Outline for December 4, 2014

Reading: *text*, §11, 26 **Assignments due:** Homework #4, due December 10, 2014 at 11:55pm

1. Key Exchange
   a. Needham-Schroeder and Kerberos
   b. Public key; man-in-the-middle attacks
2. Cryptographic Key Infrastructure
   a. Certificates (X.509, PGP)
   b. Certificate, key revocation
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
4. Network Organization for Security
   a. Firewalls and a DMZ
   b. Network architecture
   c. Availability