Security Protocols

IMPORTANT NOTES:
Study lecture materials at least 1 hour and prepare Q1-5 prior to the tutorial session. Prepared questions will be discussed in the tutorial session.

1. What is the place of TLS in the TCP/IP network stack?
2. What are the tasks of the TLS handshake and the TLS record protocol?
3. What is the role of `ChangeCipherSpec` message in TLS record protocol?
4. How TLS prevent the man-in-middle attack?
5. IPsec operates at which layer of TCP/IP protocol stack?
6. What is the difference between Authentication Header and Encapsulating Security Payload protocols of IPsec?
7. What is the difference between Tunnel mode and Transport mode of ESP?
8. Explain why a VPN in most cases does not provide end-to-end encryption.
9. Explain the purpose of the numeric comparison or passkey entry association models in the Bluetooth LE Secure Connections protocol.