Sample Midterm

1. Please define the following terms in one or two sentences.
   (a) assurance
   (b) firewall
   (c) availability
   (d) cypherpunk remailer

2. Please circle the best answer, and justify it.
   (a) Which of the following is a good password?
      i. Mary
      ii. bananna
      iii. Clas$-1s+Boring
      iv. kglem23+fy
   (b) Which of the following is not an access control model?
      i. DAC
      ii. ORCON
      iii. RBAC
      iv. FTP
   (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 is not a principle of secure programs?
      i. Paranoia: assume the user will try to attack the system using the program
      ii. Stupidity; assume the user will not know anything about the program
      iii. Impossibility: assume anything that can’t happen, will happen
      iv. Clarity: assume the user needs to know, and rely on, the way the internals of the program works

3. What is non-repudiation? Please give an example of a situation requiring non-repudiation.

4. Why is a precise statement of security requirements critical to the determination of whether a given system is secure?

5. 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.