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. Mandatory Access Control (MAC)
   b. Discretionary Access Control (DAC)
   c. Originator-Controlled Access Control (ORCON)
   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. Classical cryptosystems; Caesar cipher, Vigenère cipher, one-time pad, DES
   c. Public key cryptosystems; RSA
   d. Confidentiality and authentication with secret key and public key systems
   e. One-way hash functions (cryptographic hash functions)
8. Key Distribution Protocols
   a. Kerberos and Needham-Schroeder
   b. Certificates and public key infrastructure
9. Cryptography and Networks
   a. Forward searches, misordered blocks, repetitions
   b. End-to-end and link encryption
   c. Where to put the encryption
   d. Secure electronic mail
10. Passwords (selection, storage, attacks, aging)
    a. UNIX password scheme, what the salt is and its role
    b. Password selection, aging
    c. Challenge-response schemes
    d. Attacking authentication systems: guessing passwords, spoofing system, countermeasures