IY5512: Coursework 7a

If feedback is required, coursework solutions must be submitted electronically via the course Moodle page. The deadline for receipt of submissions is 23:59 UK time on Friday 6/11/15. Coursework submissions should normally be in the form of a single pdf file. If you use Word, a free add-on to enable you to save a document in pdf format can be obtained from the Microsoft web site. Take care to ensure that you include your full name on the first page of your submission, the course number (IY5512), and the coursework number.

These questions are designed to test and extend your understanding of Part 7a of the course material.

1. The method used within Unix to protect and verify passwords has changed over time.

   a. Briefly describe four entries in the Unix `/etc/passwd` file that are relevant to authorisation and access control.
   b. How were user passwords protected when they were stored in the `/etc/passwd` file?
   c. In the context of password protection, what purposes were served by the use of random 'salt' values, and by repeated iteration of the DES algorithm?
   d. What major vulnerabilities did this approach to password protection have, independent of the cryptographic technique used?
   e. How have these problems been overcome in more recent versions of Unix?

2. MD5 has replaced a modified version of DES for use in password protection in more recent versions of Unix. Does this make any significant difference to the security of the user authentication system? Explain your answer.

3. Describe (briefly) how the Unix access control system operates. Indicate in your description which types of file operations are controlled via directories. In your answer cover the notions of permissions and classes.