QUESTION 1.

4 **(a)** **(i)** A set of rules …
governing communications/transmission of data /sending and receiving data

(ii) For example, (Web) browser / email client

(iii) For example, Web server / email server [1]

(iv) Security //example: for example, alteration of transmitted messages [1]
Privacy // for example, only intended receiver can view data [1]
Authentication // for example, trust in other party [1]

[Max 2]

(b) For example:

which protocol will be used… [1]
there are a number of different versions of the two protocols [1]
session ID … [1]
uniquely identifies a related series of messages between server and client [1]
session type … [1]
reusable or not [1]
encryption method … [1]
public / private keys to be used // asymmetric/ symmetric [1]
authentication method … [1]
use of digital certificates / use of digital signature [1]
compression … [1]
method to be used [1]

[Max 2 parameters]

[Max 4]

(c) For example:

banking [1]
private / secure email [1]
shopping [1]
financial transactions [1]
secure file transfer [1]

[Max 2]

QUESTION 2.

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 3.

<table>
<tr><th>Question</th><th>Answer</th><th>Marks</th></tr>
<tr><td>6(a)</td><td>1 mark for each term/description

<table>
<tr><th></th><th>Description</th><th>Term</th></tr>
<tr><td>A</td><td>The result of encryption that is transmitted to the recipient</td><td>Cipher text</td></tr>
<tr><td>B</td><td>The type of cryptography where different keys are used, one for encryption and one for decryption.</td><td>Asymmetric or Public key</td></tr>
<tr><td>C</td><td>Electronic document used to prove the ownership of a public key // Electronic document used to prove that the data is from a trusted source</td><td>Digital certificate</td></tr>
<tr><td>D</td><td>Key needed to decrypt data that has been encrypted by a public key // Key needed to encrypt data so that it that can be decrypted by a public key
// the key used in asymmetric encryption which is not shared</td><td>Private key</td></tr>
</table></td><td>4</td></tr>
<tr><td>6(b)</td><td>1 mark for C in the correct place
1 mark for A followed by D in any position
1 mark for D followed by B in any position

1 Browser requests that the server identifies itself
2 C
3 Browser checks the certificate against a list of trusted Certificate Authorities
4 A
5 D
6 B
7 Server and Browser now encrypt all transmitted data with the session key</td><td>3</td></tr>
</table>

QUESTION 4.

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**