
Notes for December 10, 1999

1. Greetings and Felicitations!
2. Puzzle of the Day
3. PKI
 - a. X.509 model, other models
4. PEM, PGP
 - a. Goals: confidentiality, authentication, integrity, non-repudiation (maybe)
 - b. Design goals: drop in (not change), works with any RFC 821-conformant 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
 - e. Details: canonicalization, security services, printable encoding (PEM)
 - f. PGP v. PEM