Lecture 16 Outline

October 26, 2016

Reading: *text*, 11.1*–11.2*, 11.4*, 12.1*, 12.3*, 12.4.1* **Assignments**: Homework 3, due Nov. 4; Lab 3, due Nov. 4

1. Greetings and felicitations!
2. Puzzle of the Day
3. Key Exchange
   a. Needham-Schroeder and Kerberos
   b. Public key; man-in-the-middle attacks
4. Key Generation
   a. Cryptographically random numbers
   b. Cryptographically pseudorandom numbers
   c. Strong mixing function
5. Cryptographic Key Infrastructure
   a. Certificates (X.509, PGP)
   b. Certificate, key revocation
6. Digital Signatures
   a. Judge can confirm, to the limits of technology, that claimed signer did sign message
   b. RSA digital signatures: sign, then encipher
7. Networks and ciphers
   a. Where to put the encryption
   b. Link vs. end-to-end
8. PEM, PGP
   a. Goals: confidentiality, authentication, integrity, non-repudiation (maybe)
   b. Design goals: drop in (not change), works with any RFC 821-conforment MTA and any UA, and exchange messages without prior interaction
   c. Use of Data Exchange Key, Interchange Key
   d. Review of how to do confidentiality, authentication, integrity with public key IKs