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 | O = DigiCert Inc | CN = yahoo.com | Elliptic Curve Public Key | Mod: N/A  e: N/A | Signing |
| [www.facebook.com](http://www.facebook.com/) | PKCS #1 SHA-256 With RSA Encryption | O = DigiCert Inc | CN = \*.facebook.com | Elliptic Curve Public Key | Mod: N/A  e: N/A | Signing |
| [www.twitter.com](http://www.twitter.com/) | PKCS #1 SHA-256 With RSA Encryption | O = DigiCert Inc | CN = twitter.com | PKCS #1 RSA Encryption | Mod: 2048 bits  e: 65537 | Signing,  Key Encipherment |
| [www.youtube.com](http://www.youtube.com/) | PKCS #1 SHA-256 With RSA Encryption | O = Google Trust Services LLC | CN = \*.google.com | Elliptic Curve Public Key | Mod: N/A  e: N/A | Signing |
| [www.pinterest.com](http://www.pinterest.com/) | PKCS #1 SHA-256 With RSA Encryption | O = DigiCert Inc | CN = \*.pinterest.com | PKCS #1 RSA Encryption | Mod: 2048 bits  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/) | SHA-256 with RSA Encryption | O = Entrust, Inc. | CN = www.chase.com | RSA | Mod: 2048 bits  e: 65537 | Signature, Key Encipherment |
| [www.bankofamerica.com](http://www.bankofamerica.com/) | SHA-256 with RSA Encryption | O = Entrust, Inc. | CN = www.bankofamerica.com | RSA | Mod: 2048  e: 65537 | Signature, Key Encipherment |
| [www.wellsfargo.com](http://www.wellsfargo.com/) | SHA-256 with RSA Encryption | O = DigiCert Inc | CN = www.wellsfargo.com | RSA | Mod: 2048  e: 65537 | Signature, Key Encipherment |
| [www.paypal.com](http://www.paypal.com/) | SHA-256 with RSA Encryption | O = DigiCert Inc | CN = www.paypal.com | RSA | Mod: 2048  e: 65537 | Signature, Key Encipherment |
| [www.citibank.com](http://www.citibank.com/) | SHA-256 with RSA Encryption | O = DigiCert Inc | CN = www.citi.com | RSA | Mod: 2048  e: 65537 | 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 Encryption | O = Let’s Encrypt | CN = \*.stanford.edu | RSA | Mod: 2048  e: 65537 | Signature, Key Encipherment |
| [csumb.edu](http://www.csumb.edu/) | SHA-256 with RSA Encryption | O = Internet2 | CN = csumb.edu | RSA | Mod: 2048  e: 65537 | Signature, Key Encipherment |
| [www.usc.edu](http://www.usc.edu/) | SHA-256 with RSA Encryption | O = Amazon | CN = www.usc.edu | RSA | Mod: 2048  e: 65537 | Signature,  Key Encipherment |
| [www.cpp.edu](http://www.cpp.edu/) | SHA-256 with RSA Encryption | O = Amazon | CN = www.cpp.edu | RSA | Mod: 2048  e: 65537 | Signature,  Key Encipherment |
| [www.sandiego.edu](http://www.sandiego.edu/) | SHA-256 with RSA Encryption | O = Internet2 | CN = www.sandiego.edu | RSA | Mod: 2048  e: 65537 | 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 Encryption | O = Let’s Encrypt | CN = \*.eff.org | RSA | Mod: 2048  e: 65537 | Signature,  Key Encipherment |
| [www.ieee.org](http://www.ieee.org/) | SHA-256 with RSA Encryption | O = DigiCert Inc | CN = www.ieee.org | RSA | Mod: 2048  e: 65537 | Signature,  Key Encipherment |
| [en.wikipedia.org](http://www.en.wikipedia.org/) | SHA-256 with RSA Encryption | O = Let’s Encrypt | CN = \*.wikipedia.org | Elliptic Curve | Mod: N/A  e: N/A | Signature |
| [www.dav.org](http://www.dav.org/) | SHA-256 with RSA Encryption | O = Let’s Encrypt | CN = www.dav.org | RSA | Mod: 2048  e: 65537 | Signature,  Key Encipherment |
| [www.unitedway.org](http://www.unitedway.org/) | SHA-256 with RSA Encryption | O = GlobalSign nv-sa | CN = \*.unitedway.org | RSA | Mod: 2048  e: 65537 | Signature,  Key Encipherment |

Item #5 – Personal / Other

|  |  |
| --- | --- |
| URL | HTTPS Supported  (Yes / No / Depends) |
| http://fortnite.com | Yes |
| http://www.hotels.com | Yes |
| http://outof.love | Yes |
| http://www.toyota.com | Yes |
| http://www.subaru.com | Yes |