchange keys
3. Key Exchange
 - (a) Needham-Schroeder and Kerberos
 - (b) Public key; man-in-the-middle attacks
 - (c) The discrete log problem and Diffie-Hellman