Outline for February 8, 2016

Reading: §11 in text **Assignments due:** Project progress report, due February 8

1. Cryptographic Key Infrastructure
   a. Certificates (X.509, PGP)
   b. Certificate, key revocation
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
3. Networks and Ciphers
   a. Problems
   b. Link, end-to-end encryption
   c. SSLv3: the good, the bad, and the broken