Sample Midterm

This is an example of the sort of questions I will ask. The actual midterm will be longer, of course, and may well have questions about the readings as well as the lectures.

1. Please define the following terms in one or two sentences.
   (a) assurance
   (b) firewall
   (c) availability
   (d) cypherpunk remailer
2. Please label the following as a "policy" or a "mechanism". Justify your answers.
   (a) Only students may use the system.
   (b) A program that checks that the user enters the correct password.
   (c) Systems can be connected to the Internet on alternate Thursdays only.
   (d) A firewall that prevents access to the system from non-University systems.
3. Please circle the best answer, and *justify it*.
   (a) Which of the following is a good password or pass-phrase?
      i. Mary
      ii. bananna
      iii. Clas$-1s+Boring
      iv. kglem23+fy
      v. cat glasses fishbowl jabba
   (b) Which of the following is *not* an authentication mechanism?
      i. biometrics
      ii. location
      iii. password
      iv. public key (the key, not the cryptosystems)
   (c) Which of the following best describes a computer worm?
      i. A program that copies itself into other programs
      ii. A program that copies itself to other computer systems
      iii. A program that copies keystrokes and sends them to another system over the network
      iv. A program that accepts commands from a remote server and sends spam to a list of emails
   (d) Which of the following defines the principle of open design?
      i. No part of the design or implementation of a system should be kept secret.
      ii. At least two publicly disclosed conditions should be met before access is granted.
      iii. Security should never depend on secrecy of design or implementation.
      iv. The simpler the design, the greater the security.
4. What is a digital signature? Please give an example of a situation in which it would be necessary.
5. Why is a precise statement of security requirements critical to determining whether a given system is secure?
6. Microsoft has stated that some of its Windows operating systems have on the order of 33.5 *million* lines of code. What are the security implications of this? Please be explicit.