**Question 1**

**Question 2**

RSA is the algorithm used for the key exchange in the TLS handshake.

RSA is used during the exchange that is made between the client and the server whilst the secret key is computed. It is also during the exchange of messages between the server and the client.