Attachment #18 – SSL Handshake Process

Client   **Server**

1. Client Says Hello

Sends Cryptographic Info

2. Server Says Hello

Sends Crypographic Info and Server Digital Certificate

3. Secret Key Exchange

Client verify server certificate. Generate shared secret key and
send to server.

4. Client Generate Session Key

Client notifies server when finish.

5. Server Generate Session Key

Server notifies client when finish.

6. Secured Session Established.

Data exchange may begin.