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) |  |  |  |  | Mod:  e: |  |
| [www.facebook.com](http://www.facebook.com) |  |  |  |  | Mod:  e: |  |
| [www.twitter.com](http://www.twitter.com) |  |  |  |  | Mod:  e: |  |
| [www.youtube.com](http://www.youtube.com) |  |  |  |  | Mod:  e: |  |
| [www.pinterest.com](http://www.pinterest.com) |  |  |  |  | Mod:  e: |  |

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) |  |  |  |  | Mod:  e: |  |
| [www.bankofamerica.com](http://www.bankofamerica.com) |  |  |  |  | Mod:  e: |  |
| [www.wellsfargo.com](http://www.wellsfargo.com) |  |  |  |  | Mod:  e: |  |
| [www.paypal.com](http://www.paypal.com) |  |  |  |  | Mod:  e: |  |
| [www.citibank.com](http://www.citibank.com) |  |  |  |  | Mod:  e: |  |

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) |  |  |  |  | Mod:  e: |  |
| [csumb.edu](http://www.csumb.edu) |  |  |  |  | Mod:  e: |  |
| [www.usc.edu](http://www.usc.edu) |  |  |  |  | Mod:  e: |  |
| [www.cpp.edu](http://www.cpp.edu) |  |  |  |  | Mod:  e: |  |
| [www.sandiego.edu](http://www.sandiego.edu) |  |  |  |  | Mod:  e: |  |

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) |  |  |  |  | Mod:  e: |  |
| [www.ieee.org](http://www.ieee.org) |  |  |  |  | Mod:  e: |  |
| [en.wikipedia.org](http://www.en.wikipedia.org) |  |  |  |  | Mod:  e: |  |
| [www.dav.org](http://www.dav.org) |  |  |  |  | Mod:  e: |  |
| [www.unitedway.org](http://www.unitedway.org) |  |  |  |  | Mod:  e: |  |

Item #5 – Personal / Other

|  |  |
| --- | --- |
| URL | HTTPS Supported  (Yes / No / Depends) |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |