**Digital Certificates, 9/18/2018**

* Root certificates:
  + Built into Mozilla Firefox: <https://ccadb-public.secure.force.com/mozilla/IncludedCACertificateReport>
  + The EFF SSL Observatory: <https://www.eff.org/observatory>
  + Moxie Marlinspike on the problem with root certificate authorities: <https://youtu.be/8N4sb-SEpcg>
* When Certificate Authorities fail:
  + Symantec-secured website shutdown coming soon:

<https://www.zdnet.com/article/symantec-secured-website-shutdown-coming-soon/>

* + 23,000 HTTPS certificates axed after CEO emails private keys: <https://arstechnica.com/information-technology/2018/03/23000-https-certificates-axed-after-ceo-e-mails-private-keys/>
  + Google’s plan to distrust Symantec Certificates: <https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html>
  + “Google takes Symantec to the woodshed for mis-issuing 30,000 HTTPS certs,” <https://arstechnica.com/information-technology/2017/03/google-takes-symantec-to-the-woodshed-for-mis-issuing-30000-https-certs/>
  + Symantec Employees Fired for Issuing Rogue Certificates: <http://arstechnica.com/security/2015/09/symantec-employees-fired-for-issuing-rogue-https-certificate-for-google/>
  + DigiCert purchases Symantec certificate authority business: <https://www.theregister.co.uk/2017/08/03/symantec_q1_2018/>
  + “Google Drops the Boom on WoSign, StartCom Certs for Good,” <https://arstechnica.com/information-technology/2017/07/google-drops-the-boom-on-wosign-startcom-certs-for-good/>

PGP key signing party:

* Protocol: <http://keysigning.org/methods/sassaman-projected>

Problems with PGP:

* Usability:
  + “Why Johnny Can’t Encrypt,” 1999: <https://people.eecs.berkeley.edu/~tygar/papers/Why_Johnny_Cant_Encrypt/OReilly.pdf>
  + “Why Johnny Still Can’t Encrypt,” 2015: <https://arxiv.org/pdf/1510.08555.pdf>
  + Snowden’s PGP tutorial: <https://vimeo.com/56881481>
* Criticisms of PGP:
  + Moxie Marlinspike: <http://web.archive.org/web/20180103172052/https://moxie.org/blog/gpg-and-me>
  + Matthew Green: <https://blog.cryptographyengineering.com/2014/08/13/whats-matter-with-pgp/>
  + Flippo Valsorda: <https://arstechnica.com/information-technology/2016/12/op-ed-im-giving-up-on-pgp/>
  + SilentCircle: <https://silentcircle.wordpress.com/2013/08/09/to-our-customers/>
  + XKCD: <https://xkcd.com/1181/>

Secure Messaging Apps:

* How to Keep Messages Secure (Yes, Teen Vogue!): <https://www.teenvogue.com/story/how-to-keep-messages-secure>
* Signal:
  + Profiles of Moxie Marlinspike, Signal:
    - <https://www.wired.com/2016/07/meet-moxie-marlinspike-anarchist-bringing-encryption-us/>
    - <https://www.wsj.com/articles/moxie-marlinspike-the-coder-who-encrypted-your-texts-1436486274>
  + Evading censorship in Egypt and UAE: <https://www.wired.com/2016/12/encryption-app-signal-fights-censorship-clever-workaround/>
  + <https://ssd.eff.org/en/module/how-use-signal-–-private-messenger>
  + Partnering with Skype: <https://signal.org/blog/skype-partnership/>
* WhatsApp:
  + <https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/>
  + China blocks WhatsApp: <https://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html>
  + WhatsApp stymies court order: <https://www.nytimes.com/2016/03/13/us/politics/whatsapp-encryption-said-to-stymie-wiretap-order.html>
* Payout programs for secure messaging apps: <https://zerodium.com/program.html>

**Lifelong Learning**

To learn more about cryptography, the following are some of the best and most readable books.

|  |  |
| --- | --- |
| Macintosh HD:Users:anthony:Desktop:51RRKXRP0RL._SY346_PJlook-inside-v2,TopRight,1,0_SH20_.jpg | “The Code Book” by Simon Singh.  This is a very interesting and gripping book about the history and intrigue of cryptography and cryptanalysis.  BYU Library: <http://search.lib.byu.edu/byu/id:byu2657194>  Amazon: <http://amzn.com/0470474246> |
| Macintosh HD:Users:anthony:Desktop:41Tuv9saPgL._SY346_PJlook-inside-v2,TopRight,1,0_SH20_.jpg | “Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age” by Steven Levy.  A very engaging look at the modern history of cryptography, including the development of DES, RSA, and PGP. Also, it describes the fight in the 1990’s to legalize the use of strong cryptography.  BYU Library: <http://search.lib.byu.edu/byu/id:byu2931203>  Amazon: <http://amzn.com/0140244328> |
| Macintosh HD:Users:anthony:Desktop:51oEJqoe5RL._SY346_PJlook-inside-v2,TopRight,1,0_SH20_.jpg | “The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet” by David Kahn.  The bible of the history of Cryptography. A deep dive (at 1,200 pages) but still readable.  BYU library: <http://search.lib.byu.edu/byu/id:byu2089306>  Amazon: <http://amzn.com/0684831309> |
| Macintosh HD:Users:anthony:Desktop:41bQahpPfJL.jpg | “Cryptography Engineering: Design Principles and Practical Applications” by  Niels Ferguson, Bruce Schneier, Tadayoshi “Yoshi” Kohno.  The updated successor to the classic “Applied Cryptography” by Bruce Schneier. This book explains how modern crypto works and how to implement it in your systems.  BYU Library: <http://search.lib.byu.edu/byu/id:byu4424191>  Amazon: <http://amzn.com/0470474246> |