

7(a)	One from Symmetric (cryptography / encryption) Quantum (cryptography)
7(b)	One mark per mark point (Max 4) MP1 The two keys held by the organisation are a <u>private</u> key and a <u>public</u> key MP2 The organisation makes the public key available to anyone who wishes to send them secure transmissions // The sender obtains the organisation's public key MP3 The sender uses the organisation's public key to encrypt the message / plain text // The sender uses the organisation's public key to turn the message into cipher text MP4 The organisation uses its private key to decrypt the message.

9	One mark per mark point (Max 4) MP1 the company generates a public and private key pair locally using a web browser and an RSA key generator tool, which may be part of the CA's web page MP2 the company requests a digital certificate from a Certificate Authority (CA) MP3 the CA responds with its public key and digital certificate, MP4 ... signed with its private key MP5 the company gathers authentication information e.g. its public key MP6 ... and sends it to the CA signed with the company's private key and encrypted with the CA's public key MP7 the CA verifies the received information and generates/issues the digital certificate.
---	---

7(a)	1 mark for a correct method: 1 mark each to max 2 for a corresponding description Method: Encryption Description: • Data is encoded/scrambled using a key to create cipher text • if intercepted it cannot be understood • without being decrypted using a key
7(b)	1 mark each to max 5 • The sender hashes the document / message • to produce a digest • The sender encrypts the digest to create the digital signature • The message and the signature are sent to the banker / receiver • The receiver decrypts the signature to reproduce the digest • The receiver uses the same hashing algorithm on the document received to produce a second digest • The receiver compares this digest with the one from the digital signature • If both of the receiver's digests are the same the document has not changed
7(c)	1 mark each to max 3 • The data is put through an algorithm to create a checksum value • The data and checksum are sent to the receiver • The receiver performs the same algorithm on the data • if both checksums match the data is verified

9(a)	One mark for each mark point (Max 2) MP1 Ensure security/privacy when using the internet MP2 Data encryption MP3 Identification / authentication of client and server
9(b)	One mark for each mark point (Max 2) MP1 When transmitting authentication data e.g. passwords, session cookies MP2 When transmitting data that must be protected from modification on its way to or from a server e.g. user input, or results from the server MP3 When transmitting data classified as non-public.

10	One mark for identifying a protocol and one mark for stating its purpose MP1 Handshake protocol MP2 To establish a secure and reliable connection between two devices, systems or networks // Permits the web server and client to authenticate each other to make use of encryption algorithms MP3 Record protocol MP4 Provides a secure and reliable way to send and receive data over a network // To exchange records between the client and server // Responsible for securing application data and ensuring its integrity and authenticity during transmission // Encrypts and authenticates data exchanged between a client and a server // Deals with the format for data transmission.
----	---

7	One mark for each correct marking point (Max 4) MP1 An SSL/TLS connection is initiated by an application/client. MP2 Every new session begins with a handshake as defined by the SSL/TLS protocols. MP3 The client requests the digital certificate from the server // The server sends the digital certificate to the client. MP4 The client verifies the server's digital certificate MP5 ... and obtains the server's public key. MP6 The encryption algorithms are agreed. // The symmetric session keys are generated/defined. MP7 A secure session is established between client and server.
---	--