The Encryption/Decryption Dickwads of Cipherspace

by Raleigh Muns

At White House Policy meetings, it appears, the economic side of the table is out getting coffee whenever the national security squad turns on the overhead projector.” Thus spake James Aley in Fortune (May 16, 1994, “How Not to Help High Tech”, p. 100) in reference to the worldwide battle involving one man’s efforts to bring uncrackable cryptography to the unwashed computer masses.

Philip Zimmerman, owner of Boulder Software Engineering of Boulder, Colorado, utilized a public domain mathematical formula called the RSA algorithm (for its inventors, Messrs. Rivest, Shamir, and Adelman) to independently develop state of the art “guerilla freeware” for the masses called PGP (for “Pretty Good Privacy”). Zimmerman has rationalized that since the military, the government, and organized crime all have access to cryptographically secure communications, that the common person should have the same capabilities. “When cryptography is outlawed, only outlaws will have cryptography.” Note that Zimmerman did not produce a piece of software that would be sold. He publicized the RSA algorithm and the PGP source code, and waited (successfully) for the information age axiom “information wants to be free” to take over. It did.

In a world where companies routinely claim the right to monitor employee electronic mail and telephone calls, and where post-Nixonian governments typically use illegally obtained information as leverage for attacking opponents (the media calls these “high placed anonymous sources”), the citizenry is the last to be able to communicate privately.

In a recent Wall Street Journal article (April 28, 1994, p. l), author William Bulkeley cites electronic mail from Latvia thanking Zimmerman for creating PGP which is used to keep politically unpopular information from the local Polizei. “If dictatorship takes over Russia, your PGP is widespread from Baltic to Far East now and will help democratic people if necessary.”

A common rallying cry by the “cipherpunk” community on the Internet discussion group alt.security.pgp is “They’ll have to pry my PGP from my cold, dead fingers.” This is the first Usenet discussion group in which I have seen the term “dickwad” applied to correspondents. Zimmerman himself has chimed in on occasion, though his lawyers have advised he keep mum while a Federal Grand Jury probes his role in exporting prohibited munitions. You see, PGP as “public key cryptography” has been classified by the State Department as a prohibited munitions. In the borderless world of the Internet terms such as “international export” are absurd.

While Zimmerman may be under the Federal gun for exporting weaponry, the Feds themselves have apparently exported the RSA algorithm and public key cryptographic software in various engineering proceedings with no qualms. The war being fought is fraught with yet stranger and stranger twists and turns. Those unaffiliated with sanctioned business or government agencies seem to be most likely to come under attack. If you purchase the cryptographic software from any of the companies holding the patents and copyrights, you are safe from harassment - but are your communications safe? The same people bringing you the trust-us-we-won’t-look-at-your-messages-without-a-warrant Clipper Chip only seem to have a problem with software, like PGP, which is independently developed and verified by an amorphous cadre of international cipherpunks as being free of trap doors. A “trap door” is a hook in the software which would allow “someone” to decode a message. The whole point of the Clipper Chip is to allow the government easy access to Clipper encrypted information. Examples of harassment against PGP users abound on the Internet. In the Usenet discussion group alt.security.pgp a user utilizing the name of David Sternlight has even examined a pro-PGP user’s computer files in order to report that said user has illegal PGP software on his computer account and thus should have his Internet contract revoked. “Sternlight” has become notorious as a well-spoken, literate, clean-cut opponent (who claims not to be an opponent) to the use of what he considers illegal software in violation of copyright and patent law (sounds innocuous).

Until recently, copyright and patent issues were the primary weapons used by the anti-cryptography cabal (all upstanding citizens). Stranger twist is that the copyright on the RSA algorithm isn’t valid outside the United States. The Europeans have independently developed compatible versions of PGP which are legal abroad. So Zimmerman may be accused of exporting “munitions” (cryptographic software) to countries that already have legal versions of those same “munitions”!

The current whirlpools in the rapids have found the original developers of the RSA algorithm, The Massachusetts Institute of Technology (MIT was origi-
nally funded by the U.S. Government), releasing an apparently copyright and patent safe version of PGP for the public to use. This PGP version 2.5 lasted only three days on the Internet before it was pulled by MIT or their handlers. Version 2.6 is due any day. What happened? Was there an obvious trap door that would indicate collusion by parties interested in a weakened version of PGP for the masses? Alt.security.pgp cipherpunks will be adding grist to the mill, and I will be reading it, as the next weeks pass.

Final note: Rep. Maria Cantwell (D-Washington) via the House Foreign Affairs committee, has introduced legislation which would allow the legal export of encryption software. The Clinton administration, to no one's surprise, has gone on record opposing this relaxation of the export laws. It will also be interesting to see what happens to Cantwell as time passes. Skeletons, real or otherwise, have a habit of coming out of closets around Halloween.

Raleigh Muns publishes Fugitive Pope, which Playboy recently characterized as "Ranting attempts at reincarnating a wacky librarian as a foulmouthed folk hero" that "recalls questions you had in grade school but forgot when you matured."