Lab 4 Worksheet  
Exploring Public Key Certificates

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/) | PKCS #1 SHA-256 With RSA Encryption | DigiCert Inc | \*.fantasysports.yahoo.com | Elliptic Curve Public Key | Mod:  e: | Signing  Key Agreement |
| [www.facebook.com](http://www.facebook.com/) | PKCS #1 SHA-1 With RSA Encryption | DigiCert Inc | DigiCert High Assurance EV Root CA | PKCS #1 RSA Encryption | Mod:2048  e:65537 | Signing  Certificate Signer  CRL Signer |
| [www.twitter.com](http://www.twitter.com/) | ANSI X9.62 ECDSA Signature with SHA384 | Let's Encrypt | x.com | Elliptic Curve Public Key | Mod:  e: | Signing |
| [www.youtube.com](http://www.youtube.com/) | PKCS #1 SHA-256 With RSA Encryption | Google Trust Services | \*.google.com | Elliptic Curve Public Key | Mod:  e: | Signing |
| [www.pinterest.com](http://www.pinterest.com/) | PKCS #1 SHA-256 With RSA Encryption | DigiCert Inc | \*.pinterest.com | PKCS #1 RSA Encryption | Mod:2048  e:65537 | Signing  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/) | PKCS #1 SHA-256 With RSA Encryption | DigiCert Inc | www.chase.com | PKCS #1 RSA Encryption | Mod:2048  e:65537 | Signing  Key Encipherment |
| [www.bankofamerica.com](http://www.bankofamerica.com/) | PKCS #1 SHA-256 With RSA Encryption | "Entrust, Inc." | www.bankofamerica.com | PKCS #1 RSA Encryption | Mod:2048  e:65537 | Signing  Key Encipherment |
| [www.wellsfargo.com](http://www.wellsfargo.com/) | PKCS #1 SHA-256 With RSA Encryption | DigiCert Inc | www.wellsfargo.com | PKCS #1 RSA Encryption | Mod:2048  e:65537 | Signing  Key Encipherment |
| [www.paypal.com](http://www.paypal.com/) | PKCS #1 SHA-256 With RSA Encryption | DigiCert Inc | www.paypal.com | PKCS #1 RSA Encryption | Mod:2048  e:65537 | Signing  Key Encipherment |
| [www.citibank.com](http://www.citibank.com/) | PKCS #1 SHA-256 With RSA Encryption | DigiCert Inc | www.citi.com | PKCS #1 RSA Encryption | Mod:2048  e:65537 | Signing  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/) | PKCS #1 SHA-256 With RSA Encryption | Certainly | www.stanford.edu | PKCS #1 RSA Encryption | Mod:2048  e:65537 | Signing  Key Encipherment |
| [csumb.edu](http://www.csumb.edu/) | PKCS #1 SHA-384 With RSA Encryption | Internet2 | csumb.edu | PKCS #1 RSA Encryption | Mod:2048  e:65537 | Signing  Key Encipherment |
| [www.usc.edu](http://www.usc.edu/) | PKCS #1 SHA-256 With RSA Encryption | Let's Encrypt | about.usc.edu | PKCS #1 RSA Encryption | Mod:2048  e:65537 | Signing  Key Encipherment |
| [www.cpp.edu](http://www.cpp.edu/) | PKCS #1 SHA-256 With RSA Encryption | Amazon | www.cpp.edu | PKCS #1 RSA Encryption | Mod:2048  e:65537 | Signing  Key Encipherment |
| [www.sandiego.edu](http://www.sandiego.edu/) | PKCS #1 SHA-384 With RSA Encryption | Internet2 | www.sandiego.edu | PKCS #1 RSA Encryption | Mod:2048  e:65537 | Signing  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 Encryption | Let's Encrypt | \*.eff.org | SHA-256 with RSA Encryption | Mod:2048  e:65537 | Digital Signature, Key Encipherment |
| [www.ieee.org](http://www.ieee.org/) | SHA-256 with RSA Encryption | Amazon | \*.ieee.org | SHA-256 with RSA Encryption | Mod:2048  e:65537 | Digital Signature, Key Encipherment |
| [en.wikipedia.org](http://www.en.wikipedia.org/) | SHA-256 with RSA Encryption | Let's Encrypt | \*.wikipedia.org | Elliptic Curve | Mod:  e: | Digital Signature |
| [www.dav.org](http://www.dav.org/) | ECDSA with SHA-384 | Google Trust Services | www.dav.org | Elliptic Curve | Mod:  e: | Digital Signature |
| [www.unitedway.org](http://www.unitedway.org/) | SHA-384 with RSA Encryption | Network Solutions L.L.C. | \*.unitedway.org | SHA-384 with RSA Encryption | Mod:2048  e:65537 | Digital Signature, Key Encipherment |

Item #5 – Personal / Other

|  |  |
| --- | --- |
| URL | HTTPS Supported  (Yes / No / Depends) |
| https://blackboard.louisville.edu/ | Yes |
| https://www.amazon.com/ | Yes |
| https://www.upsers.com | Yes |
| https://web.groupme.com | Yes |
| http://httpforever.com/ | No |