Lecture 16 Outline

May 7, 2018

Reading: §10.4–10.5, 11.1, 11.2.1.1

Assignments: Homework 3, due on May 9, 2018 at 11:59pm
Lab 2, due on May 7, 2018 at 11:59pm

1. Cryptographic Checksums
   a. Function $y = h(x)$: easy to compute y given x; computationally infeasible to compute x given y
   b. Variant: given x and y, computationally infeasible to find a second x' such that $y = h(x')$
   c. Keyed vs. keyless
2. 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
3. Interchange and Session Keys
4. Key Exchange
   a. Needham-Schroeder and Kerberos