Sample Final Questions

1. 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
   e. web cookie
2. Show how ACLs and C-Lists are derived from an access control matrix.
3. 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?
4. 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?
5. Consider the problem of managing certificates. One expert said that a hierarchical scheme, such as that employed by PEM, is more likely to be used for business than the Web of Trust employed by PGP. What specific features of the hierarchical system as implemented for PEM (and for other Internet applications) led him to make this assertion? Why might these features lead him to make this statement?