Study Guide for Midterm

This is simply a guide of topics that I consider fair game for the mdterm. 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. Ethics and Law
   a. Exporting cryptographic programs, enciphered messages
   b. Ethical and legal problems of break-ins
   c. License to hack
2. Robust Programming
3. Cryptography
   a. Types of attacks: ciphertext only, known plaintext, chosen plaintextt
   b. Types of ciphers: substitution, transposition, product (both substitution and transposition)
   c. Goal of ciphers; what makes a cipher theoretically unbreakable
   d. Caesar cipher, Vigenere 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
4. User and System Authentication
   a. One-way hash functions (cryptographic hash functions)
   b. UNIX password scheme, what the salt is and its role
   c. Challenge-response schemes
   d. Attacking authentication systems: guessing passwords, spoofing system, countermeasures
5. UNIX identities
   a. Real UID, effective UID, saved UID, audit/login UID
   b. Primary and secondary group identities, real and effective GIDs
   c. Roles and the difference between them and a user identity
6. Access Control
   a. Fence registers, base and bounds registers, tagged architectures
   b. Multiple levels of privilege
   c. UNIX protection scheme
   d. ACLs, capabilities, lock-and-key
   e. MULTICS ring protection scheme
   f. MAC, multilevel (military) security
   g. ORCON, originator-controlled security
   h. Differences between MAC, DAC, ORCON
   i. Bell-LaPadula model
7. Integrity and Trust
   a. Relevance of trust
   b. Trusted Computing Base
   c. Thompson's compiler modification