Notes for March 5, 1997

1. Hello
   a. Remember, Randy Leben on Friday; moved to 1131 EU-II
2. X.509 The Directory
   a. Intent: 1-way, 2-way (mutual), 3-way (same as 2-way but without timestamp)
   b. Token format and Colin I'Anson's bug
   c. 1-way: A sends token to B
   d. 2-way: A sends token to B, B sends token to A with same nonce
   e. 3-way: 2-way with nonce signed and returned
   f. 3-way flaw: needs nonce and intended target
3. PEM, PGP
   a. Goals: confidentiality, authentication, integrity, non-repudiation (maybel)
   b. Design goals: drop in (not change), works with any 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. Certificate-based key management
   g. PGP v. PEM