Study Guide for Midterm

This is simply a guide of topics that I consider fair game for the midterm. I don't promise to ask you about them all, or about any of these in particular; but I may very well ask you about any of these.

1. Fundamentals
    a. What is security?
    b. Basics of risk analysis
    c. Relationship of security policy to security
    d. Policy vs. mechanism
    e. Assurance and security
2. Saltzer's and Schroeder's Principles of Secure Design
3. Robust Programming
4. Policies
    a. What is a policy?
    b. Trust
    c. Types of access control (MAC, DAC, ORCON, RBAC)
    d. Policy languages
5. Confidentiality Models
    a. Bell-LaPadula Model
    b. Lattices and the BLP Model
6. Integrity models
    a. Biba
    b. Clark-Wilson
7. Cryptography
    a. Types of attacks: ciphertext only, known plaintext, chosen plaintext
    b. Caesar cipher, Vigenère cipher, one-time pad, DES
    c. Public key cryptosystems; RSA
    d. Confidentiality and authentication with secret key and public key systems