# Using Google Chrome

4.a) Provide screen captures of each of the asymmetric key exchange handshake packets

Graphical user interface, text, application, Word

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

4.b) Identify the set of cipher suites (screenshot) available in the browser, and the one selected by the server.

Cipher suits avaliable:

Graphical user interface, text, application, Word

Description automatically generated

Selected:

Graphical user interface, text, application, email

Description automatically generated

4.c

Identify the place (packet) in the conversation where the client and server start using symmetric keys and explain why you think this is the place.

Text

Description automatically generated with low confidence

Assymmetric Encryption : Used for establishing secure connection between client and server.

Symmetric Encryption: Used for communication once secure connection is established.

I believe after sending each other Change cipher spec they confirm both have their session keys ready and will now use symmetric encryption for further data transfers [starting at Application Data packet].

# Working on Firefox

* 1. 5.a Provide screen captures of each of the asymmetric key exchange handshake packets

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

5.b ) Identify the set of cipher suites (screenshot) available in the browser, and the one selected by the server.

Cipher suits avaliable:

Graphical user interface, text, application, email

Description automatically generated

Selected:

Graphical user interface, text, application, email

Description automatically generated

5c

Identify the place (packet) in the conversation where the client and server start using symmetric keys and explain why you think this is the place.

The same point after change cipher spec.

Graphical user interface, text, application, email

Description automatically generated

6.a In Chrome we can see a Keep-Alive packet. The firefox browser does not keep sending a keep alive packet.

Graphical user interface, text, application, email

Description automatically generated

6.b Chrome has 16 ciphers avaliable and Firefox has 17. The GREASE one in chrome is a chrome specific reserved cipher.

Ciphers 0xc00a and 0xc009 are present in firefox but not in chrome.

Ciphers 0xcca9 and 0xcca8 are present in chrome but not in firefox.

6.c No

7. No, it now uses TLSv1.2 versus TLSv1.3 used in the above examples. TLSv1.3 is relatively new. It is picking up the stream due to faster handshake and other benefits. It also reduces latency for imporving the website perfomance. Moreover, TLS1.3 is not backward compatible with v1.2 – it poses a difficult decision for upgrading of the system. The website seems to be build on a framework that best supports TLSv1.2 and not TLSv1.3.