My Secret Life with Phil Zimmermann

>login? XXXXXXXX

>password? XXXXXX

>command? list

: text by Simson L. Garfinkel

: art by Mark Monday

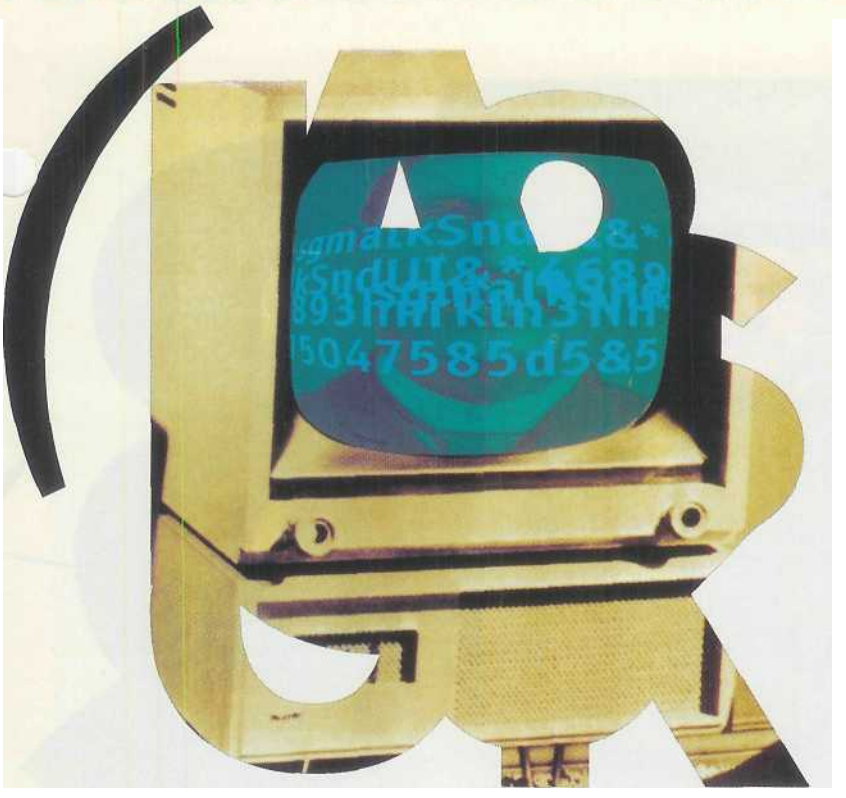
: It had all of the makings of a drug deal that was about to go bad.

: The year was 1993, and I was in a hotel room in California. Outside in the hallway was a motley collection of West Coast computer hackers, college professors and G-men from the FBI. There was even a CIA agent with whom I had just finished lunch. All of us were attending the Third Conventional on Computers, Freedom and Privacy. The main topic of debate: the U.S. Government's proposed Clipper chip and other efforts by the U.S. Government to regulate the spread of cryptography. And here I was, getting ready to thumb my nose at them all.

: In front of me stood a little man. He was well dressed, with a coat and a tie, and a trim beard. Of course, this immediately made him stand out, because the only people who were wearing ties were the feds, and this man was certainly not one of them. Just a few minutes before, this man had caught me in the hallway. "Are you Simson Garfinkel?" he asked rather quietly. "I've got something in my hotel room for you."

: I looked at his name tag. It said "Phillip R. Zimmermann." Underneath that were the initials "PGP." "Is that some sort of company?" I asked. "No," he said, "it's a program. Come with me."


BEGIN
"Anonymous" is a dirty word.



: Today Zimmermann and his program are well known, but back in March 1993, I didn't know the difference between PGP and a designer drug. But I was intrigued, so I followed him back to his room. "You are carrying a laptop computer, aren't you?" he asked.

: "Of course," I told him. "Doesn't everybody?"

: Once we were safely sequestered inside his room, I opened up my backpack and took out my Dell subnotebook. I hooked up the floppy disk drive, looked around, and was startled to see that there was a third person in the room. The third man handed me a floppy disk and told me to copy the files onto my hard disk in a special directory, "\PGP".

: "Technically, what we are doing is illegal," Zimmermann told me. I laughed, a little nervous.

: What made the our activities culpable was U.S. patent 4,405,829, which had been issued on on Sept. 20, 1983, to three MIT professors—Ron Rivest, Adi Shamir and Len Adleman. The patent covered a new mathematical technique known as public key cryptography, and it gave the patent holders the right to sue and collect damages from anyone inside the United States who used their encryption technique without first getting permission. Three days later, the professors started their own company, RSA Data Security, to realize the promise of their discovery.

: RSA was a fundamentally new kind of encryption system—truly a breakthrough. From the dawn of human history until the spring of 1977, when the MIT professors made their discovery, every encryption system ever devised had a common flaw: the keys to unlock them. Until RSA, if you wanted to send somebody a secret message, you and that person first needed to agree upon a key that you would both keep forever secret. If anybody else knew your key, then your message was as secret as yesterday's newspaper.

: With public key cryptography, everybody has two keys: a public key and a secret key. The key that locks does not unlock. So you can publish your public key in the phone book or post it on the Internet, and people that you have never met can use that key to send you secret messages. And nobody, not even the National Security Agency, can crack those messages open unless they have the matching secret key.

: There is another advantage to RSA cryptography as well—one that is often overlooked. Because the encryption algorithm is based on the a series of mathematical equations, rather than a codebook or a simple cipher, you can make RSA codes harder to break simply by using longer keys. Sure, codes with variable-length keys existed before RSA, but none of them were any good. With RSA, for the first time in the world, it was suddenly possible for ordinary citizens to create codes that the world's strongest governments couldn't crack.

: Together, these two features are RSA's greatest attraction to users, and its biggest threat.

: RSA Data Security stumbled during its first few years of operation until it was taken over by a burly Greek powerhouse named Jim Bidzos. Within a year, the company had turned profitable. Within two years, Bidzos had signed licensing agreements to put RSA's patented technology into Lotus Notes and Novel Netware. And he had also received a visit from the Feds. RSA's technology, they told him, was a threat to the nation's security. If other people overseas should start using RSA to communicate, our government wouldn't be able to spy on their electronic communications. And thus, in the interest of national security, RSA Data Security was barred from selling its best cryptography overseas. But that didn't stop Bidzos from selling the technology within the U.S., and during the following years, he built up a respectable list of companies who were bundling the technology into their products.

: In November 1986, Bidzos flew to Boulder, Colo., to meet with two promising programmers: Charlie Merritt and Phil Zimmermann. For nearly a year, Merritt and Zimmermann had been trading phone calls. Merritt had developed a version of RSA that ran on the early Z80 computer; Zimmermann wanted to take Merritt's ideas and make the program on the IBM PC. The two had planned the meeting for nearly a year. Bidzos, for his part, was looking for some programmers to help him on a contract.

: But what started out as a great opportunity for everybody to meet ended terribly—the chemistry simply wasn't there. Zimmermann said that he was thinking of moving to Canada, where his taxes wouldn't support the U.S. war machine. Bidzos, it turned out, needed the programmers to work on a contact for the Navy. After some tense moments, the three decided to go for dinner. Bidzos and Merritt wanted to go to "eat thick slabs of dead cow, drink, and smoke some fine cigars in a dim steak house," Merritt recalls. Zimmermann took them to a well-lit vegetarian restaurant.

: Before Bidzos left, he gave Zimmermann a copy of a program called MailSafe, a simple DOS-based application that allowed people to create public and private keys, encrypt files with RSA and certify keys. (Bidzos would later say that PGP ripped off all of the ideas in MailSafe; Zimmermann says that he lost the copy that Bidzos left and never ran the program.) Merritt stayed with Zimmermann the rest of the week, teaching Zimmermann everything there was to know about doing the high-speed arithmetic required for RSA. "When I left, PRZ knew how my codes worked.

He knew 95 percent of what I knew. He was now a 'real danger' to the national security machine," recalls Merritt.

That's where things stayed for five /ears, until the summer of 1991. That summer, the U.S. Senate was considering a resolution called S.266, the Senate's 1991 omnibus anti-crime bill. At the insistence of Senator Joseph R. Biden (D-Del.), a sentence was inserted that read "it is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text contents of voice, data and other communications where appropriately authorized by law."

: Many people who read this legislation took it as a direct ban on the use of cryptography within the United States. Simply put, if the Biden language had become law, it would have been illegal to use encryption within the United States that the FBI couldn't crack. (Other bastions of liberty, such as France and Singapore, already have such legislation on their books.)

: S.266 was a shot heard round cyberspace. Throughout the country, the proposal caused numerous phone calls and letters to Washington—usually to con- "essmen who had no idea what encryp- ,n was, let alone that there was a growing controversy surrounding its use. But in Boulder, Colo., S.266 did something very different: It inspired Phil Zimmermann to finish his long, drawn out encryption program.

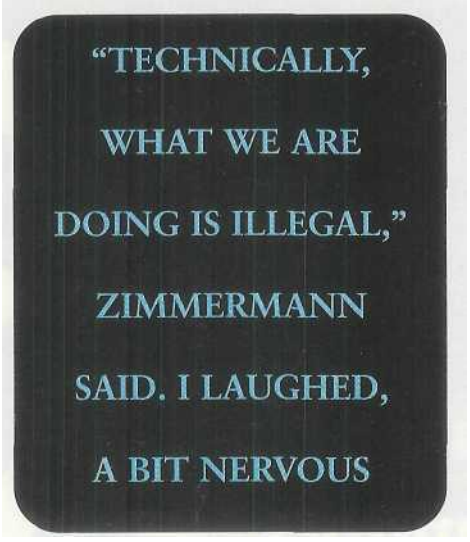
: That program was PGP 1.0. Like MailSafe, PGP 1.0 allowed people to create public and secret keys, to encrypt files and to certify keys belonging to other people. When it looked like the whole thing was working, Zimmermann gave it to a friend who posted it on the Internet.

: PGP 1.0 had a lot of problems. For starters, the RSA algorithm was good, but PGP 1.0 also used another encryption algorithm of Zimmermann's own devising. Called "Bass-O-Matic," the algorithm was not secure. But unlike other programs, PGP was released with the complete source-code, meaning that other programmers could take the program and replace the buggy parts with more stable stuff. It took an international group of programmers working from the fall of 1991 through the fall of 1992, but finally a new version of PGP was released. Called PGP 2.0, this version replaced Bass-O-Matic with a well- own encryption algorithm called . JEA, included a user interface that supported multiple human languages (French, English, Spanish and German, to name a few), and had an improved algorithm for compressing files before they were encrypted (because there was no way to compress files afterward).

: And, of course, the better PGP got, the more of a threat it posed to RSA Data Security. So just as PGP was beginning to catch on, lawyers for RSA Data Security were sending letters to universities and online services, such as CompuServe, demanding that they remove PGP from their software libraries. Even though PGP was free software, they said, it implemented algorithms that were patented.

* * *

: Back in the hotel room, Zimmermann explained to me that he had promised RSA's lawyers that he would not distribute any more copies of PGP. But that wasn't going to stop him from making sure that people got it—or from telling me his story. And over the following months, Zimmermann and I spoke often about what he was doing. A year later, the Computers, Freedom and Privacy conference was held in Chicago. I remember looking around the hotel's



lobby, when I ran across an editor from the MIT Press. He wanted to know if I knew of anybody who was interested in writing a book.

: "I'm not sure," I said, then excused myself. The editor hadn't said anything, but I was under contract to be writing a book for the Press. Somehow, though, other projects had come up, and I had never gotten around to it.

: A few minutes later, I ran into Zimmermann. "I want to write a book about PGP," he told me. Talk about serendipity.

: Over the next few months, Zimmermann and the Press talked and talked and talked. Zimmermann didn't just want to publish a book *about* PGP—he wanted to publish the program. Every single line. The reason was that he wanted to thumb his nose at the United States' antiquated laws regarding the export of encryption programs. Although it's illegal to export computer programs that implement unbreakable cryptography, as Jim Bidzos learned, it's quite legal to export books that have programs printed in their pages. So why not just print the program in an Optical Character Reader font. that could be scanned in by computer, the way groceries are?

: It wasn't that easy, of course. Even though Zimmermann didn't care about the patents on RSA, MIT did. After all, MIT owned the RSA patent, and had merely licensed it to RSA Data Security. So MIT Press first needed to figure out a way to legitimize PGP in the eyes of RSA Data Security.

: For a few months, when it looked like MIT was getting cold feet, Zimmermann came back to me and asked if I knew of any other publishers that would be interested in printing his book about PGP. I said that I would look around, and called my editor at O'Reilly & Associates, which had published my first book *(Practical UNIX Security,* 1991). It turned out that my editor at ORA was very interested in a book on PGP. So I put together a book proposal and an outline for Zimmermann, who had never written a book proposal before.

: A few months later, Zimmermann called me back and said that it looked like he was going to go ahead with the MIT Press after all. The reason: MIT had figured a way to legitimize PGP. It turned out that RSA had recently published a program called RSAREF, which was a free implementation of the RSA algorithms that was being made available for non-commercial use. All Zimmermann had to do was to take out his encryption algorithms (the ones that Charlie Merritt had taught him how to write), and put in the routines from RSA Data Security. What a hack! O'Reilly & Associates would no longer be needed.

: When I called my editor to break the bad news, we decided that a book about PGP was too good an idea to give up. If Zimmermann wouldn't write it, my editor said, then I would have to. So I did. •

O'REILLY & ASSOCIATES PUBLISHED SIMSON GARFINKEL'S BOOK *PGP: PRETTY GOOD PRIVACY* IN 1994. PHIL ZIMMERMANN'S BOOKS *THE OFFICIAL PGP USER'S GUIDE,* AND *PGP: SOURCE CODE AND INTERNALS,* WERE PUBLISHED IN 1995 BY MIT PRESS.