# Homework 3 Internet security Answers

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]  
        
      Contents of drafts can be obscured; the material is confidential;

If intercepted, the contents would be unreadable;

Only the two writers with the private key(s) to decrypt would be able to read and understand the material;

* 1. Explain why asymmetric encryption would be more suitable than symmetric encryption to encrypt their messages. [2]

Does not require a shared key; // The key is never transmitted;

Can use each other’s public key to encrypt messages

This public key does not need to be kept secret

They know that only the owner of the appropriate matching private key will be able to decrypt the contents of the drafts

The examiners might never have met so could not have exchanged a key in person

* 1. 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]  
       
     Writer A’s public key, which can decrypt this, may have been made available to people other than Writer B;

(ii) Explain why Writer A should not use their own public key to encrypt the data. [1]  
  
Only writer A’s private key can decrypt this which is unknown to writer B;

(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]

Writer A’s computer creates a hash from their message text;

The hash is encrypted using writer A’s private key;

The digital signature (encrypted hash) is appended to the original message text;

The message is sent (probably using asymmetric encryption) to writer B who uses writer A’s public key to decrypt the digital signature;

Successful decryption verifies that the owner of the public key signed the message;

A digital certificate is used to obtain and verify the owner’s public key;

1. Network security can be enhanced by the use of a firewall.
   1. Define what is meant by a firewall. [1]  
        
      Hardware or software used at the border of a network that filters traffic to determine if it should be allowed in or out of the network.
   2. Compare the effectiveness of firewalls that provide basic packet filtering to   
      those that use stateful inspection. [3]  
        
      Packet filtering only considers if the port number should be allowed through…

…whereas stateful inspection actually analyses the payload of each packet

Stateful inspection allows the firewall to keep track of a conversation between two end points determining if the payload is consistent with the requests sent out…

…but packet filtering considers every packet as unique and only passes packets through if they match an open port number.

1. 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]

A Trojan requires intervention to install and cannot self-replicate. Viruses and worms can self-replicate. A virus also requires human intervention for it to spread. Worms are self-executing.

* 1. Describe **three** precautions that users can take to minimise   
     the risk of introducing malicious software onto a single computer. [3]  
       
     1 mark for precaution identified (3 max) and the corresponding outline of benefit:

Do not open or run files that you are not sure about the contents of;

Viruses spread by a user executing files so the impact of this can be reduced

Ensure all software / OS is up-to-date;

Vulnerabilities can be utilised by worms and viruses but patching the software can protect from this;

Ensure passwords are complex and not easy to guess;

Some malicious software attempts to gain access using common passwords so this risk should be minimised;

Have an anti-virus package installed;

This type of software can scan each executed file for the presence of a virus;

Ensure virus definitions are up-to-date;

Anti-virus software needs to know about the characteristics of the latest viruses in order to be effective;

[Total 20 Marks]