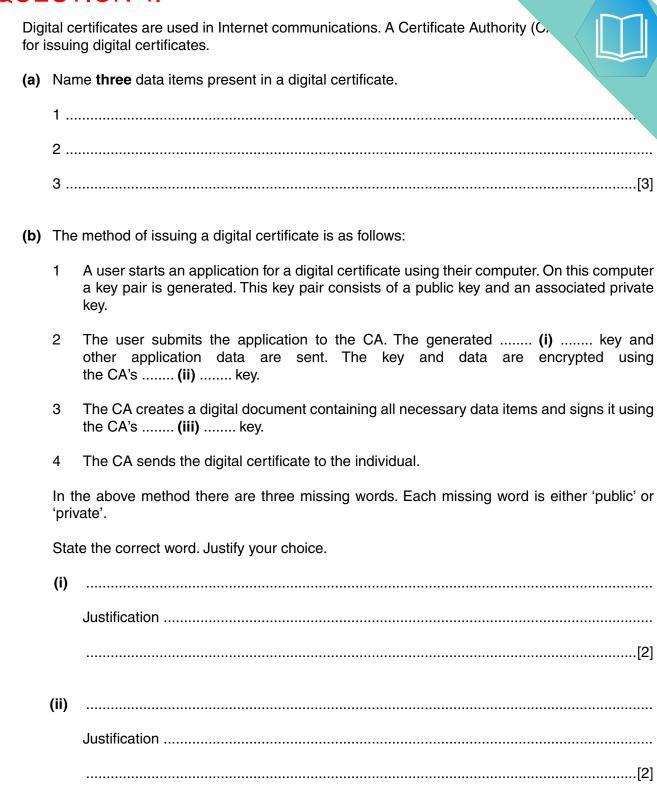
QUESTION 4.

(iii)

4



.....

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 5.

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

H			١.
ı			ı
ı			Ш
ı	L		Ш
Ľ			4

(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)			
		Worm	
			[2]
	e two vulnerabilities that the malware in part (a)(i) or p oreability 1		
Vuln	erability 2		

[2]

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



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

	anglian elemente elemente el anglian elgrianare production aly and elem	
(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.	

QUESTION 6.



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 .
		ro

	(ii)	Explain the purpose of the TLS protocol.	
			[၁]
(b)	The	andshake process has to take place before any exchange of data using the TLS protoc handshake process establishes details about how the exchange of data will occur. Digi ificates 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.	
	Des	scribe, in outline, the other steps in the handshake process.	
			[3]
(c)	Give	e two applications where it would be appropriate to use the TLS protocol.	
	1		
	2		
			 [2]

QUESTION 7.

14

3		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]

QUESTION 8.

1 (a) The following incomplete table shows descriptions relating to the security of a Complete the table with the appropriate terms.



	Description	Term
A	The original data to be transmitted as a message	
В	An electronic document from a trusted authority that ensures authentication	
С	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.