T-110.4206 Information Security Technology
Exam 11.5.2007

1 Explain briefly the following concepts and acronyms related to data security. (6 p)

a) A certificate
b) Secret key encryption
c) Hash function
d) BS 7799 (ISO 17799)
e) Public key encryption
f) Buffer overflow

2 Justify briefly the following statements as either correct or false. Grading is based on the **justification** you give (6 p)

a) A rootkit is a set of programs that is used to hide the tracks of a break-in to a computer system
b) Old WWW-based services can be made secure by protecting the server computer with a firewall and by protecting the connection to the service with SSL
c) A Common Criteria -certified product may be used in any environment without fear of its security failing
d) One of the benefits of an ACL (access control list) is that it is easy to find all the access rights for an object
e) For protecting software that is offering services to the network, the easiest and overall most cost-efficient method is to keep the program code secret
f) A certificate is useless unless its validity is verified from a CRL-list

3 Firewalls (6 p)
How do packet filtering firewalls and applications level firewalls work? What are the main differences in protection offered? Give an example where a packet filtering firewall would suit better and another example where an applications level firewall would be more suitable.

4 Passwords (6 p)

a) Name and describe two attacks that are targeted towards finding the password of *any user* in the system (2 p)
b) Name and give an example of two attacks that attempt to find the password of a *specific user* and that are different from the attacks in the previous part (a) of the question. (2 p)
c) A password is an example of an authentication system that is based on the principle of "what the user knows". Name the two other principles used for user authentication and give an example of each.

5 Security policy models for multilevel and multilateral security (6 p)
Several formal or semiformal security policy models have been discussed during the course and in the course literature (BLP, Biba, etc.). Describe two of these models. You should include in your description:

- Rules used in the model, formally if possible.
- Give an example of what the system can be used for and what would then be the subjects and objects for the system.