QUESTION 1.

2 (a)	• Spam • Worm **Pharming** redirect website to fake website // domain name server compromised // proxy server compromised **Phishing** through email attempt to obtain somebody's confidential data / install malware	1 1 1 1
(b)	**Spam** • user's inbox is filled by large amount of unwanted email • user / email server employs filtering software that can divert / delete spam email **Worm** • could corrupt user's computer // delete data // consume bandwidth • run anti-virus software in the background // not connect to the Internet // keep OS up-to-date	 1 1 **or** 1 1

(c)	**encryption**: process of turning plain text into cipher text **public key**: key widely available that can be used to encrypt message that only owner of private key can decrypt // can be used to decrypt a message thereby confirming originator of message	1
(d) (i)	digital signature	1
(ii)	• software is put through hashing algorithm • hash total is encrypted with private key (digital signature) • software + encrypted hash / digital signature are sent • receiver is in possession of sender's public key • the received hash total / digital signature is decrypted with public key (SH) • the receiver hashes received software (RH) • If SH matches RH then software is authentic and has not been altered	Any **four** points 1 mark each

QUESTION 2.

3	**(a)**	A Phishing B Virus C a standalone piece of software which can reproduce itself automatically D sending unsolicited emails to a distribution list	1 1 1 1
	(b)	e.g. phishing **problem**: identity fraud / misuse of financial data **solution**: ignore email / don't respond to email e.g. virus **problem**: computer may stop working // lost files **solution**: running anti-virus software	 1 1 **or** 1 1
	(c)	**cipher text**: encrypted text which is not understandable **private key**: key only known to owner that can be used to encrypt message to confirm author of message // can be used by owner to decrypt a message thereby ensuring only owner can read message	1 1
	(d)	• Manager encrypts email • using public key of colleague • colleague decrypts email • using his/her private key	1 1 1 1
			Total: 12
4	**(a)**	**(i)** HomeAddress ThisHouseNo 34	1

QUESTION 3.

6 (a)

Description	Term
Malware which attaches itself to another program.	VIRUS
Malware designed to redirect the web browser to a fake website.	PHARMING
Email that encourages the receiver to access a website and give their banking details.	PHISHING

[1]

[1]

(b) (i) Plain text is the original text [1]

Cipher text is the encrypted version of the plain text [1]

(ii) Asymmetric keys means that the key used to encrypt (public key) is different from the key used to decrypt (private key) [1]
Ben acquires Mariah's public key [1]
Ben encrypts email … [1]
using Mariah's public key [1]
Ben sends encrypted email to Mariah [1]
Mariah decrypts email … [1]
Using her private key [1]

[Max 4]

QUESTION 4.

<table>
<tr><th>Question</th><th>Answer</th><th></th></tr>
<tr><td>2(a)(i)</td><td>Worm</td><td></td></tr>
<tr><td>2(a)(ii)</td><td>Phishing</td><td></td></tr>
<tr><td>2(a)(iii)</td><td>Malicious software that replicates by inserting a copy of itself (1)
into a file of data (1)</td><td>2</td></tr>
<tr><td>2(b)</td><td>Example:
No <u>up-to-date</u> anti-virus (or equivalent) software
Regular virus scans not performed
Operating system not up-to-date
Attachments/suspicious links clicked on
1 mark for any valid vulnerability</td><td>Max 2</td></tr>
<tr><td>2(c)(i)</td><td>public</td><td>1</td></tr>
<tr><td>2(c)(ii)</td><td>Bob sends his <u>digital certificate</u>
Digital certificate contains Bob’s public key
Successful decryption of certificate using CA’s public key provides legitimacy
1 mark for any valid point – max 2</td><td>2</td></tr>
<tr><td>2(c)(iii)</td><td>
<table>
<tr><th>The person performing the action</th><th>What that person does</th><th></th></tr>
<tr><td>Anna</td><td>Requests Bob’s public key.</td><td></td></tr>
<tr><td>Bob</td><td>Sends Anna his public key.</td><td>1</td></tr>
<tr><td>Anna</td><td>Encrypts email with <u>Bob’s public key</u>.</td><td>1</td></tr>
<tr><td>Anna</td><td>Sends the email to Bob.</td><td></td></tr>
<tr><td>Bob</td><td>Decrypts email.
Using his private key.</td><td>1
1</td></tr>
</table>
</td><td>4</td></tr>
</table>

QUESTION 5.

Question	Answer	
2(a)(i)	Pharming	
2(a)(ii)	Phishing	
2(a)(iii)	A standalone/independent piece of malicious software 1 that can replicate/duplicate itself 1	
2(b)	No up-to-date anti-virus (or equivalent) software (used) / Regular virus scans not performed No firewall Operating system not up-to-date/obsolete Attachments/suspicious links in emails clicked on Clicking on website with an out of date security certificate **max 2**	**2**
2(c)(i)	(Certificate) serial number 1 Certificate Authority (that issued certificate) 1 Valid date(s) // Date of expiry 1 Subject name (name of user/owner, computer, network device) 1 Subject public key 1 Version (Number) 1 Hashing algorithm (data or signature) 1 **max 3**	**3**
2(c)(ii)	CA uses hashing algorithm .. 1 To generate a message digest from the particular certificate 1 Message digest is encrypted with CA's private key 1	**3**
2(c)(iii)	Need to know that the certificate is genuine (and has not been altered) // Authenticate or verify it (came from the CA)	**1**

QUESTION 6.

Question	Answer	
5(a)	**1 mark** per bullet point • Keys • Cipher text • Manager's public and private keys in correct spaces • Wiktor's public and private keys in correct spaces • Plain text Asymmetric encryption uses different **keys** for encrypting and decrypting data. When Wiktor sends a message to his manager, the message is encrypted into **cipher text** using his manager's **public** key. When the manager receives the message, it is decrypted using her **private** key. When the manager replies, the message is encrypted using Wiktor's **public** key, and when Wiktor receives the message, it is decrypted into **plain text** using his **private** key.	
5(b)	**1 mark** per bullet point (**max 6**) • Browser requests that the server identifies itself • Server sends a copy of its (Digital) Certificate • … containing its public key • Browser checks the certificate • …against a list of trusted Certificate Authorities • If the browser trusts the certificate • … a symmetric session key is created • …this is (by the browser) encrypted using the server's public key and sent to the server • Server decrypts the symmetric session key • … using its private key • Server and browser now encrypt all transmitted data with the session key	**6**
5(c)	**1 mark** for type of malware and **1 mark** for prevention, **max 2 (x 2)** For example: • Virus • Have company policies to ensure that anti-virus software is installed, regularly updated and run • Spyware • Have company policies to ensure that anti-spyware software is installed, regularly updated and run • Phishing • Have network policies to ensure that the firewall criteria include SPAM filters, whitelist, blacklist etc.	**4**

QUESTION 7.

Question	Answer	Marks
5(a)	**1 mark** per bullet point • Sanjeet's computer/software encrypts the message with the government department's public key • The government department's computer/software decrypts the message with their private key	**2**
5(b)	**1 mark** per bullet point (max 2) • The government department's computer/software creates the message digest • Sanjeet's computer/software recreates this message digest • If both copies of the message digest match the message has been verified	**2**

Question	Answer	
5(c)(i)	For each of the two: **1 mark** for the identification of the **vulnerability** and **1 mark** for further description, effect or example e.g. not updating virus definitions (1 mark) which would allow for recently developed viruses to attack the computer system (1 mark) opening email from unknown sources (1 mark) download a virus (1 mark)	
5(c)(ii)	**1 mark** from: • Anti-malware software running in the background • up-to-date anti-virus (definitions) • logging off when not using computer • ensuring firewall is enabled • strong password • not sharing passwords, etc.	**1**