Outline for April 27, 2000

1. Authentication protocols?
   a. classical: need trusted third party for both secrecy, authentication
   b. public key: need to verify to whom public key belongs
2. Challenge-response
   a. UNIX passwords
   b. Kerberos
   c. S/Key
   d. Diffie-Hellman and Sun's Secure RPC
3. Public key
   a. Standard: encipher with private key, decipher with public key
   b. Binding public keys to identity: certificates
   c. X.509, PGP web of trust
   d. PEM hierarchy of certification