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. Saltzer and Schroeder's design principles
   c. Relationship of security policy to security
2. Ethics and Law
   a. Exporting cryptographic programs, enciphered messages
   b. Ethical and legal problems of break-ins
   c. License to hack
3. Robust Programming
4. 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
5. Vulnerabilities Models
   a. RISOS
   b. PA
   c. Uses
6. Penetration Studies
   a. Relationship to formal verification and testing
   b. Flaw Hypothesis Methodology
   c. Using vulnerabilities models
7. 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
   e. What the DES is, characteristics
   f. Public key cryptosystems
   g. RSA
   h. Confidentiality and authentication with secret key and public key systems
8. Cryptographic checksums, digital signatures
   a. What they do
   b. What makes a good checksum
   c. What makes a good digital signature; RSA
9. Key Infrastructure
   a. Certificates and what they do

   b. Distribution of public keys
   c. Distribution of secret (classical) keys
   d. Key revocation
   e. Key escrow
10. Key Infrastructure
   a. Certificates and what they do
   b. Distribution of public keys; web of trust vs. hierarchy
11. Cipher Techniques
   a. Stream ciphers
   b. Block ciphers