**Lab 09 Template – Ethan Roepke**

Some questions require multiple parts to be answered, be sure to discuss them in full.

**Part 01:**

1. **Screenshot of the output from openssl ec -text -in <netid>\_private\_key.pem |less (5 points)**
2. **What is the difference between the two curve identifiers? (5 points)**
3. **What does the CONNECTED(00000003) line indicate about the steps that occurred before establishing the SSL/TLS handshake? (5 points)**
4. **Take a screenshot of the client key\_share information(5 points)**
5. **What information do you think the client key\_share fields are providing to the server? How might the server use this information during the TLS 1.3 handshake to establish a secure connection?  Does this contribute to perfect forward secrecy?  Why or why not?(10 points total, 2.5 points each question)**
6. **Take a screenshot of the supported version extension for the server.  What version(s) of TLS does the server actually support?**
7. **Points total, 5 points screenshot, 5 points question)**
8. **Take a screenshot of the key\_share information.(5 points)**
9. **Take a screenshot of the certificate chain(5 points)**
10. **Look at the subject (s) and the issuer (i) for each of the two certificates.  Which number is the certificate for the Certificate Authority (CA)?  Why?**
11. **points total, 5 points for each question)**
12. **What happens if the server’s certificate validation fails at any depth?(5 points)**
13. **Expand the acronym for each piece of the cipher suite and explain the purpose of each.(10 points total, 2 points each piece)**
14. **What does “getting new key material” mean? (5 points)**
15. **Why would creating pkcs12 files be a bad idea generally speaking?(5 points)**
16. **Take a screenshot of the ciphers supported in s\_server binary. (5 points)**
17. **Find and record in your lab report at least one that should no longer be used in the real world.**  **Support your reason why it shouldn’t be used. (10 points total)**