



by **Paris2K**: published in New Order Newsletter #9

Table of Contents

- 1.1 Disclaimer
- 1.2 Preface
- 1.3 Introduction to Cryptography
- 1.4 Introduction to the Public Key Crypto-System
- 1.5 Introduction to PGP
- 1.6 PGP weaknesses, bugs and vulnerabilities
- 1.7 Conclusion
- 1.8 After Word

1.1 Disclaimer

I would like to say that in no way does the author of this tutorial encourage any sort of illegal activities. This article may be published on your site, printed, copied, etc. etc. as long as it stays intact and the author is credited.

After I was asked to write a short tutorial on PGP / Encryption and E-mail security for newbies, I did what all writers do in such a case, I started to do some research. Because although I have been working with PGP for quite some years now, one can never know everything. I was going to write about PGP, so the best place to start seemed to be the official PGP manual that comes with the PGP software. But, after reading the first few pages of the official manual I came to the conclusion that the people of Network Associates have done a great job in making the official manual simple and easily understandable for anyone without any sort of knowledge of or experience with, encryption. So why would I write another tutorial about it then? That's what I asked myself. Why do all this work when someone has done it already? Well, first of all, I could just point the official manual out to you guys, and tell you to read it, but then most of you probably wouldn't, and second of all, that would leave the Neworder newsletter (for which this tutorial is originally written) without an article. Then what? Well I could just copy everything that's in the official manual, but that's not like me, and no-one would benefit from that. However, I decided to write the tutorial anyway. The basic introduction to Cryptography might have some resemblances to the PGP official manual, but hey... that's quite normal since both documents are about PGP ;-). In the rest of the tutorial I will try to supply you with some fresh content on how to use PGP's many features.

1.3 Introduction to Cryptography

Ever since we can remember people have wanted to send messages to other people and make sure that third parties could not read these messages. The Official PGP Manual mentions the example of Julius Caesar who did not trust his messengers and therefore thought of a secret language that only he and the right recipients of the message could understand. Many things have changed since the time of Caesar, but what hasn't changed is people's desire to keep their private information private! And that's where cryptography comes in.

First we'll have a look at some basic terms:

>>Plain text is normal, readable text that you see every day. It's the information or message that you want to keep private. (For Example: bla bla everyone can read this)

>>Cipher text is that same message or information, but now in an unreadable state. (For Example: cymn m896cndn d97-d jilkn0- d0-8d87659^)

>>Cryptography is a way of using mathematics to encrypt data so that it is not readable for everyone

>>Encryption is the act of making a private message unreadable/encrypted

>>Decryption is the process of making that unreadable/encrypted message readable again (decrypted)

Cryptography

Now cryptography is, in theory a quite simple method. There are two important parts of a cryptography-system One is the mathematic algorithm and the second is the key (or the password /passphrase). The algorithm is sort of a mathematical formula that changes your plain text into unreadable/encrypted text. Now if anyone could just get this algorithm than anyone could read the text. That's why there's the second part; the key. The key is the part that you yourself make up. And since the algorithm uses the key to encrypt the plain Text, every different key will result in a different encrypted text, even if the original plain text was the same. Are you keeping up? I'll show it in short:

plain text x algorithm + private key1 = encrypted text1

plain text x algorithm + private key2 = encrypted text2

So what we see here is that the same plain text becomes different encrypted texts when different keys are used. So only the person with the right key that was used to encrypt the plaintext, can decrypt the encrypted text back to plaintext.

Weakness

Well. at first this seems like a great way to make sure your data stays private, but we aren't in Caesar's century anymore and there are some smart people out there. (Government, hackers, criminals, etc.) Now what is the weakness of this kind of encryption method?

Well, the right key must be send from encrypter to decrypter. For Example: If you send an encrypted e-mail to your friend, he will have to know what key you used, or else he will never be able to read the e-mail. So you will have to get the right key to him. This is dangerous. Who can you trust?

What way of communications is secure enough to get this key to him? So that's a huge weakness; people could intercept the key. (We all know about sniffers, keyloggers, etc.)

Then what do we do? What method do we use to securely encrypt our data? Well, that's where PGP

comes in.

1.4 Introduction to Public Key Crypto-system

What is this Pretty Good Privacy you keep talking about? Well I'll tell you. PGP is a crypto-system that is based on the Public Key Crypto-system. And that's what makes it more secure than the conventional system. I'll explain:

In 1976 the Public key Cryptography system was invented by a cryptographer and privacy advocate named Whitfield Diffie together with an electrical engineer named Martin Hellman.

In 1977 Ron Rivest, Adi Shamir, and Len Adleman, researchers at MIT discover another more general public key system called RSA. The National Security Agency (NSA) forbids MIT and Rivest, Shamir & Adleman to publish this. They do not listen!

From these early researches into a whole new Cryptography - system, PGP was born. (Read the entire history, which is much more elaborate, at <http://www.cypherspace.org/~adam/timeline/>)

The Public Key Crypto-System

The Public Key Crypto-System would be the solution to the weakness of the conventional Crypto-system. The basic idea behind the Public Key Crypto-system is that you make use of not just one key but a set of keys.

A Public Key (You guessed it!) and a private key. The Public Key is made public to anyone who might want to send you encrypted information and the private key, you keep to yourself. Now everyone can send you information that is encrypted with your public key, but you are the only one who can decrypt this information, since you are the only one with the private key that belongs with your public key. Now if you would like to send encrypted data to someone else, you just go and get their publicly available Public Key and encrypt the data. Then they, and only they whose public key it was, will be able to decrypt the information that you have sent them. It solves the biggest problem that the conventional Crypto-system had, because there is no more need to transport the private key from the encrypter to the decrypter.

In schema:

>>Encryption:

*plain text + Public Key = encrypted text

>>Decryption:

*encrypted text + Private Key = plain text

1.5 Introduction to PGP

Now you know the basic idea behind PGP Encryption. In reality, PGP is a so called hybrid Crypto-System, which means that PGP uses a combination of conventional Cryptography and Public Key Cryptography. However, explaining this would make us go into too much detail, which is not the idea behind this tutorial. If you want to read more about the theory behind PGP and Encryption as a whole, check out Applied Cryptography by Bruce Schneier, the Original PGP Manual or basically any other books, articles or websites you can find about encryption.

PGP Desktop Security

So what can I use PGP for?

Well, PGP Desktop Security is a full package of software with many features. This package includes 1.PGPmail, 2.PGPdisk, 3.PGPfire and 4.PGPvpn.

1. PGPmail

=====

PGPmail makes it possible for you to send and receive message that are encrypted with the PGP Cryptography-system. You can find other people's Public Keys and encrypt/decrypt e-mail messages. PGPmail comes with a plug-in for E-mail programs like Microsoft's Outlook, Outlook Express and for Eudora.

2. PGPdisk

=====

PGPdisk is a utility that allows you to encrypt files on your hard drive. You can either encrypt your entire hard drive or create a partition where you want to store your private / sensitive files. (Encrypted) This part of PGP Desktop Security, I find particularly handy. It's easy to use, quick and makes my data accessible to me only.

3. PGPfire

=====

PGPfire is the firewall that comes with the PGP software. I'm sure you all know what that is.

4. PGPvpn

=====

PGPvpn allows you to create so called "virtual private networks". This is basically a network that transfers all data like a normal network would, only the data is not send in clear text, but encrypted with the PGP Crypto-system. (Let them sniff away!)

There are also programs out there that combine the PGP Crypto - system with popular messenger software, like ICQ, MSN Messenger. AIM, etc.

1.6 PGP Weaknesses, bugs and vulnerabilities.

Of course, like every piece of software, there have been bugs found in PGP, through the years. Below I will list some links to articles about security bugs found in PGP, and other PGP related news, for those of you who have become interested in PGP.

PGP with Outlook Stores Password Pass Phrases in the Clear

>> <http://www.securiteam.com/windowsntfocus/5SP0Y0A6KM.html>

PGP - A phoenix from the flames?

>> <http://www.vnunet.com/News/1129968>

PGP Public Key Server DoS and Remote Code Execution

>> <http://neworder.box.sk/showme.php3?id=6634>

Multiple User PGP ID Attack

>> <http://neworder.box.sk/showme.php3?id=5609>

Network Associates PGP Keyserver Lets Remote Users Execute Arbitrary Code and Gain Privileges on the Server

>> <http://neworder.box.sk/showme.php3?id=5297>

#PGP at Neworder

>> <http://neworder.box.sk/codebox.links.php?&key=pgpenc>

1.7 Conclusion

PGP is a secure crypto-system that can protect your private and sensitive information from a whole lot of people that shouldn't have access to your data. You can use it to securely exchange e-mail and encrypt your hard drive. It's safe and it's easy to use.

There is, however, after writing this tutorial, another thing to be said. Governments have never been very fond of civilians using cryptography.

The American NSA for example, first wanted to keep the Public Key Crypto-System a secret and use it for military purposes only. And US Government has always been lobbying to get access to the keys to crypto-systems; to get a backdoor into the crypto methods, to be able to encrypt any message. In other countries we see the same thing happening.

Government agencies forcing software developers to insert backdoors into their programs and trying to create laws that force people to give up keys.

It is said that PGP had a backdoor like this installed. I don't know. Ask yourself; do I want keep normal people and hackers out and do I not worry about the NSA or the US Government at all. Than you can use PGP and sleep well at night. Especially since the 11th of September tragedy and since we know that Terrorists use the internet to communicate and plan their attacks we have seen Governments of all countries crack down on privacy and encryption. But the right to privacy is a basic human right that all people posses according to international law and national constitutions and although terrorists and other criminals should be hunted down and fought, the civil/human rights of innocent people should not be infringed on. I believe in this strongly and will publish an article on this subject soon.

1.8 Afterword

The article, which started out as a simple explanation of how PGP Encryption works, and what you can do with the PGP Software almost turned into a civil libertarian protest against government infringement on human rights ;-) lol But I hope that the idea behind PGP and Cryptography has become a bit clearer to you guys who didn't know much about it yet.

Extra Note:

This article focussed on windows users. PGP also exist as an open source program for unix/linux systems. Its called GPG. Check out this site if you are interested in this unix/linux version:
<http://www.linuxjournal.com/article.php?sid=4828>

Greetings,

Paris2K
