# Homework 3 Internet security

1. Two examiners are collaborating on an examination paper. They are sharing drafts of the paper with each other electronically. They are concerned other people may intercept these communications and leak the material.  
   1. Explain why encryption might be appropriate. [2]
   2. Explain why asymmetric encryption would be more suitable than symmetric encryption to encrypt their messages. [2]
   3. Writer A is using asymmetric encryption to send a file to writer B.  
        
      (i) Explain why Writer A should not use their own private key to encrypt the data. [1]

(ii) Explain why Writer A should not use their own public key to encrypt the data. [1]

(iii) A digital signature may be used to improve security. Explain how a digital signature proves that a message has come from Writer A. [4]

1. Network security can be enhanced by the use of a firewall.
   1. Define what is meant by a firewall. [1]
   2. Compare the effectiveness of firewalls that provide basic packet filtering to   
      those that use stateful inspection. [3]
2. Malicious software introduced to a network can cause damage to operating systems and data loss.
   1. Explain the difference between a Trojan, a virus and a worm. [3]
   2. Describe three precautions that users can take to minimise   
      the risk of introducing malicious software onto a single computer. [3]

[Total 20 Marks]