# Lab 7-F SSL

Name – Sati, Ankit Date – 9/30/2021

Section - 001

Total in points (Maximum 100 points)–

Professors Comments –

Affirmation of Independent Effort – Ankit Sati

1. Timing Diagram

Letter

Description automatically generated

1. The three fields are: Content type (1 byte), Version (2 bytes), Length (2 bytes).
2. Graphical user interface, text, application

   Description automatically generatedThe client hello record is:
3. Yes, the record contains “challenge”. The value of this in hexadecimal is 66 df 78 4c 04 8c d6 04 35 dc 44 89 89 46 99 09

A picture containing table

Description automatically generated

1. Yes, the record advertises the supporting cyber suites. The public key algorithm - RSA

Symmetric key - RC4 Hash algorithm - MD5

1. The specified chosen cypher suites are: The public key algorithm - RSA Symmetric key - RC4

Hash algorithm - MD5

1. Yes, there is an included nonce in the record that is of 32 bits which serves to prevent a replay attack
2. Yes, the session ID serves as a unique identifier.
3. The certificate is included in a different record and it does fit inside an Ethernet frame.
4. Yes, a pre-master secret is included in the exchange record. This is used to generate encrypted keys. This is 128 bytes in length.
5. The change cipher spec record indicates the encryption of the contents of the SSL records. This is 6 bytes in length.
6. The MAC address of the previous handshake messages is being encrypted.
7. Yes, the server sends a Change Cipher Spec record to the client to ensure that all records end up being different from the others.
8. This data is encrypted using the symmetric key encryption algorithm using the generated keys from the client and server.