Lab 4 Report  
Exploring Public Key Certificates

**James Cook**

1. What Operating System (OS) were you using for this exercise? (Windows 7, Windows 10, MacOS 10.11, etc?)

Linux Ubuntu

1. What browser were you using for this exercise? (The exact version would be useful)

Firefox Version 135.0.1 (64-bit)

1. Referring to the first four tables in the worksheet, what observations can you make from this small sample size?

DigiCert is very common among websites. Google uses their own certification. Elliptic Curve algorithm is common as well.

1. Referring to the table in item #5 of the worksheet, what observations can you make on this small sample size?

Most websites nowadays only supports https and redirects all http connections.

1. Of those sites that support HTTPS in item #5, what is your guess as to why?

Because the sites handle sensitive information such as ID and PW which should be protected.

1. What did you learn from this exercise (if anything)?

RSA is widely used across all industries or types of websites. Financial websites entirely used RSA. This might suggest that they have high trust in RSA’s security,

1. How could this exercise be improved?

Default firefox browser is outdated and crashes on many websites, making this lab unable to complete. I had to use the latest version of firefox.