Question	Answer	Marks
8(a)	**One** mark for each correct marking point **(Max 2)** • The SSL and TLS protocols provide communications security over the internet / network • … they provide **encryption** • They enable two parties to identify and authenticate each other • … and communicate with confidentiality and integrity.	**2**
8(b)	**One** mark for each correct marking point **(Max 4)** • An SSL/TLS connection is initiated by an application • … which becomes the client • The application which receives the connection becomes the server • Every new session begins with a handshake (as defined by the (SSL/TLS) protocols) • The client requests the digital certificate from the server // the server sends the digital certificate to the client • The client verifies the server's digital certificate • …and obtains the server's public key • The encryption algorithms are agreed • The symmetric • … session keys are generated / defined	**4**

Question	Answer	Marks
8(a)(i)	Any **two** from • To ensure the message is authentic // came from a trusted source • To ensure that only the intended receiver is able to **understand** the message • To ensure the message has not been altered **during transmission** • Non-repudiation, neither the sender or receiver can deny the transmission occurred	**2**
8(a)(ii)	Symmetric Asymmetric	**2**
8(b)(i)	Any **two** from • Any eavesdropping can be identified (as the state will be changed) • Integrity of the key once transferred can be guaranteed (cannot be copied and decrypted at a later date) • Longer/more secure keys can be exchanged	**2**
8(b)(ii)	Any **two** from • Limited range • requires dedicated fibre (optic) line and specialist hardware • cost of dedicated fibre (optic) line and specialist hardware is expensive • polarisation of light may be altered whilst travelling down fibre optic cables	**2**

Question	Answer	Marks
6(a)	**One** mark for each correct point (**Max 2**) • A private key is the unpublished/secret key/never transmitted anywhere. • It has a matching public key • It is used to decrypt data that was encrypted with **its** matching public key.	**2**
6(b)	**One** mark for each correct point (**Max 2**) • The message to be sent is encrypted using the **recipient's public** key. // The message to be sent is encrypted using the **sender's private** key. • The message is decrypted using the **recipient's private** key. // The message is decrypted using the **sender's public** key.	**2**
6(c)	**One** mark for each correct point (**Max 4**) • The message together with the digital signature is decrypted using the receiver's private key • The digital signature received is decrypted with the sender's public key to recover the message digest sent • The decrypted message received is hashed with the agreed hashing algorithm to reproduce the message digest of the message received • The two message digests are compared • … if **both digests** are the same the message has **not** been altered // if they are different the message has been altered.	**4**