|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Site** | **Key Exchange Method** | **Key Size (in bits)** | **Cipher Suite Chosen** | **Supports Session Resumption** | **Compression** | **Expansion** | **Certificate Authority** | **SSL Handshake** | |
| **Bytes Read** | **Bytes Written** |
| [facebook.com](http://www.google.com/url?q=http://facebook.com&usd=2&usg=ALhdy2_WHDytuUWKIMekYVE-cgx60eOs8A) | TLSv1/SSLv3 | 2048 | ECDHE-RSA-AES128-SHA | Yes | NONE | NONE | VeriSign | 4797 | 375 |
| [gmail.com](http://www.google.com/url?q=http://gmail.com&usd=2&usg=ALhdy2-BvMszBD_atYTZmUgAgm5ZH7b2sg) | TLSv1/SSLv3 | 2048 | ECDHE-RSA-RC4-SHA | Yes | NONE | NONE | Google/GeoTrust/Equifax | 3724 | 347 |
| [play.google.com](http://www.google.com/url?q=http://play.google.com&usd=2&usg=ALhdy29x8qDLBQojhD_bjpESSL2adqJZug) | TLSv1/SSLv3 | 2048 | ECDHE-RSA-RC4-SHA | Yes | NONE | NONE | Google/GeoTrust/Equifax | 10179 | 347 |
| [zionsbank.com](http://www.google.com/url?q=http://zionsbank.com&usd=2&usg=ALhdy2_vbRmuTgsd6JNTs6Z55gKZfUb05Q) | TLSv1/SSLv3 | 2048 | RC4-SHA | Yes | NONE | NONE | Entrust | 3888 | 539 |
| [discover.com](http://www.google.com/url?q=http://discover.com&usd=2&usg=ALhdy2-wHPUtizh2HrStXdiRtU86x6L14w) | TLSv1/SSLv3 | 2048 | RC4-SHA | Yes | NONE | NONE | VeriSign | 4603 | 539 |
| [github.com](http://www.google.com/url?q=http://github.com&usd=2&usg=ALhdy2-eOreyrClus9PGks7sGPHhfDTSNQ) | TLSv1/SSLv3 | 2048 | RC4-SHA | Yes | NONE | NONE | DigiCert | 3936 | 539 |
| [amazon.com](http://www.google.com/url?q=http://amazon.com&usd=2&usg=ALhdy2_qa2BsfhdbwpxAKwimCYDGs1IlHQ) | TLSv1/SSLv3 | 2048 | RC4-SHA | Yes | NONE | NONE | VeriSign | 4287 | 539 |
| [paypal.com](http://www.google.com/url?q=http://paypal.com&usd=2&usg=ALhdy29lGF-kS6frudGBBs3bNNntHEWhnw) | TLSv1/SSLv3 | 2048 | AES256-SHA | Yes | NONE | NONE | VeriSign | 4275 | 551 |
| [facwiki.cs.byu.edu](http://www.google.com/url?q=http://facwiki.cs.byu.edu&usd=2&usg=ALhdy282ryEA1NmkWxfPWlcnZy6D2xi9EQ) | TLSv1/SSLv3 | 2048 | DHE-RSA-AES256-SHA | Yes | NONE | NONE | DigiCert | 4215 | 423 |

Dallin Christensen

CS 465

Lab 7 - TLS

After seeing all of the TLS connection properties for the sites I checked, I was somewhat surprised to see that all of them used TLSv1 with a 2048 bit key. I was glad that they all use a key size that is cryptographically strong. I was also glad that all of the sites support session resumption. Another observation that I made was that the SSL handshake wrote a consistent number of bytes for each site (most of them wrote 539 bytes).

Even though a lot of the sites I looked at used an RC4-SHA cipher suite, I was surprised to see that Facebook, Google, Amazon, Paypal, and BYU all used different cipher suites.