B they use digital signatures and public keys

C they are a combination of digital certificates, public key cryptography and CAs

D they use asymmetric keys, hashing algorithms and certificate authorities

E they are a combination of digests, hashing algorithms and asymmetric cryptographic algorithms

8 SSL provides which of the following?

A message integrity only

B confidentiality only

C compression and authentication

D message integrity, confidentiality and compression

E authentication, encryption and digital signatures

9 Which of the following indicates a secure website?

A http and closed padlock

B http and open padlock

C https and closed padlock

D https and open padlock

E green closed padlock only

10 Which of the following is not part of security?

A non-repudiation

B bit streaming

C data integrity

D data privacy

E user authentication

End of chapter questions

1 a) Explain what is meant by QKD.

[2]

b) The following eleven statements refer to the transmission of an encryption key using quantum key distribution protocols.
Put each statement into its correct sequence, 1-11. The first one has been numbered for you.

[10]

sequence	statement
	the sender and receiver are now fully synchronised
	the photons are sent through four random polarisers which give one of four possible polarisations and bit values
	the process is repeated until the whole of the encryption key has been transmitted

1	the sender uses a light source to create the photons
	one of the two beam splitters is chosen at random and the photon detectors are read
	the sender now informs the recipient where, in the sequence, the correct beam splitters had been used
	the polarised photons travel along the fibre optic cable to the destination
	the encryption key can now be sent and received safely since eavesdroppers would find it impossible to crack the key code
	the sender now compares this sequence to the polarisation sequence used by the sending station
	at the destination, there are two beam splitters (diagonal and vertical/ horizontal) and two photon detectors
	the recipient sends back the sequence of beam splitters to the sender

2 **a)** Explain the terms *SSL* and *TLS*.

[3]

b) Explain the following terms used in TLS.

i) Record protocol

ii) Handshake protocol

iii) Session caching

[5]

c) Give **two** differences between SSL and TLS.

[2]

3 A user keys a URL into their browser and hits the <enter> key.
Re-order the following stages, 1-6, to show how an SSL digital certificate is used to set up a secure connection between client (user) and website.

[6]

order	**stage**
	browser and web server now encrypt all data/traffic sent over the connection using the session key and a secure communication can now take place
	client's browser requests secure pages (https) from the web server
	once trusted, the browser uses public key to agree temporary session key with web server; session key is sent back to web server
	the web server uses its private key to decrypt the session key and then sends back an acknowledgement that is encrypted using the session key
	once the client's browser gets the SSL digital certificate it checks the digital

	signature, validity of start and end dates and whether the domain listed in the certificate matches the domain requested by the user
	the web server sends back the SSL digital certificate containing the public key; this is digitally signed by a third party called the Certificate Authority (CA)

b) List **four** items found on a digital certificate.

[4]

c) Explain how a digital signature can be formed from a digital certificate.

[2]