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. Bad Programming and Good Programming
3. 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
4. Electronic mail
   a. Ordinary mail: security issues
   b. PEM: how it works, security issues
5. Certificates
   a. PEM Hierarchy
   b. Web of trust
6. Identity
   a. People and processes
   b. Computers
   c. Cookies and such
   d. Anonymity: remailers and proxy web browsers
7. Authentication
   a. Passwords
   b. Challenge-response
   c. How UCD does authentication for MyUCDavis
8. Any of the handouts