Abdelrahman Adel
1701296

PAGE
DATE

Assignment 5

Theoretical

(1) In this scenario both ends will work to create a session key as follows:

1- Client Hello message
2- Server Hello message
3- Key exchange
4- Session Key Generation on both ends
5- Encryption Handshake from client to server

(2) The key exchange would change as follows:

1- Authentication of public key of website
2- Diffe-Hellman Key Exchange
3- Session Key Generation
4- Encryption Handshake

#