**SSL/TLS Assignment**

|  |
| --- |
| * This is an individual assignment. * The due date is Tuesday, November 26, 1:00 (sec01) / 5:30 (sec76). * For this assignment, you will need to use Wireshark. * Follow the usual naming convention. |

1. What is the session ID of the SSL/TLS handshaking? List the first four hex-digits only.

**4269**

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

**4896 bytes**

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

**34 cipher suites supported**

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

**TLS\_RSA\_WITH\_RC4\_128\_MD5 (0x0004)**

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?

**128**

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

**Bank of America**