Outline for May 15, 2003

1. Cryptographic techniques
   a. Example: Privacy-Enhanced Electronic Mail (PEM)
2. Authentication protocols?
   a. classical: need trusted third party for both secrecy, authentication
   b. public key: need to verify to whom public key belongs
3. Challenge-response
   a. UNIX passwords
   b. S/Key
4. 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
5. Representation of identity
   a. Users, groups, and roles