Lecture 18 Outline

October 31, 2016

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

1. Networks and ciphers
   a. Where to put the encryption
   b. Link vs. end-to-end
2. PEM, PGP
   a. Quick review
      i. Goals: confidentiality, authentication, integrity, non-repudiation (maybe)
      ii. Design goals: drop in (not change), works with any RFC 821-conforming MTA and any UA, and exchange messages without prior interaction
      iii. Use of Data Exchange Key, Interchange Key
      iv. Review of how to do confidentiality, authentication, integrity with public key IKs
   b. Details: canonicalization, security services, printable encoding (PEM)
   c. PGP v. PEM