# SSL Handshake

SSL: Secured Sockets Layer

TLS: Transport Layer Security

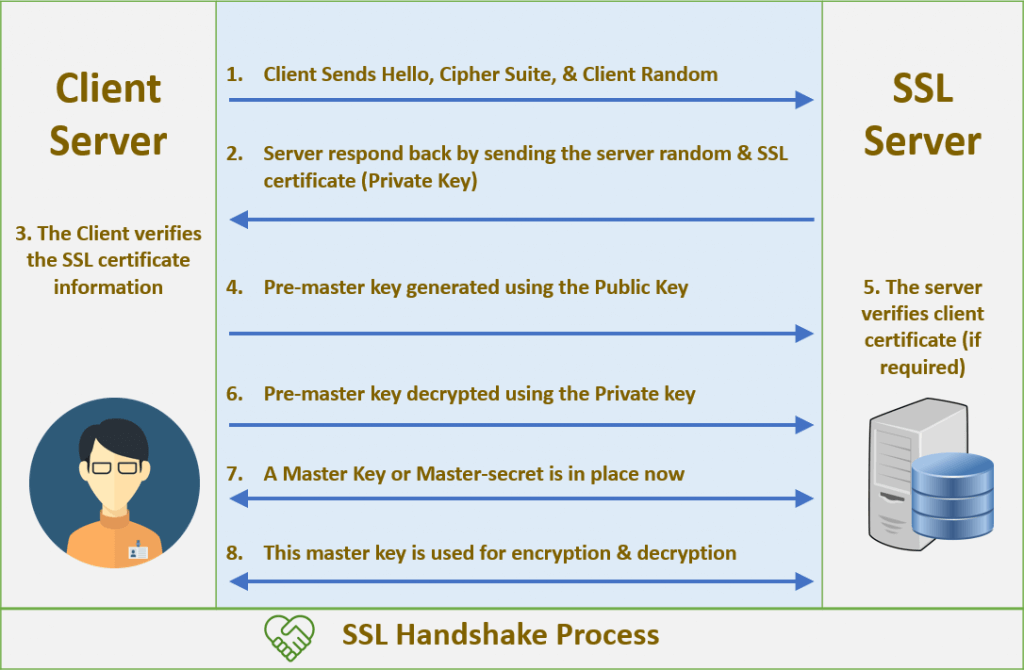
1. Client: “Hello there. I want to establish secure communication between the two of us. Here are my cipher suits and compatible SSL/TLS version.”
2. Server: “Hello Client. I have checked your cipher suits and SSL/TLS version. I think we’re good to go ahead. Here are my certificate file and my public key. Check ‘em out.”
3. Client: “Let me verify your certificate. (After a while) Okay, it seems fine, but we need to verify your private key.

What I’ll do is, I will generate and encrypt a pre-master (shared secret key) key using your public key. You Decrypt it using your private key and we’ll use this master key to encrypt and decrypt the information”

1. Server: “Done.”

[Now that both the parties know who they’re talking to, the information transferred between them will be secured using the master-key. Keep in mind that once the verification part is over, the encryption takes place through the master-key only. This is symmetric encryption.]

1. Client: “I’m sending you this sample message to verify that our master-key works. Send me the decrypted version of this message. If it works, our data is in safe hands.”
2. Server: “Yeah, it works. I think we’ve accomplished what we were looking for.”



# Public Keys, Private Keys, and Certificates

When performing authentication, SSL uses a technique called public-key cryptography.

Public-key cryptography is based on the concept of a key pair, which consists of a public key and a private key. Data that has been encrypted with a public key can be decrypted only with the corresponding private key. Conversely, data that has been encrypted with a private key can be decrypted only with the corresponding public key.

Diagram shows the use of a public key in encrypting
a word, and the use of a private key in decrypting the word.