3. [20 marks] Negotiate This

There are two main ways a client and server can agree on a TLS ciphersuite. One is client preference: the client has an ordered list of ciphersuite preferences, and the server picks the ciphersuite that is *most* preferred by the client, and that is supported by the server. The other method is server preference: the server has a list of ciphersuite preferences and the picks the ciphersuite that is *most* preferred by the server, and that is supported by the client.

Deliverables. Place a file Q3 in a directory Q3. Thinking about ciphersuite preferences of the following clients and servers, use SSL Labs Server Test and SSL Labs Client Test to help you answer the following questions. For each of the following which ciphersuite would be selected if:

(a) Chrome 57 connected to whisperlab.org and the server picks

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

(b) Chrome 57 connected to whisperlab.org and the client picks

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

(c) Android 7.0 connected to uwo.ca and the client picks

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

(d) IE 7 / Vista connected to uwo.ca and the server picks

TLS_RSA_WITH_AES_128_CBC_SHA