Outline for May 24, 2005

1. ORCON
    a. Originator controls distribution
    b. DAC, MAC inadequate
    c. Solution is combination
2. Role-based Access Control (RBAC)
    a. Definition of role
    b. Partitioning as job function
    c. Containment
3. What is a cryptosystem?
    a. $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{D}, \mathcal{E})$
    b. Attacks: known ciphertext, known plaintext, chosen plaintext
4. Classical Ciphers
    a. Transposition ciphers
    b. Substitution ciphers
    c. DES
5. Public-Key Cryptography
    a. Properties
    b. Diffie-Hellman
    c. RSA
6. Cryptographic Hashes
7. Access Control Mechanisms
    a. Access control lists
    b. Capabilities
    c. Locks and Keys
    d. Type checking
    e. Ring-based access control
    f. PACLs