Outline for May 13, 2004

1. Interchange, Session Keys
2. Classical Key Exchange
   a. Needham-Schroeder
   b. Kerberos
3. Public Key Exchange
4. Key Generation
   a. Random vs. pseudorandom
   b. Mixing
5. Key Infrastructures
   a. Certificates
   b. Merkle's Tree Authentication scheme
   c. X.509 certificates
   d. PGP certificates
6. Key Escrow
   a. Goals
   b. EES and Clipper