Outline for May 13, 2003

1. Cryptographic checksums
   a. Requirements
   b. Keyed vs. keyless cryptographic checksums
   c. HMAC
2. Digital signatures
   a. Classical cryptography
   b. Public key cryptography
3. Key Exchange
   a. Kerberos
   b. Diffie-Hellman and Sun's Secure RPC
4. Cryptographic techniques
   a. End to end cryptography
   b. Link cryptography
   c. Example: Privacy-Enhanced Electronic Mail (PEM)