Notes for March 10, 1997

1. Hello
   a. Projects due Friday
2. Certificates
   a. Binding key to name, notion of issuer
   b. PEM trust hierarchy, certificate types
   c. X.509/PGP web of trust model
3. Common Implementation Vulnerabilities
   a. Unknown interaction with other system components (DNS entry with bad names, assuming finger port is finger and not chargen)
   b. Overflow (year 2000, 2038 for UNIX, lpr overwriting flaw, sendmail large integer flaw, su buffer overflow)
   c. Race conditions (xterm flaw, ps flaw)
   d. Environment variables (vi one-upsmanship, loadmodule)
   e. Not resetting privileges (Purdue Games incident)