QUESTION 4.

2 (a)	Examples: Serial number Certificate Authority that issued certificate CA digital signature Name of company/organisation/individual/subject/owner owning Certificate 'Subject' public key Period during which Certificate is valid // some relevant date	**A mark for each correct data item –** **Max 3**
(b) (i)	Public The individual keeps their private key private // the public key can be known by others (the public)	**1** **1**
(ii)	Public The individual does not know the private key of the CA // the individual only knows the public key of the CA // only the CA can decrypt the packaged information	**1** **1**

(iii)	Private 'Only' the CA's public key will allow decryption of the Certificate // proving the certificate was issued by the CA	
(c) (i)	Digital signature	**1**
(ii)	Alexa's digital certificate (Includes) Alexa's public key Used to hash message received // produce message digest Generated hash compared to digital signature	**1** **1** **1** **1** **Max 2**
(iii)	Examples: Financial transaction Legal document	 **1** **1**

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	
4(a)(i)	A (known) set of rules 1 Agreed/standard method for data transmission // governs how two devices communicate 1	
4(a)(ii)	**Max 2 marks** for purpose: • Purpose of TLS is to provide for secure communication (over a network) • maintain data integrity • additional layer of security **Max 2 marks** for further explanation from: • TLS provides improved security over SSL • TLS is composed of two layers / record protocol and handshake protocol • TLS protects this information by using encryption • Also allows for authentication of servers and clients	**Max 3**
4(b)	• The client validates (the server's) TLS Certificate • The client sends its digital certificate (to the server if requested) • Client sends an encrypted message to the server using the server's public key • The server can use its private key to decrypt the message … • … and get data needed for generating symmetric key • Both server and client compute symmetric key (to be used for encrypting messages) // session key established • The client sends back a digitally signed acknowledgement to start an encrypted session • The server sends back a digitally signed acknowledgement to start an encrypted session **1 mark** for each point, **max 3** points	**3**
4(c)	Applications, for example: • online banking • private email • online shopping • online messaging etc. **1 mark** for each point, **Max 2**	**2**

Question	Answer	Marks

QUESTION 7.

Question	Answer	Marks
8(a)	**1 mark** per bullet point to **max 2** • Serial number • Identification of Certificate Authority (that issued the certificate) • Version (number) • Valid from // start date • Valid to // end date • Subject name (name of user/owner/computer/network device) • Subject's public key • Hashing algorithm • Algorithm used to create signature • Algorithm used to hash certificate • Hashed certificate	**2**
8(b)	**1 mark** for each correct term A **hashing** algorithm is used to generate a message digest from the plain text message. The message digest is **encrypted** with the sender's **private key**.	**3**

QUESTION 8.

<table>
<tr><th>Question</th><th>Answer</th><th></th></tr>
<tr><td>1(a)</td><td>1 mark per correct row
<table>
<tr><th></th><th>Description</th><th>Term</th></tr>
<tr><td>A</td><td>The original data to be transmitted as a message</td><td>Plain text</td></tr>
<tr><td>B</td><td>An electronic document from a trusted authority that ensures authentication</td><td><u>Digital</u> certificate</td></tr>
<tr><td>C</td><td>An encryption method produced by a trusted authority that can be used by anyone</td><td>Public key</td></tr>
</table></td><td></td></tr>
<tr><td>1(b)(i)</td><td>1 mark per bullet point to max 2

• To ensure a document is authentic // came from a trusted source
• To ensure a document has not been altered during transmission
• Non repudiation</td><td>2</td></tr>
<tr><td>1(b)(ii)</td><td>1 mark per bullet point to max 3

• The message is hashed with the agreed hashing algorithm …
• … to produce a message digest
• The message digest is encrypted with the <u>sender’s</u> private key…
• … so the digital signature can be decrypted with <u>sender’s</u> public key</td><td>3</td></tr>
</table>