End of chapter questions

1 a) QKD is a protocol used when sending encryption keys over a fibre optic network using quantum cryptography technology

(b) Order: 10, 2, 6, 1, 5, 9, 3, 11, 8, 4, 7

(2) (a) SSL = secure socket layer

TLS = transport layer security

- TLS is a more modern version of SSL.
- They are client-server applications.
- They are standard cryptographic protocols …
- … to ensure security, authenticated communication.
- SSL encrypts the data.
- User knows if SSL secure due to HTTP and closed padlock.

b) i) Record protocol

- can be used with or without encryption
- contains data being transferred over Internet.

ii) Handshake protocol

- permits website and client to authenticate each other and to make use of encryption algorithms
- secure session between client and website is established.

iii) Session caching

- avoids need to utilise computer time during each TLS connection
- TLS can establish either a new session or attempt to resume existing session …
- … the latter can save considerable computer time.

c) Differences between SSL and TLS

- It is possible to extend TLS by adding new authentication methods.
- TLS can make use of session caching which improves overall performance of computer compared to using SSL.
- TLS separates handshaking process from record protocol layer (which holds all the data).

3 a) Order: 6, 1, 4, 5, 3, 2

b) Items on a digital certificate

- serial number
- CA that issued the certificate
- CA digital signature
- name of company/organisation
- subject's public key
- period during which certificate is valid
- version number
- expiry date of certificate
- algorithm identification
- signature algorithm used
- company details/identifier.

(c) All certificate details condensed and put through a hashing algorithm (e.g. MD4/5) then encrypt the number using the CAs private encryption key.