Sample Final

These are sample questions that are very similar to the ones I will ask on the midterm. I expect the final will be approximately the same length.

1. Consider a system that used the Bell-LaPadula model to enforce confidentiality and the Biba model to enforce integrity.
   (a) If the security classes were the same as integrity classes, what objects could a given process (with some security class that also served as its integrity class) access?
   (b) Why is this scheme not used in practice?

2. Define each of the following terms in one short sentence:
   (a) public key cryptosystem
   (b) challenge-response
   (c) computer worm
   (d) end-to-end encryption

3. Show how ACLs and C-Lists are derived from an access control matrix.

4. Discuss the revocation problem with respect to access control lists and capabilities. How might one efficiently implement a command to revoke access to an object by one particular user?

5. What is a certificate? What is it used for?

6. The following routine reads a file name from the standard input and returns its protection mode. It treats the argument as a file name, and returns the protection mode of the file as a short integer. Identify three non-robust features of this routine, and state how to fix them.

```
/* return protection mode of the named file */
short int protmode(void)
{
    struct stat stbuf;
    char inbuf[100];

    gets(&inbuf);
    stat(inbuf, &stbuf);
    return(stbuf.st_mode&0777);
}
```