Many computerised cipher systems use asymmetric encryption methods to resolve the key exchange problem that is associated with symmetric ciphers, such as the Vernam and Caesar ciphers.

0 1 . 1 Explain what the key exchange problem is, in relation to a symmetric cipher.

[2 marks]

0 1 . 2 A message is to be transmitted from computer A to computer B. The message will be encrypted using asymmetric encryption. To enable computer B to authenticate that the message was sent by computer A, a digital signature will also be sent with the message.

Explain how computer B will decrypt the message and verify that it was sent by computer A.

In your response you should refer to the specific keys that will be used in this process.

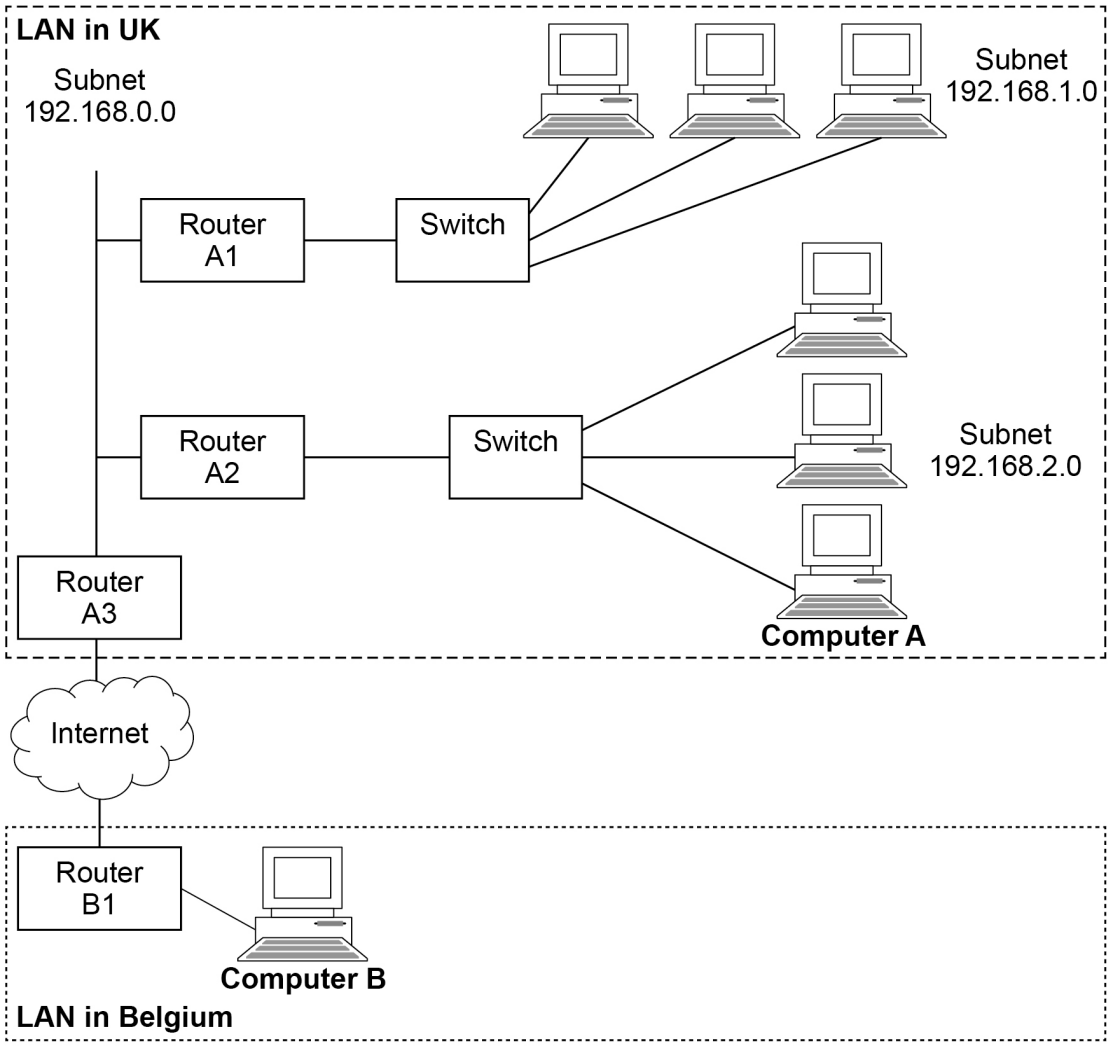
You do **not** need to explain how computer A will encrypt the message or create the digital signature.

[4 marks]

0 2 **Figure 5** shows a computer (**Computer A**) which is located on a LAN in the UK. It is connected, via the Internet, to an email server (**Computer B**) which is located on a LAN in Belgium.

Computer A has IP address 192.168.2.3 and **Computer B** has the public IP address 141.134.27.8

Figure 5



0 2 . 1 In addition to routing, **Router A3** also acts as a firewall to protect the computers on the LAN in the UK.

Explain **four** different ways that a firewall can protect computers on a LAN.

[4 marks]

0 3 . 1 When a person in the house uses the network to load a webpage it is likely that the Domain Name Server (DNS) system will be used.

Describe the main purpose of the DNS system **and** how it works.

[3 marks]

0 4 **Figure 2** shows some of the fields contained in a packet, transmitted on a computer network.

Figure 2

Destination Address	Source Address	Payload (data)	Checksum

0 4 . 1 Name **two** fields typically included in a packet which are **not** shown in **Figure 2**.

[2 marks]

Field 1 _____

Field 2 _____

0 4 . 2 Packets of data are transmitted using packet switching.

Describe the role of a router in packet switching.

[2 marks]

_____

_____

_____

_____

0 5 . 1 The booking system can be accessed through a website which uses CRUD and REST.

Describe what Uniform Resource Locators (URLs) are used for in a RESTful application.

[1 mark]

0 6 An email is being sent from User A on Computer A to User B on Computer B.

0 6 . 1 Whilst being transported across the Internet, the email data passes through a number of routers and one gateway.

Describe the additional functionality of a gateway, beyond that of a router.

[1 mark]

0 6 . 2 The email message needs to be sent securely as it contains confidential information.

The message will be encrypted using asymmetric encryption. To enable Computer B to authenticate that the message was sent by Computer A, a digital signature will also be sent with the message.

Describe how:

- Computer A will encrypt the message and create the digital signature
- Computer B will decrypt the message and verify that it was sent by Computer A.

In your response you should refer to the specific keys that will be used in this process.

[6 marks]

0 7 Anti-virus software and user training are measures that can be used to reduce the threat posed by viruses.

Describe **four other** measures that can be used to reduce the threat posed by viruses.

[4 marks]

0 8 A student has a Local Area Network (LAN) in her house. She uses one of the computers on the LAN as a web server to host a website for a club that she is a member of.

Figure 4 shows the Uniform Resource Locator (URL) of a page on the website.

Figure 4

`http://www.loveapug.org.uk/pictures/cutepugs.html`

0 8 . 1 State the protocol and domain name used in the URL in **Figure 4**.

[1 mark]

Protocol _____

Domain name _____

0 8 . 2 Describe how domain names are organised.

[2 marks]

_____

_____

_____

_____

_____

_____

0 8 . 3 Explain the service provided by Internet registries **and** why they are needed.

[2 marks]

_____

_____

_____

_____

_____

_____