**Lab 08 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 rsa -text -in <netid>\_private\_key.pem(10points)
2. **Comparison of the same/different values observed across the extra generated** keys. (15 points, 5 points each question)
   1. Which values are constant?
   2. Which ones vary?
   3. What do these values represent?
3. **Discussion of the differences between FTP and SFTP.** (15 points, 5 points each question)
   1. Why would you want one over the other?
   2. Why did we need to specify our private key?
   3. What protection does this offer?
4. **Screenshot of the five messages [netid]1.txt, [netid]2.txt, … [netid]5.txt**(10points)
5. **Discussion on hash verification** (10 points, 5 points each question)
   1. What is known about the message?
   2. What is the message protected against and what is it vulnerable to?
6. **Discussion on what the message generated in step 8e protected against and what it is vulnerable to (compared to the message we downloaded in step 6)**
7. points, 5 points each part)
8. **Screenshot of the signed certificate ([netid]\_certificate.pem) when looked at through openssl**(10 points)
9. **Discussion from step 12** (20 points, 10 points each answer, 10 points each why)
   1. Do any parts of the certificate match with your private key? If so, why?
   2. What was happening during the Certificate Signing process? Why did you need to submit it for signing?