T-110.4206 Information Security Technology
Exam 6.3.2008

1 Explain briefly the following concepts and acronyms related to data security. (6 p)
   a) Intrusion Detection
   b) MAC
   c) Malware
   d) Buffer overflow
   e) Biometrics
   f) CIA-model

2 Justify briefly the following statements as either correct or false. (6 p)
   a) Data security does not necessarily require using strong encryption algorithms.
   b) A company should store copies of important encryption keys.
   c) An e-commerce service can be designed so, that breaking the security of the front end web server does not give access to the whole system.
   d) It is possible to measure the level of security.
   e) When an intrusion is suspected, the most important thing is to disconnect the company network from the Internet.
   f) IP addresses in the Internet can not be traced.

3 a) Describe two benefits from having firewall software in a workstation in addition to the company firewall between the LAN and the Internet. (2 p)
   b) What is required from a firewall connecting a company LAN to the Internet to stop a virus inside an e-mail message? (2 p)
   c) Describe briefly one security related standard useful in designing the security for an organization. (1 p)
   d) Describe briefly a security related professional certification. (1 p)

4 Protecting information (6 p)
   a) What encryption keys are needed to send an encrypted and signed e-mail message, in a practical situation and with a largish message content? Describe how each key is used and where the key is obtained from. (3 p)
   b) Describe a method to break a password if the hash-file of a system's passwords has been obtained. (1 p)
   c) Describe one attack that can be performed against a WWW server using the input in the forms and describe how to protect the system against this attack during design and implementation. (2 p)

5 Server software, like WWW or email servers, may have vulnerabilities or security holes, which enable an attacker to gain access to the server host. How are these weaknesses created? Describe on the general level two of these vulnerabilities and how they are exploited. How would you prevent the creation of security vulnerabilities when leading a software project (list at least two methods you would use)? (6 p)