Module 6

1. The digital signature is a set of the previous messages between the client and server that is summarized using a hash function, and signed with the private key that goes with the public key on the certificate.

2. The client sends over a “hello” message to tell the server that it is there. The server then responds with its own “hello” message. In this “hello” message, the server will send a certificate, a server key exchange with the digital signature to show that it is who it says it is, and a “hello done” message. The client will then send back a public value. These can all be used to create a pre-master secret. Both the server and the client will have the pre-master secret. That secret is then combined with the random numbers from earlier in the process to create the Master Secret. The communication between the server and the client during this process is how they agree on a Master Secret.

3. The “Change Cipher Spec” is used by both the server and the client to tell the other that it is time to start encryption of messages. The “Finished Messages” are then sent over. These messages are both encrypted and should match. If they don’t, that tells either the server, client, or both (depending on who sent the different message) that the security of the connection has been compromised. This is because the “Finished Messages” are summaries of everything that has happened in the connection process.