Security and the Internet:
The History and Uses of PGP

by
Chris Shelton

CIS 460 - Telecommunication and Networking

Don Teiser

May 1, 1995

Executive Overview

PGP is a public key encryption program which has brought powerful cryptography to the masses. Largely though the efforts of one man, Phil Zimmermann, this program has allowed anyone with access to the internet to obtain a free copy of the program that has ended the governmental monopoly on powerful encryption. By skillfully combining a number of existing tools into a highly portable program, Zimmermann created a milestone program which gave individuals access to virtually unbreakable cryptography at no cost.

The introduction of PGP was not without problems. The U.S. Senate, FBI, and RSA Data Security all fought against PGP's use on various grounds. With the release of the most recent version of PGP, the patent infringement questions posed by RSA have been solved. However, the government investigation into Zimmermann's export of munitions, the government's classification for cryptographic software, continues to this day.

PGP offers a wide variety of options to the user. These include the ability to send documents over insecure channels which can only be read by the intended recipient, and no one else. PGP also manages public and private keyrings, which are used in the encryption process. Another function of PGP is the production of digital signatures, which prove that a document was produced by a particular person. Lastly, PGP is very portable and robust; it can be compiled on almost any computer system, and can produce output which can be safely sent over the internet.

The future uses of PGP and other public key encryption programs are widespread. Many of the current problems with data security could be solved with the widespread implementation of cryptography. There are plans for expanding the use of public key cryptography into all forms of data communications. The only significant concern is the government's continuing fight to keep powerful encryption out of the hands of United States citizens.

Table of Contents

Security and the Internet: The History and Uses of PGP

Introduction

Over the past few years, the use of the internet to exchange information has expanded tremendously. The number of people using the net is difficult to gauge, but estimates of 20 to 30 million people have been made by many people. This growth is expected to continue at an exponential rate for the foreseeable future.

Most people do not realize that any information sent or received via the internet can be intercepted by any of the nodes along the path from sender to receiver. Digital communications are more susceptible to unnoticed alteration or interception than more traditional methods of communication. While information recorded on paper must be manually read by a human in order to be understood, digital information can be scanned almost instantaneously by computers that can search volumes of data looking for any requested key words, or other important information.

The news media are littered with examples of tampering with digital communications. Most of the reports include descriptions of hackers breaking in to digital vaults, and retrieving classified personal information. Most hacker attacks are harmless, as the silent investigators simply want to see if they can succeed in breaking through security systems, and do not alter the information that they uncover. However, some people use the information uncovered for personal benefit.

Who is listening to you?

If you are a trusting person, you may question the need for security when sending email messages. However, considering the potential for electronic forgery and surveillance, it is a good idea to not send any information over the internet that needs to be kept private. While it is unlikely that a random hacker will intercept your innocuous note to a friend, our government has a number of agencies with the ability, desire, and authority to eavesdrop on any of your private conversations, whether they are sent electronically or not.

Over the past couple of decades, the NSA and CIA have increased their efforts to monitor the communications of all US citizens. With the recent end of the cold war, the US intelligence community has shifted its focus inward, looking at the activities of the people they are supposedly protecting: the American people. The extent and reasons for this increased surveillance were described well by John Perry Barlow in an article that he wrote in the November 1993 issue of Communications of the ACM. In the following quote, Barlow describes the effect of Executive Order 12333, issued by President Reagan early in his first term.

> "In other words, the intelligence community was specifically charged with investigative responsibility for international criminal activities in the areas of drugs and terrorism.

Furthermore, within certain fairly loose guidelines, intelligence organizations are "authorized to collect, retain or disseminate information concerning United States persons" that may include "incidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws."

Given that the NSA monitors a significant portion of all electronic communications between the U.S. and other countries, the opportunities for "incidentally obtaining" information that might incriminate Americans inside America are great.

Also, over the course of the Reagan-Bush administrations, the job of fighting the war on drugs gradually spread to every element of the executive branch.

Even the Department of Energy is now involved. At an intelligence community conference last winter I heard a proud speech from a DOE official in which he talked about how some of the bomb-designing supercomputers at Los Alamos had been turned to the peaceful purpose of sifting through huge piles of openly available data... newspapers, courthouse records, etc., ... in search of patterns that would expose drug users and traffickers. They are selling their results to a variety of "lawful authorities," ranging from the Southern Command of the U.S. Army to the Panamanian Defense Forces to various county sheriff's departments.

History of PGP

With the expanding governmental effort to eavesdrop on private conversations, the demand for personal cryptography has increased. Because of problems with traditional, single key cryptographic algorithms, a need developed for sending secure information over insecure channels.

The problems of traditional cryptography were overcome with the introduction of the first widely available program to implement an effective public key cryptosystem: PGP. By combining several algorithms developed by others, Phil Zimmermann developed PGP. This program, which was able to run on PC’s, was originally released in June 1991. Mr. Zimmermann, in the well written help file, described why he wrote PGP.

> If privacy is outlawed, only outlaws will have privacy. Intelligence agencies have access to good cryptographic technology. So do the big arms and drug traffickers. So do defense contractors, oil companies, and other corporate giants. But ordinary people and grassroots political organizations mostly have not had access to affordable "military grade" public-key cryptographic technology. Until now.
>
> PGP empowers people to take their privacy into their own hands. There's a growing social need for it. That's why I wrote it.

In order to insure that his program would be available to anyone who wanted it, he decided to give PGP away as freeware. But the introduction of PGP had a rocky start, as many different organizations did not want the public to be able to utilize the power of PGP.

In the spring of 1991, after the end of the Gulf War, a message from Bill Murray, a security consultant for the NSA warned of a threat to publicly available cryptography. Buried within Senate Bill 266, an anti-terrorism bill authored by Senators DeConcini and Biden, was a sentence which stated that "providers...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 when appropriately authorized by law." This email message cascaded across the internet, and soon came to the attention of Phil Zimmermann. He realized that if this bill became law, it would essentially outlaw privately held cryptographic programs such as PGP.[1]

Kelly Goen, a friend of Phil Zimmermann and defender of cryptographic technology for the masses, was given a copy of PGP by Mr. Zimmermann. Upon hearing of the impending threat to private security being debated by our government, he went on a mission to distribute PGP as widely as possible.

D-day, defending freedom

On a weekend around the first of June, Goen began uploading complete PGP to systems around the U.S. He called several times, telling me his progress.

He was driving around the Bay Area with a laptop, acoustic coupler and a cellular phone. He would stop at a pay-phone; upload a number of copies for a few minutes, then disconnect and rush off to another phone miles away.

He said he wanted to get as many copies scattered as widely as possible around the nation before the government could get an injunction and stop him.

I thought he was being rather paranoid. In light of the following, perhaps he was just being realistic.

Government counter-attacks

About two years after the PGP uploads, the government began threatening to prosecute Zimmermann for illegal trafficking in munitions - cryptography. [He was first visited by U.S. Customs agents on Feb. 17, 1993.] For more than two years, they have been investigating whether he "exported" PGP. It appears at press-time that they will probably prosecute him.

The allegation seems to be that, since he permitted someone else - over whom he had no control anyway - to upload PGP to some Internet hosts inside the United States, Zimmermann thus exported this controlled munition![2]

---

[1]Warren, Jim. "The Persecution of Phil Zimmermann," Micro Times, April 1995. Posted to comp.org.cpsr.talk by Jim Warren on April 4, 1995 and reposted to alt.security.pgp on April 5, 1995 by Zbigniew Fiedorowicz.

[2]Warren, Jim. "The Persecution of Phil Zimmermann," Micro Times, April 1995. As posted to alt.security.pgp.

That's right, the federal government classifies encryption as a munition, and restricts its exportation into foreign countries. As of the writing of this paper, Phil Zimmermann's legal situation has remained unchanged. The government is still investigating his case, but has yet to begin a formal trial for trafficking in munitions.

The most recent development in this area is the federal lawsuit that the Electronic Frontier Foundation is sponsoring in an attempt to overturn the export control laws on cryptographic materials. This lawsuit, which was filed on February 21, 1995, claims that the laws regulating export of cryptographic documents and software are unconstitutional. Their press release, which was posted to numerous security and cryptographic related newsgroups as well as the EFF's web site, explains the need for more widespread use of cryptography as well as the unconstitutionality of the current laws.

> "EFF believes that cryptography is central to the preservation of privacy and security in an increasingly computerized and networked world. Many of the privacy and security violations alleged in the Kevin Mitnick case, such as the theft of credit card numbers, the reading of other people's electronic mail, and the hijacking of other peoples' computer accounts, could have been prevented by widespread deployment of this technology. The U.S. government has opposed such deployment, fearing that its citizens will be private and secure from the government as well as from other vandals.
>
> The problem is that the government currently treats cryptographic software as if it were a physical weapon and highly regulates its dissemination. Any individual or company who wants to export such software -- or to publish on the Internet any "technical data" such as papers describing encryption software or algorithms -- must first obtain a license from the State Department. Under the terms of this license, each recipient of the licensed software or information must be tracked and reported to the government. Penalties can be pretty stiff -- ten years in jail, a million dollar criminal fine, plus civil fines. This legal scheme effectively prevents individuals from engaging in otherwise legal communications about encryption.
>
> The lawsuit challenges the export-control scheme as an "impermissible prior restraint on speech, in violation of the First Amendment." Software and its associated documentation, the plaintiff contends, are published, not manufactured; they are Constitutionally protected works of human-to-human communication, like a movie, a book, or a telephone conversation. These communications cannot be suppressed by the government except under very narrow conditions -- conditions that are not met by the vague and overbroad export-control laws. In denying people the right to publish such information freely, these laws, regulations, and procedures unconstitutionally abridge the right to speak, publish, to associate with others, and to engage in academic inquiry and study. They also have the effect of restricting the availability of a means for individuals

to protect their privacy, which is also a Constitutionally protected interest."[3]

Until the laws concerning the copyrights and patents of electronically published materials have been clarified, I believe that this case will remain unsettled for a long time. However, the EFF states that it is "firmly committed to this long term project," and believes that the governments position is in violation of the Constitution.

In addition to his problems with the feds, Zimmermann was, until recently, also under attack by RSA Data Security. All versions of PGP prior to 2.6 included a public key algorithm which is patented in the United States by RSA Data Security. The most recently released versions of PGP utilize a slightly different set of algorithms which do not infringe on the patent held by RSA.

Uses of PGP

By now I hope that you are wondering what is so valuable with PGP that has caused the Senate to attempt to criminalize it, and the U.S. Customs office to investigate Phil Zimmermann for illegal export of munitions. PGP is a flexible utility program that allows the user to perform a variety of message encryption and authentication functions. By using a mixture of various command line parameters PGP will allow you to attach a digital signature to a document or binary file, compress the file, encrypt the file, and convert the encrypted file to a format suitable for transmission via email. In his book, Protect Your Privacy: A Guide for PGP Users William Stallings provided a good overview of the functions provided by PGP. Figure 1 (contained at the end of this paper), which is modeled after a similar diagram found of page 28 of Stallings' book, shows the various processes that PGP uses to provide a secure method for transfer of information.

Key Management

In addition to the processes shown on the diagram, PGP will also manage public and private key rings. The proper management of keys is the most important aspect of maintaining a secure transmission of data. PGP normally uses two different keyrings: the public keyring, and the private keyring. Your public keyring is a file which contains the keys of all people that you exchange messages with. Whenever you want to encrypt a message, PGP will ask you who the recipient is, so that their public key can be used in the encryption process. Your private keyring is usually much smaller than the public keyring. It will only contain your own private key(s) that are used to sign messages and decrypt messages sent to you by others. This keyring file must be kept secure if you want to ensure a reasonable level of privacy. However, PGP does offer a bit of extra security just in case your private keyring falls into the hands of someone else. Whenever

---

[3]McCandlish, Stanton, EFF Sues to Overturn Cryptography Restrictions, posted to numerous privacy and security related NetNewsgroups on February 21, 1995, and also available on the World Wide Web at http://www.eff.org/pub/EFF/Policy/Crypto/ITAR_export/Bernstein_case/.

you decrypt a message sent to you, or sign a message using your private key, you must type in a secret passphrase which is used to encrypt the secret keyring on disk. The private key can only be used if you enter the correct passphrase.

Keeping your passphrase totally confidential is one of the important areas for maintaining a security when using PGP. If your secret keyring file containing your private key is somehow obtained by another person, your passphrase is the only barrier to a total loss of all security offered by PGP. In his book Protect Your Privacy, William Stallings devotes an entire chapter to the importance of setting up a secure passphrase. He advises that you should pick a passphrase that is difficult for others to guess, but not that difficult to remember. This can be more challenging than it seems. One benefit of PGP is that it does not have any length restrictions on passphrases, so you could use an entire sentence as a passphrase. Of course, you will be forced to type this same phrase every time that you want to encrypt, decrypt, or sign messages. Stallings quotes a study of performed by a Unix system administrator, in which a password guessing program was able to determine the passwords of almost 25% of the users of many various systems. Many people chose easily guessable passwords, such as their account name, common surnames, and words found in the system dictionary. He strongly encourages users of PGP to resist the temptation to use passphrases that can be easily guessed.

If your private key and passphrase is discovered by a third party, that person would have the ability to decrypt any PGP messages that were intended for you. They would also be able to forge your digital signature, and claim to be you in email messages. If you learn that your private key has been discovered by someone else, PGP will allow you to generate a key revocation certificate that must to sent to everyone with whom you exchange encrypted messages. This certificate informs other people that you private key has been violated, and to not trust any messages signed with that key.

After you have determined that you have created a secure passphrase for yourself, you can being the process of building a public keyring containing the keys of all the people with whom you will be exchanging messages. First of all, when you download PGP, you will also receive a copy of the public keys of Phil Zimmermann and some of his cohorts. If you examine this keyring with the command pgp -kvv, you will see that many of the keys have been signed by other people.

Signing public keys, your own public key as well as other people keys, is one way to build up an electronic web of trust. Whenever you sign a public key with PGP, the program asks you the following question prior to actually signing the key:

> READ CAREFULLY: Based on your own direct first-hand knowledge, are you absolutely certain that you are prepared to solemnly certify that the above public key actually belongs to the user specified by the above user ID (y/N)?

This question is PGP's way of trying to help you insure that you only sign keys that are valid, and belong to the user that they claim to be from. However, effective key management is one area in

which PGP is lacking. This fault is not a problem with the program itself, but rather with the users of the program. In order to insure that you do not add bogus public keys to your keyring, there are two approaches used to certify public keys.

The "web of trust" method, which I previously mentioned, is a method that allows you to allow certain people that you know and trust to introduce you to other users of PGP. You can configure the various public keys on your keyring to allow certain people whom you trust to act as "introducers." These introducers can vouch for the identity of the person whose public key you have received. PGP can be configured so that you must have more than one introducer vouch for any new person added to your web of trust.

In order to clarify this rather esoteric discussion of key management, I will try to give a description of how a "web of trust" could be implemented. Say that you have started using PGP to exchange messages with two different people, Alice and Bob. You trust both of the them, and have received copies of their public keys. Alice is very carefully about which keys that she signs. She will usually only sign the keys of people that she has met in person, or have been introduced to her by a couple of close friends. Bob, on the other hand, is less careful about which public keys that he signs. He has been known to sign keys of people that he has never met in person, his only contact being a few email messages. Even though you know and trust both Alice and Bob personally, you should only allow Alice to act as an "introducer" to add new people to your public key ring. If you receive a new public key from Charlie with Alice's signature attached to it, and have told PGP that Alice can be trusted as an introducer, Charlie's key will be automatically accepted by PGP as valid. However, if you receive a key from David that has been signed only be Bob, PGP will not trust the validity of this signature, unless there is another, more trusted, signature also attached to it.

In addition to the "web of trust" method of verifying the validity of public keys, some corporations have begun to offer key certification services via the internet. One of the more well known of these key servers is the SLED corporation. In order for individuals to make their public keys easily accessible to anyone in the world, they can, for a small fee, send a copy of their public key to SLED, along with verification of their identity in the form of some official document. The SLED corporation will then add the individual's public key to their database, and also sign the public key, adding an additional measure of validity to the key. The Stable Large Email Database (SLED), in addition to its services as a public key server, also functions as a database of email addresses. The database can be queried either through the use of email messages, or by filling out a form on their World Wide Web page.

The services provided by SLED add to the ease of use of PGP, as well as giving PGP added legitimacy. By utilizing both the decentralized "web of trust" method of spreading public keys, along with the centralized key server functions of SLED, a PGP user can be fairly certain that they have a valid public key for the people with whom they are exchanging documents. For example, if you receive a new public key of someone that you have never met before, via one of your trusted introducers, you can search SLED for the new person's public key. If you find their

key, and the fingerprints on both copies of their key match, then you can rest assured that you have a valid key. Of course, this assumes that the new person has had their public key certified and stored by SLED. This database is not intended to act as the only source of public keys. Only veteran PGP users are likely to pay the twenty dollar registration fee that SLED asks for certification. After paying this one-time fee, your public key can by easily obtained by anyone with internet access simply by sending a message to 'key@four11.com,' or connecting to 'http://www.four11.com/' on the world wide web.

Digital Signatures

Digital signatures are another function of PGP that allows you to be certain that the sender of a message is really who they claim to be. The text of a signed document is sent through a hash function included with PGP, called MD5. The output from MD5 is a fixed sized "fingerprint" of the file. When this "fingerprint" is encrypted with your private key, the result is a digital signature. Usually, the signature is appended to the end of the document sent with PGP. When the digitally signed message is received, the signature can be verified by the receiver by decrypting your signature with your public key, which reveals the original "fingerprint" of the document. The receiver's copy of PGP makes its own "fingerprint" of the document that was received, and compares this to the one that was attached to the document. If these two fingerprints differ in any way, then the message was changed somewhere on the path from sender to receiver. If the fingerprints are identical, then you can be fairly certain that the document was not altered during transmission, and that it came from the person who claimed to send it.

Encryption and Decryption

Encrypting and decrypting documents are the most widely known functions of PGP. Instead of using the rather slow RSA algorithm to encrypt the entire text of documents, PGP performs a three step process to encrypt messages. Once the message has been digitally signed (if this option is chosen), it is first compressed using the freeware ZIP utility that is commonly found on many Unix systems. Then the compressed message is encrypted using a conventional single key encryption algorithm called IDEA, using a one-time session key. Finally, the short session key used by IDEA is encrypted with the public key of the intended recipient(s) of the message using the RSA public key encryption algorithm. This RSA encrypted key is appended to the IDEA encrypted message, and the whole document can then be converted to "ascii armor" format, if so desired. The "ascii armor" prevents any alterations to the message while it is transmitted over the internet. An additional benefit of this process is the fact that PGP encrypted messages are usually smaller in size than plaintext. This is because text messages are highly compressible, and even with the addition of a digital signature and the RSA encrypted session key, the resulting ciphertext is usually smaller than the plaintext hidden within the message.

The ZIP compression algorithm is compatible with PKZIP, one of the most widely used compression programs on the internet. Zimmermann chose the ZIP algorithm because it is fast, and it is freely available for use within other programs. Compressing plaintext before encryption

also adds an additional measure of security. If a brute force attack is made on a PGP encrypted document, even if the attacker somehow discovers the correct RSA and IDEA keys, the plaintext resulting with be compressed, and therefore unintelligible to the human eye.

The IDEA algorithm is similar to the government supported DES encryption algorithm, but is accepted by mathematicians and cryptologists as being a much more secure encryption algorithm. The primary reason for this added security is the longer key size used by IDEA. DES utilizes a 56-bit key for encryption, while IDEA uses a 128-bit key. This additional key size makes IDEA exponentially more difficult to break by a brute force attack, where all possible keys are tried in an attempt to decipher an encrypted message through the use of automated code breaking programs.

Finally, the version of the RSA algorithm that has been utilized by all versions of PGP since 2.6, is free from the patent infringement problems that plagued earlier versions of PGP. The new versions include the RSAREF toolkit algorithm which RSA Data security has allowed to be used without royalties. Because of peculiarities of public key encryption algorithms, much larger key sizes are needed to ensure a secure key. When creating a new public/private key pair with PGP, you are given the option of choosing a key size ranging from 512 to 1024 bits in size. Most knowledgeable PGP users encourage the use of 1024 bit keys, as they are the least susceptible to brute force decryption efforts. PGP will allow the creation of key pairs of any size, but the time required to generate keys increases exponentially as key sizes are increased linearly. With the computing power available today, the likelihood of a brute force attack succeeding on a 1024 bit key is very small.

Advantages and Disadvantages of PGP

In general, PGP has numerous uses for insuring the security of data transmission. First of all, the source code of PGP is very portable, and has been compiled on many different platforms, including PC's, Macintosh, Unix systems, VAX's, and even Amigas. PGP is also able to convert text files between these different systems, so that they can be correctly received with the proper carriage return and line feed combination needed on the particular platform. Secondly, all respected cryptologists acknowledge that PGP provides a pretty good level of protection for encrypted messages and data. Finally, the government has not been involved in the development of PGP. Unlike any government approved encryption algorithm, the source code of PGP is widely available, and has been investigated by many cryptographic authorities. No one has found any "trap doors" in PGP which would reduce the strength of encryption.

PGP also has a number of disadvantages. First of all, it is difficult to learn and use all of the functions provided for security. The format of all PGP commands is identical to the structure of most Unix commands: PGP [-options] [filename] [keyring]. Unless you are a Unix veteran, you will have a difficult time learning all of the commands that PGP have available. Secondly, PGP adds an additional step to the process of sending a message or document to another person. While many programs which integrate encryption are in the planning and development stages,

very few have made it into widespread use. Thirdly, the governmental restrictions on encryption have made the development of encryption programs for worldwide use virtually impossible. Any program which offers reasonable strength encryption is still considered a munition, and is subject to highly restrictive export regulations.

Future Developments

There is hope that some, if not all, of the disadvantages of PGP will be eventually overcome. The arcane command line format for PGP has been improved upon in two of the operating systems under which PGP operates. The Macintosh version of PGP allows users to point and click to choose most of the options available with PGP. Also, a wide variety of Windows front-end programs have been released which offer the same type of interface to Windows users. However, the underlying program is still based on the command line interface of the original program, and some of the more obscure commands can only be utilized by editing command line parameters within a window. Future versions of PGP should allow for development of better graphical interfaces.

The lack of integration with other programs is also being dealt with by today's application developers. There are plans for many email programs to offer encryption as an option. While most of these programs do not plan to use PGP directly, they will likely use the public key encryption method that was popularized by PGP. Two widely known applications have plans to integrate public key encryption in future releases.

The Netscape corporation has announced plans to integrate encryption into its popular World Wide Web browser. This plan is called the Secure Sockets Layer, or SSL. It would operate at the Presentation level of the OSI model, and would therefore be unnoticed by users of Netscape. The only indication of its presence would be a small key, either broken or unbroken, at the bottom left corner of the screen. A broken key indicates that the current link does not support SSL, and is therefore insecure, while a solid key indicates support for Netscape's SSL algorithm.

The second potential application of public key encryption is being debated on the internet today. It is known as Privacy Enhanced Mail, and would integrate encryption into all email messages sent over the internet. As this application is still in the planning stages, no application supports PEM today.

The governmental restrictions on export of cryptography may be the most difficult to overcome. Considering that the government usually takes every possible opportunity to expand its power (e.g. the call for increased FBI powers in the wake of the Oklahoma City bombing), and fights every attempt to reduce its investigative authority, the EFF will have a long fight on its hands in attempting to overturn the governmental restrictions on cryptography. The only solution to this problem will be a fundamental change in the goals of government. I believe that the government should try to protect the rights of the people, rather than the power of federal

institutions.

Annotated Bibliography

Atkins, Derek. "How to Organize a Key-Signing Session," Available on the WWW at http://www.eff.org/

Description of a method to securely exchange public keys.

Barlow, John Perry. "A Plain Text on Crypto Policy," Communications of the ACM, Vol. 36, November 1993, pp. 21-26.

Barlow's informative article describes the government's policies concerning cryptography. Detailed discussion of the Clipper/Skipjack chip, and policies of the Electronic Frontier Foundation concerning cryptography.

Carey, John. "Spy vs. Computer Nerd: The Fight over Data Security," Business Week, October 4, 1993, p. 43.

Discussion of Phil Zimmermann's legal problems stemming from the release of PGP. Government crackdown on encryption, and patent problems with RSA are covered.

Kaliski, Burt. "A Survey of Encryption Standards," IEEE Micro, Vol. 13, pp. 74-81.

Detailed technical discussion of various encryption standards. Coverage of single-key and public-key cryptosystems, digital signatures, key-agreement algorithms, hash functions, and authentication codes. Applications of cryptography are discussed as well.

Levy, Steven. "Crypto Rebels," Wired, May/June 1993, pp. 54-?. (Text of article obtained from http://www.wired.com/)

Description of the history of public key cryptography from its beginnings to the introduction of PGP. Discussion of legal problems encountered by Phil Zimmermann from federal government, and RSA. Also, description of governmental attempts to restrict cryptography, and the cypherpunks who are committed to defending privacy.

McCandlish, Stanton. "EFF Sues to Overturn Cryptography Restrictions," February 21, 1995. Originally posted to alt.bbs.allsysop, alt.censorship, alt.politics.datahighway, alt.privacy, alt.security.pgp, alt.wired, comp.org.cpsr.talk, comp.org.eff.talk, misc.int-property, misc.legal, sci.crypt, talk.politics.crypto. Also available on WWW at http://www.eff.org/.

Announcement of lawsuit sponsored by EFF which attempts to overturn the governmental restrictions on the export controls that have been imposed on cryptographic algorithms and software by the government.

Peterson, Ivars. "Encrypting Controversy: A Fierce Debate erupts over Cryptography and Privacy," Science News, Vol. 143, June 19, 1993, pp. 394-396.

Comparison of public key cryptographic systems: the Clipper chip and RSA's public key algorithm.

Schneier, Bruce. "Digital Signatures," Byte, Vol. 18, November 1993, pp. 309- 312.
Uses and implementation of digital signatures using public key cryptography. Technical discussion of various standards for digital signatures.

SLED Corporation. "PGP Information," Available on WWW at http://www.four11.com/, also linked to http://www.eff.org/.
Detailed description of the database services provided by SLED for PGP users. Also, key certification services provided by SLED, and how to register your public key.

Stallings, William. Protect Your Privacy: A Guide for PGP Users, Prentice Hall, 1995.
This book offers a detailed discussion of the functions and operation of PGP. Detailed descriptions of how PGP works, using PGP on various platforms, underlying algorithms used by PGP, importance of choosing passphrases, and where to get PGP.

Warren, Jim. "Is Phil Zimmermann being persecuted? Why? By whom? Who's next?," MicroTimes, April 1995. Originally posted to comp.org.cpsr.talk by Jim Warren on April 4, 1995, and reposted to alt.security.pgp by Zbigniew Fiedorowicz on April 5, 1995.
Interesting discussion of the history of PGP, and the resulting governmental investigation of Phil Zimmermann.

Figure 1 - Steps to Encryption