QUESTION 6.

2 Digital certificates are used in Internet communications. A Certificate Authority (C… for issuing digital certificates.

(a) Name **three** data items present in a digital certificate.

1 .....

2 .....

3 .....[3]

(b) The method of issuing a digital certificate is as follows:

1 A user starts an application for a digital certificate using their computer. On this computer a key pair is generated. This key pair consists of a public key and an associated private key.

2 The user submits the application to the CA. The generated ..... **(i)** ..... key and other application data are sent. The key and data are encrypted using the CA's ..... **(ii)** ..... key.

3 The CA creates a digital document containing all necessary data items and signs it using the CA's ..... **(iii)** ..... key.

4 The CA sends the digital certificate to the individual.

In the above method there are three missing words. Each missing word is either 'public' or 'private'.

State the correct word. Justify your choice.

(i) .....

Justification .....

.....[2]

(ii) .....

Justification .....

.....[2]

(iii) .....

Justification .....

.....[2]

(c) Alexa sends an email to Beena.

Alexa's email program:

- produces a message digest (hash)
- uses Alexa's private key to encrypt the message digest
- adds the encrypted message digest to the plain text of her message
- encrypts the whole message with Beena's public key
- sends the encrypted message with a copy of Alexa's digital certificate

Beena's email program decrypts the encrypted message using her private key.

(i) State the name given to the encrypted message digest.

.....[1]

(ii) Explain how Beena can be sure that she has received a message that is authentic (not corrupted or tampered with) and that it came from Alexa.

.....

.....

.....

.....[2]

(iii) Name **two** uses where encrypted message digests are advisable.

1 .....

2 .....[2]

QUESTION 7.

6 **(a)** The table below gives descriptions of three types of malware.

Description	Term
Malware that attaches itself to another program.	
Malware that redirects the web browser to a fake website.	
Email that encourages the receiver to access a website and give their banking details.	

Complete the table by adding the correct terms. [3]

(b) Ben wants to send a highly confidential email to Mariah so that only she can read it. Plain text and cipher text will be used in this communication.

(i) Explain the terms plain text and cipher text.

Plain text .....

.....

Cipher text .....

..... [2]

(ii) Explain how the use of asymmetric key cryptography ensures that only Mariah can read the email.

.....

.....

.....

.....

.....

.....

.....

..... [4]

QUESTION 8.

2 The following incomplete table shows descriptions and terms relating to malware.

(a) Complete the table with appropriate description and terms.

	Description	Term	
(i)	A standalone piece of malicious software that can replicate itself using a network.	.....	[1]
(ii)	Use email to attempt to obtain an individual's confidential data.	.....	[1]
(iii)	....	Virus	[2]

(b) State **two** vulnerabilities that the malware in **part (a)(i)** or **part (a)(iii)** can exploit.

Vulnerability 1 .....

.....

Vulnerability 2 .....

.....

[2]

Question 2 continues on the next page.

(c) Anna has to send an email to Bob containing confidential information. Bob and Anna have never sent emails to each other before.

Bob and Anna both have public and private keys.

The first step is for Anna to request that Bob sends her one of his keys.

(i) State the key that Bob sends. .....[1]

(ii) Explain how Anna can be sure that it is Bob who has sent the key.

.....

.....

.....

.....[2]

(iii) Anna has received the key from Bob.

The following incomplete table shows the sequence of actions between Anna and Bob to communicate the confidential information.

Complete the table.

The person performing the action	What that person does
Anna	Requests Bob's <answer to **part (c)(i)**> key.
Bob	.....
Anna	.....
Anna	Sends the email to Bob.
Bob	....

[4]

Question 3 begins on page 8.

QUESTION 9.

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 10.

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 11.

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]

QUESTION 12.

5 Sanjeet is a member of the public, and he wants to send a private message t
department.

(a) Explain how asymmetric encryption is used to ensure that the message remains priv

.....

.....

.....

..... [2]

(b) When the government department replies to Sanjeet, it needs to send a verified message.

Explain how asymmetric encryption can be used to ensure that it is a verified message.

.....

.....

.....

.....

.....

..... [2]

(c) The government's computer systems are vulnerable to malware.

(i) Describe **two** vulnerabilities that malware can exploit in computer systems.

1 .....

.....

.....

.....

2 .....

.....

.....

.....

[4]

(ii) Identify **one** method that can be used to restrict the effect of malware.

.....

..... [1]

QUESTION 13.

8 Digital certificates are used in internet communications. A Certificate Authority (C… for issuing a digital certificate.

(a) Identify **two** data items present in a digital certificate.

1 .....

2 .....

[2]

(b) The following paragraph describes how a digital signature is produced. Complete the paragraph by inserting an appropriate term in each space.

A ..... algorithm is used to generate a message digest from the plain text message. The message digest is ..... with the sender's ..... .

[3]