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. Basics of risk analysis
    b. Relationship of security policy to security
2. Robust Programming
3. Security in Programming
    a. Unknown interaction with other system components
    b. Overflow (both numeric and buffer)
    c. Race conditions (TOCTTOU flaw)
    d. Environment (shell variables, UIDs, file descriptors, *etc*.)
    e. Not resetting privileges
4. Vulnerabilities Models
    a. RISOS
    b. PA
    c. Uses
5. Penetration Studies
    a. Flaw Hypothesis Methodology
    b. Using vulnerabilities models
6. Policies
    a. Mandatory Access Control (MAC)
    b. Discretionary Access Control (DAC)
    c. Originator-Controlled Access Control (ORCON)
    d. Role-Based Access Control (RBAC)
    e. Policy languages
7. Confidentiality Models
    a. Bell-LaPadula Model
    b. Lattices and the BLP Model
8. Integrity Models
    a. Biba's model
    b. Clark-Wilson Integrity Model
9. Cryptography
    a. Types of attacks: ciphertext only, known plaintext, chosen plaintext
    b. Types of ciphers: substitution, transposition, product (both substitution and transposition)
    c. Goal of ciphers; what makes a cipher theoretically unbreakable
    d. Caesar cipher, Vigenère cipher, one-time pad, DES
    e. Public key cryptosystems
    f. RSA
    g. Confidentiality and authentication with secret key and public key systems