QUESTION 1.

4 Both clients and servers use the Secure Socket Layer (SSL) protocol and its successor, the Transport Layer Security (TLS) protocol.

(a) **(i)** What is a protocol?

....

....

....

.... [2]

(ii) Name the client application used in this context.

.... [1]

(iii) Name the server used in this context.

.... [1]

(iv) Identify **two** problems that the SSL and TLS protocols can help to overcome.

1 ....

2 .... [2]

(b) Before any application data is transferred between the client and the serv process takes place. Part of this process is to agree the security parameters to

Describe **two** of these security parameters.

1 ....

....

....

....

2 ....

....

....

.... [4]

(c) Name **two** applications of computer systems where it would be appropriate to use the SSL or TLS protocol. These applications should be different from the ones you named in **part (a)(ii)** and **part (a)(iii)**.

1 ....

....

2 ....

.... [2]

QUESTION 2.

4 The Secure Socket Layer (SSL) protocol and its successor, the Transport Layer Security (TLS) protocol, are used in Internet communications between clients and servers.

(a) **(i)** Define the term **protocol**.

....

....

....

.... [2]

(ii) Explain the purpose of the TLS protocol.

....

....

....

....

....

.... [3]

(b) A handshake process has to take place before any exchange of data using the TLS protocol. The handshake process establishes details about how the exchange of data will occur. Digital certificates and keys are used.

The handshake process starts with:

- the client sending some communication data to the server
- the client asking the server to identify itself
- the server sending its digital certificate including the public key.

Describe, in outline, the other steps in the handshake process.

....

....

....

....

....

.... [3]

(c) Give **two** applications where it would be appropriate to use the TLS protocol.

1 ....

....

2 ....

....
[2]

QUESTION 3.

6 **(a)** The following table shows descriptions and terms relating to data transmission security.

Add appropriate descriptions and terms to complete the table.

	Description	**Term**
A	The result of encryption that is transmitted to the recipient.	....
B	The type of cryptography used where different keys are used; one for encryption and one for decryption.	....
C	....	**Digital certificate**
D	....	**Private key**

[4]

(b) The sequence of steps 1 to 7 describes what happens when setting up a se using Secure Socket Layer (SSL).

Four statements are missing from the sequence.

A	If the browser trusts the certificate, it creates, encrypts and sends the server a symmetric session key using the server's public key.
B	Server sends the browser an acknowledgement, encrypted with the session key.
C	Server sends a copy of its SSL Certificate and its public key.
D	Server decrypts the symmetric session key using its private key.

Write **one** letter (**A** to **D**) in the appropriate space to complete the sequence.

1. Browser requests that the server identifies itself.

2. ....

3. Browser checks the certificate against a list of trusted Certificate Authorities.

4. ....

5. ....

6. ....

7. Server and browser now encrypt all transmitted data with the session key.

[3]

BLANK PAGE

BLANK PAGE

QUESTION 4.

5 **(a)** Wiktor is an employee of a travel agent. He uses asymmetric encryption to s information to his manager.

Fill in the spaces with an appropriate term to complete the descriptions.

Asymmetric encryption uses different .... for encrypting and decrypting data. When Wiktor sends a message to his manager, the message is encrypted into .... using his manager's .... key. When the manager receives the message, it is decrypted using her .... key. When the manager replies, the message is encrypted using Wiktor's .... key, and when Wiktor receives the message, it is decrypted into .... using his .... key. [5]

(b) When customers pay for their travel booking online, a secure connection is established using Secure Socket Layer (SSL).

Explain how the customer's browser and the server used to collect the payment will establish a secure connection.

....

....

....

....

....

....

....

....

....

....

....

.... [6]

(c) The manager is concerned about the threat of malware to the company com

Name **two** types of malware. State what the company should do to help prevent t the malware.

The two methods of prevention must be different.

Malware type 1 ....

Prevention ....

....

Malware type 2 ....

Prevention ....

....
[4]