TLS: Question 2 A

- What security services are provided by TLS Record Protocol?
- Which of the following parameters correspond to session state and which to connection state?
    - Peer certificate, server and client random, server and client write keys, master secret, server and client MAC secrets, cipher spec
- *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?

TLS: Question 2 B

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

CRIME	Chosen-plaintext attack on CBC mode encryption with chained IVs
Bleichenbacher attack	Authentication cookie recovery thanks to the use of compression
BEAST	Exploits SSL Renegotiation feature
"The Hacker's Choice" DDoS attack	Utilizes fixed PKCS#1 format and chosen-ciphertext weakness of RSA to decrypt *pre_master_secret*