16-124-836
Marcel Matti ZAUDER

10.2 Question 2

10.2.A Answer the following Questions

What security services are provided by TLS Record Protocol?

Which of the following parameters correspond to session state andwhich to connection state?

***server_key_exchange* message in TLS Handshake protocol contains a digital signature of the exchanged server parameters and the random values from *client_hello* and *server_hello* messages. What is the purpose of signing these two random values?**

Which certificate issue can you spot on https://bit.ly/3EwxKOt? Which TLS higher-level protocol takes care of sending certificate and other error messages?

10.2.B Match the following SSL/TLS attacks and describe how each of them can be mitigated.