Lecture 17 Outline

May 9, 2018

Reading: §11.2.1.1, 11.2.2–11.3

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

1. Key Exchange
   a. Needham-Schroeder and Kerberos
   b. The discrete log problem and Diffie-Hellman
   c. Public key; man-in-the-middle attacks
2. Key Generation
   a. Cryptographically random numbers
   b. Cryptographically pseudorandom numbers
   c. Strong mixing function