Lecture 18 Outline

May 11, 2018

Reading: §11.4,12.1, 12.3 **Assignments:** Homework 3, due on May 11, 2018 at 11:59pm

1. Cryptographic Key Infrastructure
   a. Certificates (X.509, PGP)
   b. Certificate, key revocation
2. Cipher problems
   a. Precomputation
   b. Misordered blocks
   c. Statistical regularities
   d. Type flaw attacks
3. Networks and ciphers
   a. Where to put the encryption
   b. Link vs. end-to-end