Outline for May 6, 2004

1. CISS
    a. Intended for medical records; goals are confidentiality, authentication of annotators and integrity
    b. Patients, personal health information, clinician
    c. Assumptions and origin of principles
    d. Access principles
    e. Creation principle
    f. Deletion principle
    g. Confinement principle
    h. Aggregation principle
    i. Enforcement principle
    j. Comparison to Bell-LaPadula: lattice structure but different focus
    k. Comparison to Clark-Wilson: specialization
2. ORCON
    a. Originator controls distribution
    b. DAC, MAC inadequate
    c. Solution is combination
3. Role-based Access Control (RBAC)
    a. Definition of role
    b. Partitioning as job function
    c. Containment
4. What is a cryptosystem?
    a. (M, C, K, D, E)
    b. Attacks: known ciphertext, known plaintext, chosen plaintext
5. Transposition ciphers
    a. Show rail-fence cipher as example
    b. Show anagramming
6. Simple substitution ciphers
    a. Do Cæsar cipher
    b. Present Vigenère tableau
    c. Discuss breaking it (Kasiski method).