Answer each of the following with one-line replies. You will be awarded zero marks if you give more than one-line response. Late submissions won't be evaluated.

a) Purpose of Finish messages in TLS 1.2/1.3
b) What key is used to generate Finish message in TLS 1.2?
c) What key is used to generate Finish message in TLS 1.3?
d) What part of handshake is signed in TLS 1.2 by the server ?
d1) What key is used for signing?
e) What part of handshake is signed in TLS 1.3 by the server?
e1) Why is it different from that followed in TLS 1.2?
f) What part of handshake is encrypted in TLS 1.2?
g) What part of handshake is encrypted in TLS 1.3?
g1) Why is it different from that followed in TLS 1.2?

Your answer
a. The Finish message is sent to verify whether the key exchange and authentication processes were successful.
b. The Finish message is created by encrypting the string "client/server finished" with the Symmetric Session Key.
c. The Finish message is created by encrypting the string "client/server finished" with the negotiated Session Key.
d. Server certificate step in phase 2.
d1. The private key of the server.
e. The server uses its private key to encrypt the client random, the server random, and its DH parameter.
e1.In TLS 1.2 symmetric MAC is used to ensure that the handshake has not tampered with. In TLS 1.3 all the messages are encrypted.
f. Finished Messages
g. All handshake messages after the ServerHello are encrypted.
g1. For Robustness and to reduce Vulnerability issues.