5 Ed wants to send a message securely. Before sending the message, the software encrypts it using a symmetric key.

(a) (i) Describe what is meant by **symmetric key encryption**.

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

..................................................................................................................................... [2]

(ii) State **two** drawbacks of using symmetric key encryption.

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

..................................................................................................................................... [2]

(b) The symmetric key is to be exchanged before the message is sent.
To exchange the key securely, the use of quantum cryptography is being considered.

State **two** possible benefits of using quantum cryptography.

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

..................................................................................................................................... [2]

6 Encryption is used to provide security when messages are transferred over a communication link.

(a) (i) Explain the way in which asymmetric key cryptography is used to encrypt a message being sent from one computer user to another over the Internet.

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

..................................................................................................................................... [4]

(ii) State **two** benefits of using asymmetric key cryptography.

1 ........................................................................................................................................

...........................................................................................................................................

2 ........................................................................................................................................

...........................................................................................................................................
[2]

(b) (i) Explain the way in which Transport Layer Security (TLS) provides communication security over a computer network.

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

..................................................................................................................................... [4]

**(ii)** State **two** situations where the use of TLS would be appropriate.

1 ..........................................................................................................................................

..............................................................................................................................................

2 ..........................................................................................................................................

.............................................................................................................................................. [2]

7 **(a)** A digital certificate and a digital signature are used to ensure that a message is not changed during transmission.

Write an appropriate term in each space to complete the descriptions.

A digital certificate contains the ..................................... key of the owner. A digital certificate is obtained from the ..................................... .

Before a private message is sent to the owner of the digital certificate, this key is used to ..................................... the message.

A digital signature is also sent. The message is hashed to produce a ..................................... , which is then encrypted with the sender's ..................................... key to obtain the digital signature. [5]

**(b)** State **two** encryption protocols used in data transmission.

1 .......................................................................................................................................

2 .......................................................................................................................................
[2]

**(c)** Malware can harm computer systems.

Describe **two** methods that can be used to restrict the effect of malware.

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

..................................................................................................................................... [4]

**(d)** Identify the common logic circuit given by the truth table in **part (a)**. Give the use of each output.

Logic circuit ...............................................................................................................

Use of **X** ...............................................................................................................

Use of **Y** ...............................................................................................................

[3]

**5** Complete these statements about a virtual machine.

A virtual machine is .............................................. that emulates a

.............................................. computer system.

A virtual machine allows multiple .............................................. operating systems to run

on one computer using a .............................................. operating system.

[4]

**6** Anita is studying computer science and she is confused about some of the computer security terminology as some of the words are similar.

Anita wants to know the similarities (features that are the same) and differences (features that are different) between some of the terms.

**(a)** Give the similarities **and** differences between a **public key** and a **private key**.

Similarities ...............................................................................................................

...............................................................................................................

...............................................................................................................

...............................................................................................................

...............................................................................................................

Differences ...............................................................................................................

...............................................................................................................

...............................................................................................................

...............................................................................................................

...............................................................................................................

[4]

**(b)** Give the similarities **and** differences between a **digital certificate** and a **digital signature**.

Similarities ..........................................................................................................................

..........................................................................................................................

..........................................................................................................................

..........................................................................................................................

..........................................................................................................................

Differences ..........................................................................................................................

..........................................................................................................................

..........................................................................................................................

..........................................................................................................................

..........................................................................................................................
[4]

**(c)** Give the similarities **and** differences between **phishing** and **pharming**.

Similarities ..........................................................................................................................

..........................................................................................................................

..........................................................................................................................

..........................................................................................................................

..........................................................................................................................

Differences ..........................................................................................................................

..........................................................................................................................

..........................................................................................................................

..........................................................................................................................

..........................................................................................................................
[4]

7 Sam wants to send confidential data to an organisation. He has already received the organisation’s digital certificate. The organisation has asked him to make sure that the message containing the confidential data is encrypted and is sent with a digital signature.

**(a)** Explain the process the organisation followed to obtain its digital certificate.

.......................................................................................................................................

.......................................................................................................................................

.......................................................................................................................................

.......................................................................................................................................

.......................................................................................................................................

................................................................................................................................. [3]

**(b)** Identify **two** items included in the organisation’s digital certificate that will be used when sending the message. Give a reason why each item is required.

Item 1 .............................................................................................................................

Reason ...........................................................................................................................

.......................................................................................................................................

Item 2 .............................................................................................................................

Reason ...........................................................................................................................

.......................................................................................................................................
[4]

**(c)** Identify **two** other items included in the organisation’s digital certificate.

.......................................................................................................................................

.......................................................................................................................................

.......................................................................................................................................

................................................................................................................................. [2]

**(d)** Explain how the digital signature for Sam's message is produced.

.............................................................................................................................................

.............................................................................................................................................

.............................................................................................................................................

.............................................................................................................................................

.............................................................................................................................................

.............................................................................................................................................

.............................................................................................................................................

.............................................................................................................................................

....................................................................................................................................... [4]

**8** Martha wants to send a private message to Joshua over the Internet.

**(a)** Martha and Joshua's computers have already exchanged digital certificates.

Identify **three** items that could be contained in a digital certificate.

1 ..........................................................................................................................................

..........................................................................................................................................

2 ..........................................................................................................................................

..........................................................................................................................................

3 ..........................................................................................................................................

..........................................................................................................................................
[3]

**(b)** Joshua and Martha's digital certificates are used to ensure that Martha's message has not been altered during transmission.

Explain how asymmetric encryption uses the contents of the digital certificates to ensure that the message has not been altered during transmission.

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

.................................................................................................................................... [6]

**8** Digital certificates are used in internet communications. A Certificate Authority (CA) is responsible 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]

1 **(a)** The following incomplete table shows descriptions relating to the security of data transmission.

Complete the table with the appropriate terms.

| | **Description** | **Term** |
|---|---|---|
| **A** | The original data to be transmitted as a message | ........................................ |
| **B** | An electronic document from a trusted authority that ensures authentication | ........................................ |
| **C** | An encryption method produced by a trusted authority that can be used by anyone | ........................................ |

[3]

**(b)** **(i)** Explain the purpose of a digital signature.

..............................................................................................................................................

..............................................................................................................................................

..............................................................................................................................................

........................................................................................................................................ [2]

**(ii)** Describe how a digital signature is produced for transmission with the message.

..............................................................................................................................................

..............................................................................................................................................

..............................................................................................................................................

..............................................................................................................................................

..............................................................................................................................................

..............................................................................................................................................

........................................................................................................................................ [3]

5 **(a)** Wiktor is an employee of a travel agent. He uses asymmetric encryption to send confidential 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 computer systems.

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

The two methods of prevention must be different.

Malware type 1 ..............................................................................................................

Prevention ....................................................................................................................

.......................................................................................................................................

Malware type 2 ..............................................................................................................

Prevention ....................................................................................................................

.......................................................................................................................................
[4]

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

**(a)** Explain how asymmetric encryption is used to ensure that the message remains private.

.............................................................................................................................................

.............................................................................................................................................

.............................................................................................................................................

....................................................................................................................................... [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]

**(c)** The table shows four statements about computer architecture.

Put a tick (✓) in each row to identify the computer architecture associated with each statement.

| Statement | Architecture | | |
|---|---|---|---|
| | **SIMD** | **MIMD** | **SISD** |
| Each processor executes a different instruction | | | |
| There is only one processor | | | |
| Each processor executes the same instruction input using data available in the dedicated memory | | | |
| Each processor typically has its own partition within a shared memory | | | |

[4]

**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** | ..........................................................................<br>..........................................................................<br>..........................................................................<br>.......................................................................... | **Digital certificate** |
| **D** | ..........................................................................<br>..........................................................................<br>..........................................................................<br>.......................................................................... | **Private key** |

[4]

**(b)** The sequence of steps 1 to 7 describes what happens when setting up a secure connection 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]

6 A company specialises in educational software.

(a) The company is concerned that malware might disrupt their business.

(i) Add appropriate descriptions and terms in the table.

| | Description | Term |
|---|---|---|
| **A** | Redirection to a bogus website that appears to be legitimate to gain confidential data. | ................................ |
| **B** | Use email to attempt to gain a user's confidential data. | ................................ |
| **C** | ..........................................................................................<br>..........................................................................................<br>.......................................................................................... | **Spyware** |
| **D** | ..........................................................................................<br>..........................................................................................<br>.......................................................................................... | **Worm** |

[4]

(ii) A member of staff is using the Internet to carry out research. They are worried about the threat from terms **A** and **B**.

Identify **one** solution to the each of the threats.

Term **A** ..................................................................................................................

..................................................................................................................................

Term **B** ..................................................................................................................

..................................................................................................................................
[2]

**(b)** A customer downloads a new educational software package from the company.

Explain how the customer's and the company's computers use a hashing algorithm to assure the customer that:

- the software has come from the company (is authentic) and
- no one has altered it.

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

.......................................................................................................................................[4]

5 Katarina works for a company specialising in the sale of computer parts and accessories. She works in the London office and her colleague Lucy works in the Hong Kong office. Katarina emails confidential information to Lucy so that only Lucy can read the information.

**(a)** Explain how public and private keys are used to ensure that only Lucy has a readable copy of the confidential information.

.............................................................................................................................................

.............................................................................................................................................

.............................................................................................................................................

.............................................................................................................................................

.............................................................................................................................................

.............................................................................................................................................

.............................................................................................................................................

........................................................................................................................................[4]

**(b)** Julio is buying items from the online shop. He already has an account with the shop.

Explain how the use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) helps to keep Julio's confidential information secure.

.............................................................................................................................................

.............................................................................................................................................

.............................................................................................................................................

.............................................................................................................................................

.............................................................................................................................................

........................................................................................................................................[3]

**(c)** The manager of the company is concerned about the threat of malware.

State **three** vulnerabilities that a malware can exploit.

1 ...........................................................................................................................................

.............................................................................................................................................

2 ...........................................................................................................................................

.............................................................................................................................................

3 ...........................................................................................................................................

.............................................................................................................................................

[3]

**(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]

**(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 | ........................................................................................................<br>........................................................................................................ |

[4]

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

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

| | Description | Term | |
|---|---|---|---|
| (i) | Malicious code is installed on a personal computer so that the user is misdirected to a fraudulent web site without their knowledge. | ..................................... | [1] |
| (ii) | An attempt to acquire sensitive information, often for malicious reasons, by trying to deceive the user through the contents of an email. | ..................................... | [1] |
| (iii) | ...........................................................................<br>...........................................................................<br>...........................................................................<br>...........................................................................<br>...........................................................................<br>........................................................................... | Worm | [2] |

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

Vulnerability 1 ...................................................................................................................

...................................................................................................................................

Vulnerability 2 ...................................................................................................................

...................................................................................................................................
[2]

**(c)** Digital certificates are used in internet communications. A Certificate Authority (CA) is responsible for issuing a digital certificate.

The digital certificate contains a digital signature produced by the CA.

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

1 ..........................................................................................................................

2 ..........................................................................................................................

3 ..........................................................................................................................
[3]

**(ii)** Describe how the digital signature is produced by the CA.

...................................................................................................................................

...................................................................................................................................

...................................................................................................................................

...................................................................................................................................

...................................................................................................................................

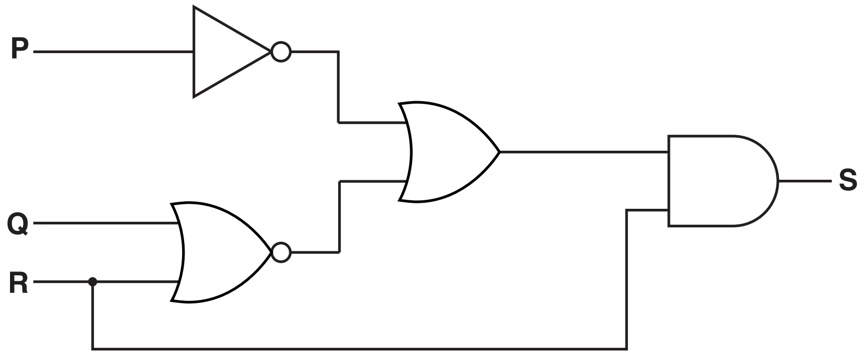
...................................................................................................................................[3]

**(iii)** Give the reason for including a digital signature in the digital certificate.

...................................................................................................................................

...................................................................................................................................[1]

**3** A logic circuit is shown:



**(a)** Write the Boolean algebraic expression corresponding to this logic circuit:

S = ..........................................................................................................................[4]

**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]

Process Y contains instructions that result in the execution of a loop, a very large number of times. All instructions within the loop are in Page 1.

The loop contains a call to a procedure whose instructions are all in Page 3.

All page frames are currently in use. Page 1 is the page that has been in memory for the shortest time.

**(iii)** Explain what happens to Page 1 and Page 3, each time the loop is executed.

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

..................................................................................................................................... [3]

**(iv)** Name the condition described in **part (c)(iii)**.

..................................................................................................................................... [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 server, a handshake process takes place. Part of this process is to agree the security parameters to be used.

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]

**2** Digital certificates are used in Internet communications. A Certificate Authority (CA) is responsible 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]

**2** Digital certificates are used in Internet communications. A Certificate Authority (CA) is responsible 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]

**3** The incomplete table below shows descriptions and terms relating to malware.

**(a)** Complete the table with appropriate descriptions and terms.

| | **Description** | **Term** |
|---|---|---|
| A | Sending emails which contain a link to a website that attempts to trick users into giving confidential personal data. | ..................................... |
| B | It replicates by inserting itself into another piece of software. | ..................................... |
| C | ..........................................................................................<br>..........................................................................................<br>.......................................................................................... | Worm |
| D | ..........................................................................................<br>..........................................................................................<br>.......................................................................................... | Spam |

[4]

**(b)** Choose term A **or** term B and describe:

- a problem that might arise for a user
- a possible solution to the problem

Term .....................

Problem ..........................................................................................................................

..........................................................................................................................................

Solution ..........................................................................................................................

..........................................................................................................................................[2]

**(c)** Explain the following terms:

Cipher text ..............................................................................................................................

...................................................................................................................................................

...................................................................................................................................................

Private key ...............................................................................................................................

...................................................................................................................................................

.............................................................................................................................................[2]

**(d)** Bill, a manager of a company, sent an email with very sensitive information to a work colleague, Alison. However, Bill also accidentally sent it to everybody in the company.

Describe the method used that ensured only Alison was able to read the original contents of the email.

...................................................................................................................................................

...................................................................................................................................................

...................................................................................................................................................

...................................................................................................................................................

...................................................................................................................................................

.............................................................................................................................................[4]

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

**(a)** Complete the table with appropriate descriptions and terms.

| | **Description** | **Term** |
|---|---|---|
| A | Unsolicited emails containing advertising material sent to a distribution list. | ........................... |
| B | A standalone piece of malicious software that can reproduce itself automatically. | ........................... |
| C | ........................................................................................<br>........................................................................................<br>........................................................................................<br>........................................................................................<br>........................................................................................ | Pharming |
| D | ........................................................................................<br>........................................................................................<br>........................................................................................<br>........................................................................................<br>........................................................................................ | Phishing |

[4]

**(b)** For one of the terms, describe:

- a problem that might arise for a user
- a possible solution to the problem

Choose between the terms:

A / B (circle your choice)

Problem ........................................................................................................................

...................................................................................................................................

Solution ........................................................................................................................

...................................................................................................................................[2]

**(c)** Explain the following terms:

Encryption ...............................................................................................................................

...............................................................................................................................

...............................................................................................................................

...............................................................................................................................

Public key ...............................................................................................................................

...............................................................................................................................

...............................................................................................................................

...............................................................................................................................[2]

**(d)** A user downloads software from the Internet.

**(i)** State what should be part of the download to provide proof that the software is authentic.

...............................................................................................................................[1]

**(ii)** Describe the process for ensuring that the software is both authentic and has not been altered.

...............................................................................................................................

...............................................................................................................................

...............................................................................................................................

...............................................................................................................................

...............................................................................................................................

...............................................................................................................................

...............................................................................................................................

...............................................................................................................................[4]