Exploring Public Key Certificates

**Items #1 through #4** provide four tables you need to fill out. Each table has five URLs that all start with “http**s**”. This prefix causes the SSL/TLS protocol to kick in, which results in the transfer of a PKI certificate from the associated website to your browser. You are going to be examining these certificates.

**For each** of the URLs in these tables, do the following:

1. Visit the URL via the browser (using http**s** as the prefix).

2. Click on the icon at the left-hand side of the address field.

3. Select the ‘>’ symbol in the popup.

4. Select **More information** from the pop-up window.

5. Select the **Security** icon.

6. Select **View Certificate** from the new window.

7. Select the **Details** tab.

8. From the **Certificate Fields** area, select the field being requested in the table.

9. Take the information from the **Field Value** area and transfer it to the table.

10. Select **Close** when you are done with the certificate.

**For item #5 of the Worksheet**.

Visit 5 other sites that you normally frequent using “http” to get there, but this time use the “http**s**”

prefix instead. Complete the table in the worksheet as you go. If HTTPS is not supported, then a

certificate will not be available to investigate. An answer of “Depends” should be given if the site only

supports HTTPS sometimes. For example, some websites suppo

Item #1 – Social Media

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| URL  **Add https:// to each URL**. | Certificate  Signature  Algorithm | Issuer (Use “O” field) | Subject  (the identity)  (Use “CN”) | Subject Public Key Algorithm | If RSA: Subject’s Public Key  (Mod bit size and exponent) | Certificate Key Usage  (**Don’t** write “Critical”) |
| [www.yahoo.com](http://www.yahoo.com/) | SHA256 | DigiCert Inc | \*.www.yahoo.com | Elliptic Curve | Mod:256  e: | Digital Signature |
| [www.facebook.com](http://www.facebook.com/) | SHA256 | DigiCert Inc | \*.facebook.com | Elliptic Curve | Mod:256  e: | Digital Signature |
| [www.twitter.com](http://www.twitter.com/) | SHA256 with RSA | DigiCert Inc | twitter.com | RSA | Mod:2048  e:65537 | Digital Signature, Key Encipherment |
| [www.youtube.com](http://www.youtube.com/) | SHA256 with RSA | Google Trust Services LLC | \*.google.com | Elliptic Curve | Mod:256  e: | Digital Signature |
| [www.pinterest.com](http://www.pinterest.com/) | SHA256 with RSA | DigiCert Inc | \*.pinterest.com | RSA | Mod:2048  e:65537 | Digital Signature, Key Encipherment |

Item #2 – Financial

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| URL  **Add** https:// **to each URL**. | Certificate  Signature  Algorithm | Issuer (Use “O” field) | Subject  (the identity)  (Use “CN”) | Subject Public Key Algorithm | If RSA: Subject’s Public Key  (Mod bit size and exponent) | Certificate Key Usage  (**Don’t** write “Critical”) |
| [www.chase.com](http://www.chase.com/) | SHA256 with RSA | Entrust, Inc. | www.chase.com | RSA | Mod:2048  e:65537 | Digital Signature, Key Encipherment |
| [www.bankofamerica.com](http://www.bankofamerica.com/) | SHA256 with RSA | Entrust, Inc. | www.bankofamerica.com | RSA | Mod:2048  e:65537 | Digital Signature, Key Encipherment |
| [www.wellsfargo.com](http://www.wellsfargo.com/) | SHA256 | DigiCert Inc | www.wellsfargo.com | RSA | Mod:2048  e:65537 | Digital Signature, Key Encipherment |
| [www.paypal.com](http://www.paypal.com/) | SHA WITH RSA | DigiCert Inc | www.paypal.com | RSA | Mod:2048  e:65537 | Digital Signature, Key Encipherment |
| [www.citibank.com](http://www.citibank.com/) | SHA WITH RSA | DigiCert Inc | www.citi.com | RSA | Mod:2048  e:65537 | Digital Signature, Key Encipherment |

Item #3 – Education

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| URL  **Add** https:// **to each URL**. | Certificate  Signature  Algorithm | Issuer (Use “O” field) | Subject  (the identity)  (Use “CN”) | Subject Public Key Algorithm | If RSA: Subject’s Public Key  (Mod bit size and exponent) | Certificate Key Usage  (**Don’t** write “Critical”) |
| [www.stanford.edu](http://www.stanford.edu/) | SHA 256 WITH RSA | Let's Encrypt | www.stanford.edu | RSA | Mod:2048  e:65537 | Digital Signature, Key Encipherment |
| [csumb.edu](http://www.csumb.edu/) | SHA 256 WITH RSA | Internet2 | csumb.edu | RSA | Mod:2048  e:65537 | Digital Signature, Key Encipherment |
| [www.usc.edu](http://www.usc.edu/) | SHA 256 WITH RSA | Amazon | www.usc.edu | RSA | Mod:2048  e:65537 | Digital Signature, Key Encipherment |
| [www.cpp.edu](http://www.cpp.edu/) | SHA 256 WITH RSA | Amazon | www.cpp.edu | RSA | Mod:2048  e:65537 | Digital Signature, Key Encipherment |
| [www.sandiego.edu](http://www.sandiego.edu/) | SHA 256 WITH RSA | Internet2 | www.sandiego.edu | RSA | Mod:2048  e:65537 | Digital Signature, Key Encipherment |

Item #4 – Non-profit

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| URL  **Add** https:// **to each URL**. | Certificate  Signature  Algorithm | Issuer (Use “O” field) | Subject  (the identity)  (Use “CN”) | Subject Public Key Algorithm | If RSA: Subject’s Public Key  (Mod bit size and exponent) | Certificate Key Usage  (**Don’t** write “Critical”) |
| [www.eff.org](http://www.eff.org/) | SHA 256 WITH RSA | Let's Encrypt | \*.eff.org | RSA | Mod:2048  e:65537 | Digital Signature, Key Encipherment |
| [www.ieee.org](http://www.ieee.org/) | SHA 256 WITH RSA | DigiCert Inc | www.ieee.org | RSA | Mod:2048  e:65537 | Digital Signature, Key Encipherment |
| [en.wikipedia.org](http://www.en.wikipedia.org/) | SHA 256 WITH RSA | Let's Encrypt | \*.wikipedia.org | Elliptic Curve | Mod:256  e: | Digital Signature |
| [www.dav.org](http://www.dav.org/) | SHA 256 WITH RSA | DigiCert Inc | \*.dav.org | RSA | Mod:2048  e:65537 | Digital Signature, Key Encipherment |
| [www.unitedway.org](http://www.unitedway.org/) | SHA 256 WITH RSA | GlobalSign nv-sa | \*.unitedway.org | RSA | Mod:2048  e:65537 | Digital Signature, Key Encipherment |

Item #5 – Personal / Other

|  |  |
| --- | --- |
| URL | HTTPS Supported  (Yes / No / Depends) |
| https://www.nfl.com/ | YES |
| https://www.webull.com/ | yes |
| https://www.nba.com/ | yes |
| https://www.usa.gov/ | yes |
| https://www.gamestop.com/ | yes |

**Debrief Questions:**

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

Windows 10

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

I started by using chrome but didn’t work. Firefox had a better system.

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

Social media isn’t very secure that is why it is hacked into a lot. Nonprofit could also be unsecure. But other things like education and financial is extremely safe.

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

Most of the websites I use are pretty secure.

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

Https is more secure then http.