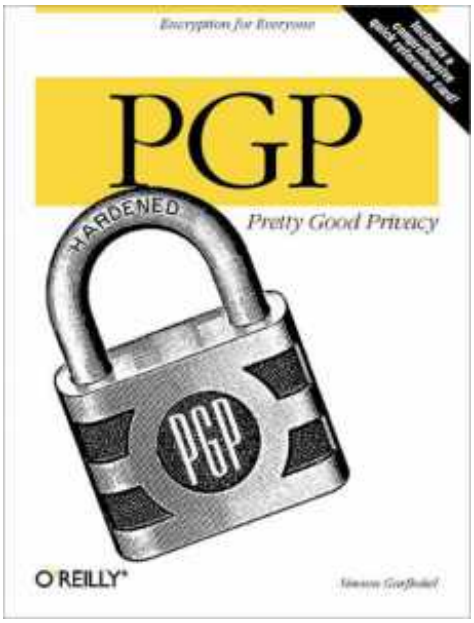
PGP: Pretty Good Privacy

thelastbastille.wordpress.com /2012/07/27/pgp-pretty-good-privacy/

Privacy is an often-underrated value in this day and age that unabashedly worships Big Brother. Both private and public snoops seek to gain advantage over others by exploiting specific pieces of information. Only truly free and sovereign individuals recognize that if they can't control what others know about them, then the Self-Ownership Axiom is nothing more than a flippant whim.



Pretty Good Privacy (aka PGP) is a type of digital mail encryption program. Email that is sent over the Internet is akin to a postcard, in that any third-party who intercepts it can read the message. Encrypted email could be analogous to a letter sealed inside of an envelope; while it is still possible for third-party interception to know whom the senders and receivers are (as well as the content of the subject line), they cannot read the message itself. PGP uniquely combines both private ***and*** public key cryptography to provide the best possible "envelope" for your email communications.

The developmental history of this truly innovative cryptographic tool is nothing less than a tenuous struggle for control between the inventor, corporate interests, and shadowy government agencies. Phil Zimmerman, Jim Bidzos, Charlie Merritt and the other assorted cast of characters reads somewhat like the founding of Facebook. First is the contest of licensing the RSA algorithm, Zimmerman's emergency release of PGP in light of the US Senate's so-called "anti-crime" bill, and then the patent dispute that eventually lead to PGP being "legally" considered munitions (thereby subject to international export controls)! FBI wiretapping and the NSA's Clipper chip were only some of the government's additional attempts to suppress this particular form of open-source public key cryptography.

While I enjoyed the history lesson, the rest of this book is completely useless. The subsequent chapters go through excruciating detail in how to use PGP *using line commands*! That is completely inapplicable with my hardware, and even if it wasn't, I'd doubt that I could obtain an older version of PGP with which to create keys using the **pgp –kg** command. Even the appendix chapter on how to install PGP for Mac showed the types of monochrome windows that I remember using on my very first laptop!

Instead of painfully trudging through this paperweight, I would recommend reading the PGP Timeline (which is a condensed history), as well as the brief yet beneficial overview of How PGP Works. The content is virtually identical and somewhat more updated. Aside from that, I would urge everyone to give PGP a try; just keep in mind that you'll need a friend to help you with it since testing it requires someone else to receive your messages and send others back.