Kadejha Jones

Shane McDonough

Shawn Ching

Lab 11

Random notes:

- ★ **Restart**: sudo systemctl restart nginx
- ★ Compare this to your public key: openssl pkey -in pub.key -pubin -text, are they the same?
    - Both of the public keys are almost exactly the same. However the numbers have an extra hex bite in the beginning on the nuc.
- ★ What is the error? You'll find it near the top of the output.
    - Can't use SSL _git_servername

Qanda

- If something is encrypted with your public key, what is the only way to decrypt it?
    a. They only way to decrypt it would be to have a private key, in other words you need the key pair to decrypt it.
- What purpose is served by encrypting something with your public key?
    a. The purpose is to keep the information you're sending private and by encrypting the information you can make sure the information is getting to where it is needed without being changed or seen.
- What prevents another rack from impersonating your certificate?
    a. They don't have our private key.
- The certificate also includes your public key, what is this used for?
    a. So others can send encrypted messages to us.
- The server needs to know what your private key is, why?
    a. They need to know it in order to verify that it is truly us.

- Do we really trust scrivCA? Why or why not?
    a. Yes! Because he is standing right in front of us. However, any regular person should not.