**SSL/TLS Assignment**

|  |
| --- |
| * This is an individual lab assignment. * The due date is Wednesday, November 17. * For this assignment, you will need to use Wireshark and the attached “https-justlaunchpage”. * Please make the solutions readable and highlight the answers. * Follow the usual naming convention. |

*Note: Provide screenshots for each answer.*

1. What is the session ID of the SSL/TLS handshaking?

A picture containing graphical user interface, text

Description automatically generated

2. What is the length (bytes) of the certificate that the server shared with the client?

Graphical user interface, text

Description automatically generated

3A. How many cipher suites are supported by the client’s browser?

Graphical user interface, text

Description automatically generated

34

3B. What is the cipher suite that the server selected?

Graphical user interface

Description automatically generated

TLS\_RSA\_WITH\_RC4\_128\_MD5

4. What is the length of the RSA Encrypted PreMaster Secret that is used to generate the Master Secret and session keys by the server and client?

Text

Description automatically generated

5. What is the name of the company that the client is talking with?

Graphical user interface, text, application

Description automatically generated

Bank of America