PGP

Pretty Good Privacy
Downloading, Installing, Setting Up, and Using this Encryption Software

A Tutorial for Beginners to PGP

Prepared by

Bernard John Poole, MSIS

Associate Professor Emeritus, University of Pittsburgh at Johnstown, Johnstown, PA, USA
with
Netiva Caftori, DA, Northeastern Illinois University, Chicago, IL, USA
Pranav Lal, International Management Institute, New Delhi, India
Robert A. Rosenberg, RAR Programming Systems Ltd., Suffern, NY, USA

Table of Contents

Introduction: A word about PGP

You may already know that encryption is the process whereby codes are used to attempt to conceal the meaning of a message. Protecting one's privacy is nothing new. It has, however, become more urgent today because of the ease with which digital data (information in databases, on hard drives or other media, in e-mail, and so forth) can be accessed, intercepted and monitored. It is also not unusual for sensitive information, transmitted or stored in digital form, to accidentally become public knowledge. Once data is in digital form, it's a bit like a greased pig. You can get your hands on it, but you can't hold onto it, because digital data is so easily duplicated and shared. This is why more and more organizations are looking to encrypt all their information.

We all should think seriously about doing the same thing. The fact that you're reading this tutorial suggests that you agree. A little paranoia goes a long way—it makes sense to take whatever means are available, and within reason, to protect yourself from unauthorized people prying into your professional or private affairs.

Where did PGP come from?

PGP (Pretty Good Privacy) is a digital data encryption program created by Phil Zimmermann, a special director of Computer Professionals for Social Responsibility (CPSR) from 1997-2000. He created PGP to promote awareness of the privacy issue in a digital age.

Rarely does anything of significance arise out of the blue. PGP is the culmination of a long history of cryptographic discoveries. Cryptography is the science of writing messages in secret codes. It is nothing new. Ever since the human species evolved, we began pondering the challenge of concealing our communications from others. Secrecy—stealth—is not a preserve of the human species. It is a matter of survival for all our brothers, sisters and cousins in the animal world from which we have evolved. Whether in times of peace or in times of war, we all harbor secret thoughts, feelings, desires, objectives, and so forth that we want to share only with those we absolutely trust, and that we want to carefully conceal from those who would take advantage of us if they knew what we had in mind.

Encryption makes this possible, and one of the strongest encryption tools available to us today is PGP. Phil Zimmermann invented PGP because he recognized that cryptography "is about the right to privacy, freedom of speech, freedom of political association, freedom of the press, freedom from unreasonable search and seizure, freedom to be left alone." Read Zimmermann's fuller explanation as to why you need PGP. Like Isaac Newton, Zimmermann was able to achieve what he achieved because he "stood on the shoulders of giants" who went before.

How does PGP work?

OK, here goes; put your thinking cap on... If this gets overly technical for you, and your eyes start to glaze over, don't worry about it. It's nice if you can understand what's going on with Public and Private Key encryption, but it's not necessary right away. You'll understand it better as you start to use it and as you interact with others who use it and can explain what's going on. For now, it's sufficient to just follow the sets of numbered steps carefully in order to learn the skills required to use PGP. But read over what follows and understand it as best you can.

When you have successfully completed Step 3 of this tutorial, you'll have created **two keys** to lock and unlock the secrets of your encoded information. A **key** is a block or string of alphanumeric text

(letters and numbers and other characters such as !, ?, or %) that is generated by PGP at your request using special encryption algorithms.

The first of the two keys you'll create is your **Public Key**, which you'll share with anyone you wish (the tutorial also will show you how you can put your Public Key on an international server so that even strangers could send you encrypted data if they wanted). Your Public Key is used to **encrypt** a message—put it into secret code so that its meaning is concealed to everyone except you.

Then there is your **Private Key**, which you'll jealously guard by not sharing with anyone. The Private Key is used to **decrypt**—decode—the data (messages and so forth) that have been encrypted using your Public Key. This means that the message encrypted (encoded) using **your** Public Key can only be decrypted (decoded) by **you**, the owner of the corresponding Private Key.

The designation of one of the two keys (Key1, say) as **Public** and the other (Key2) as **Private** is purely arbitrary since there is no functional difference between the two. PGP chooses one to act as the Public Key and designates the other as the Private Key. If it chooses to designate them in the other order (Public=Key2 and Private=Key1), it would make no difference. This is because when either key is used to **encrypt** something, the other will act as the corresponding **decrypting** key to convert the encrypted data back into its original form. This capability is at the heart of the "**Signing**" process mentioned in **Steps 7 through 9 below.**

Public and Private Key encryption solves one of **two major problems with older methods of encryption**, namely that you had to somehow **share the key** with anyone you wanted to be able to read (decrypt) your secret message. The very act of sharing the key meant that some untrustworthy so-and-so could intercept it—and frequently did. Which meant your code was practically useless.

The second major problem with older methods of encryption was the relative ease with which **the code could be broken**. Codes have to be incredibly complex if they're to foil the attempts of astute humans to crack them. This is all the more the case today when we have increasingly powerful computers to do the dirty, "brute force," work of trying every conceivable combination of key possibilities for us. PGP, and other similar encryption systems, use a key that is really—well, astronomically—large, meaning that the number of binary bits (1s and 0s) used to create it has an astronomically large number of possible combinations and the actual decimal (base 10) value they represent is astronomically huge. Unlike earlier encryption methods, the security of PGP encryption lies entirely with the key. Earlier encryption methods relied on "security through obscurity" (ie: keeping secret the method used to do the encryption). The methods used to do PGP encryption are known and documented. It is PGP's selection of the complex keys used to do an encryption that makes it next to impossible to crack.

The size of the key can be increased whenever necessary to stay one step ahead of advances in technology. Time alone will tell if PGP can stand the test of time, but for now it's one of the best encryption technologies you'll find.

If you would like to read the history of encryption and understand the origins of Zimmermann's PGP program, an excellent account is given in Simon Singh's CODE BOOK (Doubleday, New York, NY, 1999). Find out more about PGP at the International PGP home page. You might also like to join the PGP-BASICS User group where you can find speedy and informed answers to questions that might arise as you get started using PGP.

Before you begin

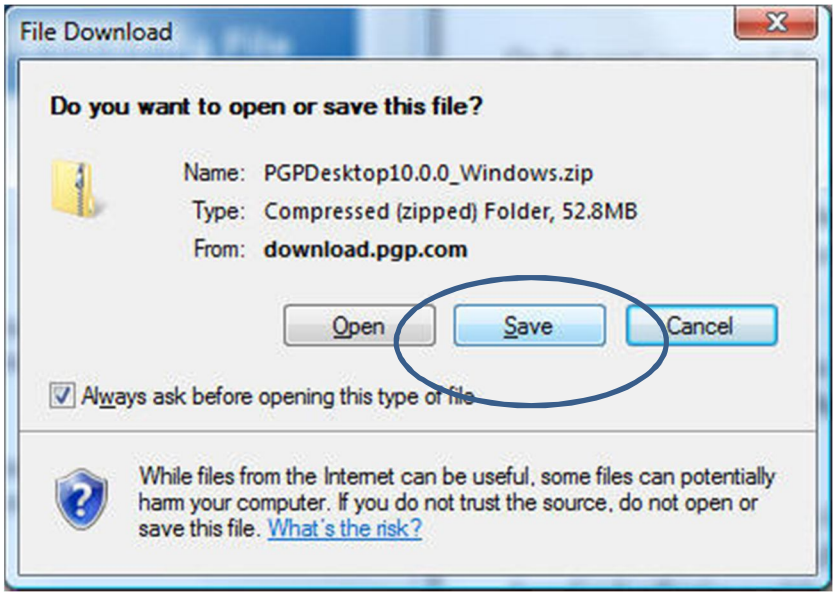
A word of warning to beginners to encryption. The PGP program, notwithstanding its user-friendly graphical user interface, may take some getting used to here and there. At the USENIX Security Symposium in 1999, Alma Whitten & J. Tygar published a paper entitled "Why Johnny Can't encrypt" in which they point out some of the usability problems associated with the software. But, like all these things, with a touch of patience and a small dose of your time, you will soon become proficient in using PGP to protect your privacy.

With this in mind, our tutorial aims to help you get over the initial hurdles at least so you can be up and running using the software without much difficulty. The features of PGP introduced in this tutorial are all you need to know to use the program to protect your privacy in the normal run of affairs. But bear in mind that to become a power user of PGP—one who takes advantage of the full suite of encryption protections—you will need to invest some time in reading the Manual that accompanies the program. The Manuals for each version of PGP can be downloaded from the PGP International web site at http://www.pgpi.org/doc/guide/.

You'll have to reboot (restart) your system after the PGP (Pretty Good Privacy) software has been downloaded and installed, so **save any work** on your computer and **quit any open programs** other than your web browser before you proceed. This tutorial has been designed for users of Windows PCs. Mac users can probably extrapolate from these instructions in order to download the software to iMacs, etc. The tutorial describes the basics of the PGP software in order to help beginners get up and running using encryption.

Step 1: Downloading and Installing PGP Desktop on your computer

- In your browser, go to the International PGP home page and, in the list of Contents on the left side of the screen, select the option to **download**.
- On the next web page, click on the second item in the list (**PGP**), then on the next page click on the item suited to your **Windows OS** (**Windows 2000**, **Windows 3.x**, **Windows 95/98/NT**, **Windows ME**, or **Windows XP**), though the subsequent steps are the same no matter which OS you choose.
- On the next page, click on the item **PGP 8.0**, as this is the latest version of PGP you want to download.
- On the next page, click on **Download PGP 8.0.2 (English)**—unless you want to use the German version.
- On the next page, read the contents of the page, and then, at the bottom, **click in the box** to confirm that "**I have read and agree to the above PGP Software License Agreement**," then click on **Accept**. At various points during this whole download and installation process you will be informed about paying options for the PGP software; ignore these terms and options because you will be using the free subset of the software (unless, of course, you want to pay for the full PGP suite of programs).
- In the next window, you will be prompted to download the **PGP Desktop 10.0 Documentation**, followed by the **PGP Desktop 10.0.0 Windows** products—**go ahead and do this,** selecting the version of the documentation that suits your needs and, for the software download, be sure to click on the **Save button** to save the program on your computer in a place where you will be easily able to find it later for installation purposes (see figure below).



- After you click on the Save button, you will be prompted to tell your browser **where** you want to **save** the **PGP program zip file**. Be sure to select a location on your desktop or hard drive where later you'll be able to easily find the downloaded installation file of the PGP software; then click on the **Save** button. The download will take a while, depending on the speed of your connection to the web.
- Once the download is complete, locate the downloaded zip file **PGPDesktop10.0.0_Windows**, **double click** on it to open it so that you can **extract** the two files you see in the zip file window, and, in the menu bar, click on **Extract all files**. You will again be prompted for where you want to put the extracted files and the default will be to put them in the same place as the zip file, which is fine; so go ahead and click on the **Extract** button.
- You will see a new yellow unzipped folder titled **PGPDesktop10.0.0_Windows**. **Double click** on this folder to open it. You will see two files inside the folder; **double click** on the file named **PGPDesktop10.0.0_Windows_Inner**.
- This will open up the inner zipped file in which are two PGP Application files, one for a **64-bit OS** and the other for a **32-bit OS**. If you don't know which OS you have, click on the **Start button** and, in the pop up menu **right click** on **(My) Computer** and, in the context menu, select the last item: **Properties**. In the info box that pops up you will be able to read whether your OS is 64-bit or 32-bit. Whichever is the case for you, in the menu bar, click on **Extract all files**. You will again be prompted for where you want to put the extracted files and the default will be to put them in the same place as the zip file, which is fine; so again go ahead and click on the **Extract** button. A new window pops up and, in this new window, **double click on the OS version that is appropriate for your system**. This will start the installation process.
- The company, PGP International, lists the following steps to install PGP Desktop on your computer, including the very important license number that you will need to successfully complete the installation. If the license number displayed on your computer is different from the one displayed below, be sure to make a note of it.
  - After installation of PGP Desktop completes, you are prompted to enable PGP for the account.
  - Click **Next** to begin the **PGP Setup Assistant**.

- Enter **Trial User** as the user name and **30 Day Product Trial** as the Organization.
- Do not enter an email address.
- Enter this license number: **DA2K7-TD3VG-729ML-GMU14-HEZT2-CWA**.
- Follow the remaining instructions onscreen to complete installation.

Note: To avoid typing errors and make the authorization easier, **copy** the entire license number, put the cursor in the **first "License Number" field**, and **paste**. The license number will be correctly entered into all six "License Number" fields. You may also copy and paste the user name and organization values in bold above.

The **Installation assistant** will prompt you through the steps—accept the **License agreement** and simply click on the **Next button** as you allow the installation to proceed. At the end of the installation process, you will be prompted to **Restart** your computer; go ahead and do this when you have completed installation of the PGP software.

Step 2: Creating your Public and Private PGP keys

If, during the installation process, you indicated that you are a new user of PGP, you will have been prompted to create a Public and Private Key pair as part of the installation process, in which case you can skip this section and proceed directly to Step 3.

Now that you have the PGP software installed on your computer, you need to create a Public and Private Key pair. This you can do at any time. Remember as you complete the steps that follow that your Public Key is so called because you will willingly share it with others so that they can use it to send you encoded information. Your Private Key is so called because it alone will decode any information that has been encoded with your Public Key. As long as you alone have knowledge of, and access to, your Private Key and the passphrase that goes with it, your privacy will be assured. Here are the steps to follow to create a new Public and Private Key pair:

- **Open PGP Desktop** by selecting **Start/Programs/PGP/PGP Desktop** or by clicking on the **PGP Desktop** icon in the **system tray** at the **lower right corner** of your screen and selecting **Open PGP Desktop** in the pop up menu.
- In the **File menu** select **New PGP Key…** to bring up the **PGP Key Generation Assistant**. Read the introductory dialog, then click on **Next.**
- The PGP Key Generation Assistant now asks you to enter your **name** and **e-mail address**. Do this now. You can use any name you want, and any valid e-mail address so you can take advantage of the PGP feature which will look up the correct key for you that goes with your Passphrase. Click **Next** when you're done entering your name and e-mail address.
- The PGP Key Generation Assistant now asks you to enter a **Passphrase**. Think carefully about this before you proceed. Choose a Passphrase that has **at least eight (8) characters (that is to say it has a minimum of 8 characters as a requirement)**, with a **mix** of upper and lowercase letters and other characters such as numbers. Bear this in mind: the odder the mix of characters and the longer your Passphrase, the better. As Herb Kanner explains, "The size of the Passphrase, and the inclusion of mixed case and non-alphabetics is to increase the difficulty of a brute force attack on your Passphrase." So, if you use a longer, randomized Passphrase (Herb's is 15 characters long, and Bernie's is 33 characters long!!), it would take an intolerably long time for even a powerful computer to try all combinations till it hit on your Passphrase. If you'd like to read more about this important subject of Passphrases, take a look at The Passphrase FAQ. Arnold G. Reinhold's DiceWare Passphrase HomePage is another excellent resource which helps you decide on a good Passphrase.

- Once you've decided on your Passphrase, write it down if necessary so you don't forget it; then, as Steve Kinney recommends, write on the note in large letters the word "**DESTROY**" or "**BURN**" to remind yourself to do this once you've used the new Passphrase often enough to know it by heart.
- **Enter** your **Passphrase** once you've decided what it will be, hit **Tab**, and **re-enter** it for confirmation. Then click **Next** again. The Key Generation Assistant will now go ahead and generate the new Key Pair. Step 3 below explains how to change your Passphrase, so if you change your mind about the Passphrase you just chose, it's not a problem to select a new one.
- If you have entered an **inadequate Passphrase**, the PGP Assistant will **warn** you and ask you to go back and **re-enter** another Passphrase. But if all is well, the PGP Key Generation Assistant will have **generated your key pair**. During the process, you may be prompted to move your mouse around or hit random keys on the keyboard to help the Assistant create a more secure key. Click **Done** when the Assistant has finished **generating your key**.

That's it! You're done creating your **PGP Public and Private Keys**. Now all you have to do is **share your Public Key** with anyone with whom you wish to exchange secure information. Steps 4 through 12 tell you how to do this, and how to use your key and those of your correspondents to encrypt and decrypt the data that you exchange.

Step 3: Changing your Passphrase

After a while, as you become more accustomed to using PGP, you may well want to change your Passphrase, especially if the one you first chose is not complex enough for your liking, or if it has become compromised by someone else discovering what it is. Changing your Passphrase is a simple process. To change your Passphrase, here's all you do:

- **Open PGP Desktop** by selecting **Start**/**Programs**/**PGP**/**PGP Desktop** or by clicking again on the **PGP Desktop** icon in the lower right corner of your screen and selecting **PGP Desktop** in the pop up menu.
- Highlight the **key you want to change the Passphrase for**, then from the **Keys** menu select **Key Properties…**.
- In the dialog box that pops up on the screen, towards the top you'll see the option to **Change Passphrase**. Click on **Change Passphrase**, and in the next dialog box, as you might expect, you're asked to enter your **current Passphrase**. Go ahead and do this, then click on **OK**.
- Now all you have to do is **decide on a new Passphrase**, write it down if necessary so you don't forget it, then in large letters write on the note the word "**DESTROY**" or "**BURN**" to remind yourself to do this once you've used the new Passphrase often enough to know it by heart.
- When you're ready, enter it in the **New Passphrase** dialog box, and **Confirm** the New Passphrase by entering it again, then click on **OK**.

Step 4: Distributing your Public Key

When you want to exchange Public Keys with a particular individual or group of individuals with whom you intend to exchange encrypted information, the best way to do this is to **send it as an e-mail** to whoever you want to have it. Read what follows carefully, however, so you understand how PGP works.

The recipient of your Public Key will have to have PGP installed on their own computer if they want to be able to add your Public Key to their keyring and use it to encrypt the data they want to send you. Likewise, you must have anyone else's Public Key on your keyring in PGP Desktop if you want to send them encrypted data. This is a bit tricky to understand at first, but think about it. Anyone who uses PGP has two keys, a Public Key and a Private Key. Your Public Key is used by other people to encrypt information they want to send you so no one else but you can know what the information contains. When you receive an encrypted message from someone (could be any kind of data, not just text), you use your Private Key to decrypt it. The neat thing is that you're the only person who can decrypt the secret message because you're the only person who has the Private Key, with the Passphrase that unlocks it (unless you share your Passphrase and Private Key with someone else, which would defeat the purpose of PGP!).

If you want to, you can put your Public Key on one or more servers that form an international server chain. Effectively, this makes your Public Key available to anyone anywhere who would like to exchange secure communications with you. Step 5 below explains how to do this.

To include your Public Key in an e-mail message, here's all you do:

- **Open PGP Desktop** by selecting **Start**/**Programs**/**PGP**/**PGP Desktop** or by clicking again on the **PGP Desktop** icon in the lower right corner of your screen and selecting **PGP Desktop** in the pop up menu.
- **Locate your keypair** among the list of keys in the dialog box and **select** it (by clicking **once** on it). Then copy it (**Edit > Copy** or **cntrl-c**)
- Start a **new message** in your e-mail editor, in the **To: box** enter the e-mail address of the recipient, and type a **subject header** such as "**My Public Key**"
- Now click to put the cursor in the **body** of the e-mail, **Paste** your Public Key (**Edit > Paste** or **cntrl-v**) into the body of the e-mail, and **send** it.

Step 5: Making your Public Key available through the Global Directory

It's a good idea eventually to place your Public Key(s) on what's called a public certificate server. This is a server where anyone can access your Public Key and use it to send you encrypted messages. You'll still be the only one who can decrypt the message because you alone have the Private Key, so you never need worry that your privacy will be compromised just because you made your Public Key public. After all, that's why it's called a Public Key. However, as a beginner to PGP, you may not want to do this right away, since you may well decide to change your Public Key at a later date for one reason or another. The thing is that, once you put your Public Key on a certificate server, you can't remove it, and there's no point littering the server with keys that are never going to be used. So keep this section of the tutorial in mind for later, after you've got used to using the program and have settled into using a particular Public Key.

Here, then, are the simple steps to make your Public Key available through the Global Directory. It doesn't matter which server you post your Public Key to, by the way, since they are all interlinked. Wherever you post your Public Key, it will be available worldwide.

- Start by **connect**ing **to the internet**, so that PGP can access the web site where your Public Key can be sent and included in the database (Global Directory) of Public Keys.
- **Open PGP Desktop** by selecting **Start**/**Programs**/**PGP**/**PGP Desktop** or by clicking on the **PGP Desktop** icon in the lower right corner of your screen and selecting **PGP Desktop** in the pop up menu.

- In the **PGP Desktop window**, among the list of keys you see there, click on the **icon representing your Public Key**. This is the key you want to post to the Global Directory.
- Now, in the **Keys** menu select **Publish to Global Directory** and follow the steps in the **PGP Global Directory Assistant**.

PGP will now access the server for you and **post your Public Key there**. When it's done, it'll inform you that the key was posted successfully and tell you that you need to go to your email account in order to respond to an email sent to you from the Global Directory server which will verify your key on the server.

Step 6: Obtaining and Adding someone else's Public Key to your keyring

Once again this is simple enough. There are two ways to do this. You can either have someone send you their key in an e-mail and then paste it into your keyring from their e-mail or, if they have their key already posted to a certificate server, you can go get it yourself. Here is all you do if you get someone's public key in an e-mail:

- First you tell your friend or friends to follow **Step 4** above to **send you their Public Key in an e-mail message**.
- **Open the e-mail message** containing the Public Key you wish to add to your keyring.
- Drag to select from `-----BEGIN PGP PUBLIC KEY BLOCK-----` all the way down to `-----END PUBLIC KEY BLOCK-----`.
- Then copy it (**Edit > Copy** or **cntrl-C**)
- **Open PGP Desktop** by selecting **Start/Programs/PGP/PGP Desktop** or by clicking again on the **PGP Desktop** icon in the lower right corner of your screen and selecting **PGP Desktop** in the pop up menu.
- In the **PGP Desktop window, paste** the Public Key you wish to add to your keyring (**Edit > Paste** or **cntrl-V**).
- Voilà! **Check the keys in your keyring** to verify that the new key has been added to the list.
- For the record, and for practice, the following are the Public Keys of the authors of this tutorial. **Add** these Public Keys to your **keyring** now.

Bernie Poole's Public Key:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.5.8 for non-commercial use
<http://www.pgp.com>
mQGiBDrlpg0RBADQIOANoihULVTQ3sddrU7XObaNMtgFY7fEpybl0fqQStPyqXHY
nMdeHQQA/d9vEviuN5kbLXW2m1Zf67mAajDc8jP/lElYQg8lv8C6XXBkVH/7i7gC
mFteHDbXCsh8Eqwh2okC3frYPpAx1I0z1VtmOGz2jFfxjVBNfuuBPhaRHQCg/0v8
TEi/i/vY7ALLMPcPCAnPgk8EAMKlb/mBTqbahBjCBWx/CLpEQQ/qVDQmlEk/BBKz
ms6t0OQXtqwcf5+kxre2Xf3XDYRYZPL9mS5oSjSLk2vma+5/Z59Xg39tWke7GULs
hle9wA8Bta/ak6t3fxCr/4MyS2BSpYsIfA+6AlPAs2rOF7EX6jOZkfhHvyS1jCBV
4Y0jA/0VoX+TaDNDZotbMT5INGMkIQS9PD8B3/ynjRdRnDpjOIVscEp0A2tyZ853
9w7TkiVoFtBg5XcM5H1j9FZBfhPg/aZGz0ofJlnvhxGiNVUE2Zxr1PwftTFUJUBu
```

7RqnliUsYCL00aFoEDXIJ4T18dB8a/KO9Jh520+RXOUOMe0G4rQkQmVybmllIFBv
b2xlIDxiZXJuaWVwb29sZUB5YWhvby5jb20+iQBOBBARAgAOBQI65aYNBAsDAgEC
GQEACgkQ+JGoqOuWpYh1fQCffB+5AYS1tGBpTBn8ILTGfJNZfkkAmwYgG8PbHJKG
MR2ip6RXYxqk6HfUuQINBDrlpg0QCAD2Qle3CH8IF3KiutapQvMF6PlTETlPtvFu
uUs4INoBp1ajFOmPQFXz0AfGy0OplK33TGSGSfgMg71l6RfUodNQ+PVZX9x2Uk89
PY3bzpnhV5JZzf24rnRPxfx2vIPFRzBhznzJZv8V+bv9kV7HAarTW56NoKVyOtQa
8L9GAFgr5fSI/VhOSdvNILSd5JEHNmszbDgNRR0PfIizHHxbLY7288kjwEPwpVsY
jY67VYy4XTjTNP18F1dDox0YbN4zISy1Kv884bEpQBgRjXyEpwpy1obEAxnIByl6
ypUM2Zafq9AKUJsCRtMIPWakXUGfnHy9iUsiGSa6q6Jew1XpMgs7AAICB/9fLWJk
MxqlKPuP4nfcDXxjYu5yYrtgTxnEA8LjwHILFHC6dS+TruOBehDWWq07PEihRVdK
3vY/oOSV70Du4yO2/siau4xUNhrP2dw1AKgDW1gNvQbeXYuxhs7vKDQGHDgYhUKm
z5E6hX5Z3HesujXnHWe8NtTqa1gM+SP3LF6oFkzTpuIoogRRULy6HUbis1v+Um4i
WI1EXchfauNwy6IzFYOTw41MExKtDyxTLjzBz/PfsncQc2zWpFAih8ZcqQkiOg8B
a+h7xp0hrPzXT0ewxb3aiELI+2oq6m0uwprWJE09REWgwe78gRwbiwlPDH4P/uL9
/tUA2PaCPaEkM7+EiQBGBBgRAgAGBQI65aYNAAoJEPiRqKjrlqWIZv0AoK/IfMGB
Pk7ZKtEr64R8NAArXBoQAJ9E90U+eHZzVN9jG/MVuJKwiNRYZw==
=xI2U
-----END PGP PUBLIC KEY BLOCK-----

Netiva Caftori's Public Key:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.5.8 for non-commercial use
<http://www.pgp.com>
mQGiBDp1yy0RBADVlyDewVwltBs7HnHCG3bXlVUODFkn/00TdbM2SPnOAIkj4giB
ylOP7Mg+Hr5y7FIBvmPWx06In6JjNQiSbpshP5YHv57UfE79nEJdWuSTQt/7j7IJ
GkHYtBRHQMIAHMgT8IB5d3gFq52jSa8hw/ixMP09a0Rw8RP9+kOE4s9UrQCg/zVH
IHswdc/mb50PjdeXwnjxQbkD/3lJYEzz8eUlFHB4rVaC1yRi21Lypf0DIMfQg5j9
xBxY4odFJKyf22PeuAjp9roURRIbGIkIGH8eXF+Mav9OqEdD80JbEn1hZuaLk1RF
k1XJjmFRdKXz+Q7JmRdbs3zXXav2cYwalgzEXT5kuXuNlThLTnLoEFop8Hl3xM4/
PdqMBACkkHb07vPY5l429tdXqL00lE6LedlBW4FLjI534QgselsrUxq5U5y0Wg1Z
//a66l5QkyaMrpsHKfkLHdaPOVCs/WeG6eLwD/cUBEM1Y9Yb5DaB0njdZB3Yxcm8
W23hpKjDanb7SbaSA16gBIWRlvrB/qU+MZAj+EXRDJmwMJq2y7QjbmV0aXZhIGNh
ZnRvcmkgPG5ldGl2YWNAb25lYm94LmNvbT6JAE4EEBECAA4FAjp1yy0ECwMCAQIZ
AQAKCRDFpFclYzXzSwiRAJ0S3djCkJJPUalRyE+vWnfnhvJmDgCfTEBN2N6GlGWO

```
mrOg1tQlZoWbd5q5Ag0EOnXLLRAIAPZCV7cIfwgXcqK61qlC8wXo+VMROU+28W65
Szgg2gGnVqMU6Y9AVfPQB8bLQ6mUrfdMZIZJ+AyDvWXpF9Sh01D49Vlf3HZSTz09
jdvOmeFXklnN/biudE/F/Ha8g8VHMGHOfMlm/xX5u/2RXscBqtNbno2gpXI61Brw
v0YAWCvl9Ij9WE5J280gtJ3kkQc2azNsOA1FHQ98iLMcfFstjvbzySPAQ/ClWxiN
jrtVjLhdONM0/XwXV0OjHRhs3jMhLLUq/zzhsSlAGBGNfISnCnLWhsQDGcgHKXrK
lQzZlp+r0ApQmwJG0wg9ZqRdQZ+cfL2JSyIZJrqrol7DVekyCzsAAgIH+wVFKD3A
FEdEBHqDZuKjLdLJIKHk4gloKeQ60R9NLLFynfIgSvgsii5uWLY9+gZ2FIGnP3Yc
GxZH1HASv+pG1sw0MnhutxZui3E3Mt69Uv1KTlTGYkfS+mXBw4Qr7hXavCkF45we
f/9Qlj6hSKVjy4YcewdvpopM9S4gVcBq+EdTp1negsCyj3YhFiEo0JEL40mnoHX7
HudJBbiBmknmBZOjxzBBeDPcu7fWV/LDCWiFoGg9uWy2KOcIt7sNXVJbukbSGYg2
hzOB2JPaqCqI5+4YfUCumNLd0lktT7S1V3/6xszEnybQL7tMtmrZZFAFHFAwLNPA
bLxdF/b26GbrTT+JAEYEGBECAAYFAjp1yy0ACgkQxaRXJWM180ttbQCg98c40J41
iXkP9CuqGR0LBJ46VNAAnj+5dH9N226fBp5TN0rAyxwBveTK
=0VvA
-----END PGP PUBLIC KEY BLOCK-----
```

Pranav Lal's Public Key:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.5.8 for non-commercial use
<http://www.pgp.com>

mQGiBDr9VmoRBADK8ZX4gTXSsOPo/y+eMv/G55y9tfZfh2tTXsIRVSloRwMN0DBD
36yjWfh3xM0Bfa7z57i5gKdjT95sVokKplbTUcMGNoJQZ4h8TWgvr2Wf2FX0U6Bl
0/cm/9iWHh0jolW2Su6WVLznbknL93Pv6ejxfT/LspKvbnQTBOl3/29CZQCg/xFC
5IVVsNP3Aqe7/fHWps10dmUD/3zq1Bhr6VG+xhZ1yKtRkpMJUX5n/2CSvGpqJrxv
vQUW++9KK5MzApMk9DXbPPyvEP8W6Gl4iOVuXyNoEPBpxu38jF2E9sH+I5llzvl9
Gm+wa0Yz6T5qz0DVrxYTgpVAsBnQsJXOoZEqMPnF4fC/Ba2RfnzpwFCjnGqvZsUc
v+3tA/wLc8yBk6mbBYzb3OKBp2y1RGZcN+52U2hTq18/OKT9CGFCrgHLAFi+Y7iK
5hfErXzUUxRJ/m3LqoUTmtPZy+nst+I/IxpmVKNoeMGXT5VcLyy8KU85Q5zz/AAp
x/QRFPJK8aNfzphBXX3g1NBt1Z/0Kz+JHxXyq16U5nNI4eYEnbQgUHJhbmF2IExh
bCA8cHJhbmF2QHNvZnRob21lLm5ldD6JAFgEEBECABgFAjr9VmoICwMJCAcCAQoC
GQEFGwMAAAACgkQ2E+b6PepG8MJFgCgo8OYI3c8YzfelRdCkPoZzkwCC8gAn27S
Wzb2PjGpeYlJsIYz1t6IixyHuQINBDr9VngQCAD6WhaZlHBHGQN6I0rzIaiEjCz2
IhMAdxipnXV2yn9m6+nrBdA22pMT8ca9dNk66OCSlDTElADuzKQq+CtZrkaMq3I1
AIj5twGGJr7TtIIg03OqZsdAbX0rdcu5HAflqPnc+TIiMij/fyp+NYtRmIIDJd4+
```

ld0gmnTjzBEEFpaA6FdzUJxAyMltJYUMjfwJNNb7ExXzvQswb6CDI9o0gct+gasy
TzqLhv/GMvqzAcOHANF0Mqtxg1kr3qVE4xN7bxvFdYpnpieJR7fc/RoYGQN+zqt1
fFQwRx5o4S8JGDku9AXhThIeyF9j4JJVfVlQgAY/Sh+nrhV2DpiIAaJhnXuPAAIC
CADzBVhZ6B76lEKLjh0A49iNSxGRHQiWt4ZNZ2Ru+DELeqhIa/hCzpwiXZQkJGL3
FuSHkhuoIKbYRpPBx9kgA+TgjmMHZObxAhT0ZCYjhBPSxFCgm080Gp+A5lR6a4gV
V7uKTtsY/6OQVgjo94sdu2nr3FPW2UIuuMsSzthuXRG3mTe+6fypwjPivlFgOZb7
hRvWnRgG03zEGuIirp3C8PtI6iJyd89npLYWZ93Z5Zu+gT00dLyCMoeToCN0VPZy
tLcFbAoMflYvaRTBpVKYCGDXq6GbMg00egHpbpnOKQCG3rGZg2vsmwke7UViB3kj
l3JevhU1XTu7wsH+WeC8tiFEiQBMBBgRAgAMBQI6/VZ4BRsMAAAAAAoJENhPm+j3
qRvDLisAoNb8Dg2RYuMVciB59pAWAd8geaz5AKD1Y6WL0QRQ//dERubgm/Aq17eE
ig==
=A47s
-----END PGP PUBLIC KEY BLOCK-----

Bob Rosenberg's Public Key:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP Personal Privacy 6.5.8
mQGiBDYehAsRBAD9Mmgv7gV3JsMQ0sMLWjk9zX4O07h2XHUow0P5hTIL+lEtcjBn
W6152pufGD0cZjEdVHctH9x/nTOoUdcepTLyIHoLVD+MboepvlizEvqfCQNWEadH
BRE3fzSMqxWTl9nAQyXjqDBi+M92mswMQXUNqhg7cxk50Aymb2rQFoc1PwCg/0mu
fQgQ0UmNTKWfovuGhxKV0/8D/1luI30t5sb4DHFB4mgY9an0r0PtSYdHU3M5jrIx
kbHnWPYtydKNWkhBOncZJOnARAQ6q9SzmdoS9bzVIf0FXAVB3TG7IqgkaxXzkCAw
xkyrcxLjuT0GAbFg3t0kAqzsVnmIgfTCCycg/Xfnn+0Nak0Q06yHtOsPz2g8xhYa
K0MDBACIPH5tpJekxd+fZtF4dHqEotrXPcslPECi3BZELAEsntoAHRS/hYtQUFFZ
7bls3/wdMYX9etlxUbfUXhdxtuxJnpT2S0VoVI4h53cnAAhe8jzCOK5qVBUXSsjX
gYgD03BcXfwM4pMIpxbk+5i+oE5E0w2hIH9sfKFbgLHBaj0ZxLQyUm9iZXJ0IEEu
IFJvc2VuYmVyZyA8Ym9iLnJvc2VuYmVyZ0BkaWdpdHNjb3JwLmNvbT6JAEsEEBEC
AAsFAjYehAsECwMCAQAKCRCnsU6BJsi/YQuOAKC8K2jIl841wmyzLE2EXxE9u1Hw
XACg3X9G1Ad9jNGOkGVOLugXnxE36FS5Aw0ENh6ECxAMAMwdd1ckOErixPDojhNn
l06SE2H22+slDhf99pj3yHx5sHIdOHX79sFzxIMRJitDYMPj6NYK/aEoJguuqa6z
ZQ+iAFMBoHzWq6MSHvoPKs4fdIRPyvMX86RA6dfSd7ZCLQI2wSbLaF6dfJgJCo1+
Le3kXXn11JJPmxiO/CqnS3wy9kJXtwh/CBdyorrWqULzBej5UxE5T7bxbrlLOCDa
AadWoxTpj0BV89AHxstDqZSt90xkhkn4DIO9ZekX1KHTUPj1WV/cdlJPPT2N286Z
4VeSWc39uK50T8X8dryDxUcwYc58yWb/Ffm7/ZFexwGq01uejaClcjrUGvC/RgBY

```
K+X0iP1YTknbzSC0neSRBzZrM2w4DUUdD3yIsxx8Wy2O9vPJI8BD8KVbGI2Ou1WM
uF040zT9fBdXQ6MdGGzeMyEstSr/POGxKUAYEY18hKcKctaGxAMZyAcpesqVDNmW
n6vQClCbAkbTCD1mpF1Bn5x8vYlLIhkmuquiXsNV6UwybwACAgwAyBlC3K4DLlAq
KOf/gzd0YoazkUyx6qte4IF/wTw/wg9wK7mDqab75zAN1DxcsmpJLaPmWAFu2rWd
U1UqeB5+hnpnrYhFkxzL+TnOa9ckI9S33iLjFPCU185FZJNlVlcgclLeog5DSzCV
TjgUeOEMsSUn5d4a7DSkHPfT8TBMlNPQBTuJGGC15H8cCC+2QmWUuLNkq90z6MR+
E5JOajj6z/7qOvfL4SOVPtQxvF5iz2zduapxGgTz4UqeVwA1X7HkXx7Cumdipg0S
Wn63j4IiHHoU4hDyanEkLX32l5PfhaQ8zfpztcy1TxaKXPPtgOGFNDCMo+dG6HfQ
AO2qsL5rDdvgu9hLeCkHaxVDgCKZ4XZ5T9SgL8v3UKep8JomEFt1kdq4KCBJ/gS/
EvXEbnj6Vs63pYtrKgoWxGCCqva8/fqUAfvsX+llGDLBCWLreMTDPisj4fXmJS7h
Cbdg4bSMbVzRUWLNQ/wJbRhR7eeMcP7vrT/q6rx3eL3QCD5cIOCiiQBGBBgRAgAG
BQI2HoQLAAoJEKexToEmyL9hzEIAoL1BDnbaEbsiFPdGsIOz302dNRNCAKCpB9tr
K5MB6twgr+Ww52xyQf6xww==
=BBVS
-----END PGP PUBLIC KEY BLOCK-----
```

If your friend or friends have a Public Key (or Keys) already posted to the Global Directory, you can go get it yourself. Here are the steps to do this:

- **Open PGP Desktop** by selecting **Start**/**Programs**/**PGP**/**PGP Desktop** or by clicking on the **PGP Desktop** icon in the lower right corner of your screen and selecting **PGP Desktop** in the pop up menu.
- In the PGP Tool Bar towards the top of the window, click on **Search for Keys**.
- In the search dialog box, type the **name of the person whose key you are looking for** and hit **OK**. PGP will go to the Global Directory server and find the key or keys for you (many people have more than one Public Key on the certificate server). If a Public for your friend exists on the certificate server, you'll soon see it displayed on your screen.
- Click on the Public Key you want so as to highlight it, and then copy it (**Edit > Copy** or **cntrl-C**).
- Go back to your **PGP Desktop** window where you see all the keys on your keyring. If one of the keys is highlighted by default, click anywhere off the list of keys to make sure no key is currently selected.
- Finally, in the **PGP Desktop** window, **paste** the Public Key you wish to add to your keyring (**Edit > Paste** or **cntrl-V**).

Step 7: Using the PGP encryption software to send (encrypt and sign) and receive (decrypt) secure e-mails

You are ready now to start using the PGP program to generate secure, encrypted digital information. In this section you'll learn how to **encrypt** messages or other data before you send them, and how to **decrypt** messages or other data that you have received.

First, the encryption process.

- **Compose the e-mail** you want to send in whatever natural language you want to use (French, English, Spanish, German, etc.).
- When you have finished composing the e-mail, make sure the cursor is still somewhere in the body of your message, and click on the **PGP Desktop** icon in the lower right corner of your screen.
- In the **PGP Desktop pop-up menu**, select **Current Window**, then in the Current Window sub menu, select **Encrypt & Sign**. This will bring up the **PGP Desktop Key Selection** dialog box where you should see the list of Public Keys including that of the person or persons to whom you wish to send your message. Note: The Private Key is kept in a file called the Private Keyring. It is encrypted with your selected passphrase so even if, somehow, someone gets access to your Private Keyring, it will be unusable without access to the Passphrase to decrypt the Key for use. Every time PGP needs access to the Private Key (to Decrypt an Encrypted Message or to Sign an Outgoing Message or someone's Public Key) the Passphrase will need to be re-entered. By default, PGP will remember [cache] your Passphrase for two Minutes so that you do not have to re-enter it if needed more than once within this time frame. However, two minutes isn't much time and the odds are you'll need to re-enter your passphrase every time unless you change this default. Step 14 explains how to do this, along with warnings about how to use the cache wisely and without risk.
- **Double click** on the Public Key of the person to whom you wish to send your message (this **selects** the key and **moves** it to the **recipients box** just below). When you have made your selection, click on **OK**.
- You will be prompted to enter your **Passphrase**. Type it in carefully, then hit **OK**. If you did everything correctly, the message will be converted to unintelligible gobbledygook (aka "**ciphertext**", as it's called in the world of cryptography). The ciphertext will look like the following:

```
-----BEGIN PGP MESSAGE-----
Version: PGP Personal Security 7.0.3
qANQR1DBwk4DepqGz+tv7awQC/sGOyvgkqLDEz3QOc4AkDuoTVl9O2y7X260NR47
w77OngPn3z/01yEpVDmkfrpdXKYmVhylICPg1yvNYTyx6EW5LIOYt1yuxLc+bjKS
piwrBdCxz5+VT8z9IQz7BNu75GBP5YMJyhZUgwFRDahPITz0ziqL9nBZeUX27PGL
ZIc32bm/18zLwbLUZi4CSPlnc9PzXTeubwnsaC0ZU1PT+WokkhPRxPrgBHLU/rMj
zqOoh2/dXGMUFY7F0zitGw1jcj+jIf49hpzPZ5oWChZQjnQdREZgaRenx3jRomol
BnT0KgGk+cBp8BIM65DyoYdMKE878n+ngTgIYUYkBLnYXfQv9pgagPlQUgmMWSK/
zRkLS3PpKJFTv629iBXKKDeCteqD4668TRty3N1sEXaFbpMZtaNWJvqlXpbbrAkO
rvKAxMq9gpA+asf6415NSX29FT4uv4D7FWF3fp2e9it8c30//9yKXQ8pJb0vfz8B
vZCwIO1me371DScIwI2D8/8EHzQMALxye7O/tpDW3BEU+NEqsHM2nXdebKl7mPk8
5voUyYZb3vz3PQHNJ+Jg14KybK8Jn7KGji19nHFgFtHN0Qoz4e5aTlZtMksWDaX+
dT6xfrKBo5wOaQHGAX3NHBAMTCqUoZajsGxsc+dQ/WB7Qw4qdZjmLtzj35HcF7s0
5RwOWZ2F9cqSj0b994llaT9zo2jXs5ZM/fAZUBPsCp55EFpe52NFKJgyJY92mYi0
1SK26VMNMdHdp4zHWZdNkhPPG0EgDsz1g+EtY6YXWQYwIKPnQUivf5mhDdhPmWK6
```

```
sAR4D7s2Vgqs2gQnvuFxpkDMc5l2rMTAE5+x228SpMPau27BDxBDKLw1i6ak23C+
l2qmiqQg0qeSFy2o7+HmyKWCENl2V84N8eLhoE+iyXj5fL2UvMlqVJePTT76Rz6p
+tD/15JYZo/8uAxIBivaB7P7k2Bqu0bmrCD4wdSKOLzhScxAj15Dtu0kWgEKGs80
VgTMu2iQLtphN7oObhWzUIf9O3MlqMnBCiOp4VFGebnJcDvullUB4OYZD6ZLIecN
8BsqsVlqawJbtWpmRf8973Yg2bicP0ISCwFaoDvR8C+wb3h9nJ9EZeO/mZGjJweR
A6yXK7wyp6JHnvACwFhUkTno7nrdq8cDaG4ssolsUSKnON87ycLFWq/mNs9fhqzF
Y3y7Q4f7hA4EL83+bxc4YGqzirWHeVXetZdft018+0Oz2Au8gRG5AVd+DX+xlr56
mJlkrlzYWG7HuEl8CRS7rAZHgRAIV3I7WDeNEYyBQNt/MfzUQY9+BmbtCsTlOnda
j8IkiL0QIW/9ZyvifxpvzKGKhxdXoqJWVSXLKHGk1qvY9epgw7QWk15crlti0Q4+
aDXvNieN9imk3UNQe2rncqzIKlbxasjparCKXiErQGFjldtTLrZcf7KjNOJuVG9J
HoOZC39ur8rkVrgWuSzrvzhpeQl0VlmdviZpocErZYPtnDQGgA3TbXX4lXoMiM1a
bOxTskUcgIBzN2L9nNfIhVaxJxMd3260SpJxElJ27V6Be97Q+YX4TF9xlH4zWFM3
NpGg1iXWNRb4VSwPE2+ZEiKirrlMsgXxfZNvAy3bAuSm0b1u7Isa/Jjab96DHff6
5g5K
=WRFH
-----END PGP MESSAGE-----
```

Now send the message just as you would normally do.

Next, the decryption process.

- **Open the e-mail** containing the encrypted message. All you'll see is unintelligible ciphertext (as shown in the examples above).
- **Drag to select** the block of **ciphertext**.
- Click once more on the **PGP Desktop** icon in the lower right corner of your screen.
- In the **PGP Desktop pop-up menu**, select **Current Window**, then in the Current Window sub menu, select **Decrypt & Verify**. This will bring up the dialog box asking you to enter your **passphrase**.
- Type your **passphrase** into the **PGP Enter Passphrase** dialog box that pops up on the screen, and hit **OK**. The **decrypted** message will come up in a new window for you to read. If you wish to keep the decrypted version, you can copy it and paste it into a word processor of your choice before saving it to disk. The decrypted message will look like the following (Note that the message is now readable and the signature has been verified):

```
*** PGP Signature Status: good
*** Signer: Robert A. Rosenberg <bob.rosenberg@digitscorp.com>
*** Signed: 06/30/2001 at 00:51
*** Verified: 06/30/2001 at 00:52
*** BEGIN PGP DECRYPTED/VERIFIED MESSAGE ***
```

```
This is a sample of what the above Encrypted&Signed message
looks like after it has been decrypted and the signature has
been successfully verified. Since the Public Key that was used
to encrypt this text belongs to Robert Rosenberg, only he can
decrypt the message to extract this message. An
Encrypted&Signed message is a Clear Signed Message (such as
the sample in Step 10 below) prior to the Encrypt Stage and
after the Decrypt Stage. While it is possible to just Encrypt a
message, it is usual to also sign it to prove its origin.
*** END PGP DECRYPTED/VERIFIED MESSAGE ***
```

That's all there is to it. To find out about the many other features of the PGP program, check out the Manual that was originally downloaded with the software. It's a **.pdf** file which will print out beautifully on your printer so you can read it at your leisure over a nice cup of tea :) Well, maybe you'll need something a bit stiffer to help you figure it all out...

On a technical note: The actual encryption/decryption is NOT being done with the Public/Private keys of your recipient(s) but with a special one-time key that is generated for use in this specific **encrypt&sign** operation. Every time you do an **encrypt&sign**, a new one-time key is generated. Unlike the Public/Private key pairs where anything encrypted with one key needs the other key to do the decrypt, these one-time keys have the ability to decrypt anything that they encrypt (hence its being known as a **Symmetric Key**). When you encrypt any data, this one-time key is used to do the actual encryption. The Public key of each recipient is then used to encrypt the one-time key and added to the encrypted text created with the one-time key. Thus what results is a list of recipients with the one-time key supplied encrypted with each person's Public Key along with the common copy of the one-time key encrypted ciphertext. This format allows a message to be sent to multiple people at the same time yet allow each to use his or her own Private Key to read it. The decrypting process involves the recipient's PGP Program scanning the list of encrypted one-time keys looking for the copy that was encrypted with their Public Key. This copy is then decrypted with the Private key to recover the one-time key which then can be used to do the actual decrypting. The Signing/Verification actions that occur during an **encrypt&sign** and **decrypt&verify** are covered in **Step 10 below** and occur prior to the encryption itself and after the corresponding decrypting of the data.

Step 8: PGP Signing your own unencrypted e-mails

Sometimes you won't want to use encryption when communicating. For example, when contributing to a listserv, posting notes that are shared with a community of folks where you can't be sure every member is using encryption, you won't encrypt your posting. But you can **sign** your posting with your PGP encrypted signature which any other PGP user will be able to verify as a way of ensuring that the note is genuinely sent by you. This notion of providing **added assurance about the source of communication** is part of what is known as the "**Web of Trust**", where people carefully **validate/verify** and **sign** each others' Public Keys so that others can find reassurance that the originator of an e-mail is who he or she appears to be. You can read more about this concept at http://www.rubin.ch/pgp/weboftrust.en.html where Patrick Feisthammel provides a fuller explanation along with an encouragement for all users of PGP to sign each others' keys. The concept of the **Web of Trust** is further explained by Hal Finney at

http://www.sandelman.ottawa.on.ca/spki/html/1996/spring/msg00120.html. For now, here are the simple steps to sign your own unencrypted mail.

1. After you have finished writing your message or e-mail, **right click** on the **PGP Desktop** icon in the lower right corner of your screen, then in the pop up menu choose **Current Window/Sign**. The message is fed into a routine called a HASH Function (a function that converts one string of characters into a fixed length string).
2. You will be prompted to enter your **Passphrase** (unless you have selected the option for PGP to recall your Passphrase from what's called the "cache"—which is not a good idea unless you know what you're doing (see Step 13), so for the time being we'll assume that you will be prompted to enter your Passphrase). In Step 14 you'll learn how to extend the time that your Passphrase is kept in the cache, along with warnings about how you should clear the cache when you leave your computer unattended for any period of time.
3. Go ahead and type your **Passphrase** and hit **OK**.
4. That's all there is to signing your unencrypted e-mails. Unfortunately, signing your unencrypted mail does not, in and of itself, reliably guarantee to the receiver of your note that you are who you say you are, so you should have your Public Key signed by at least one other trusted person who **trusts** you and **can bear witness** to your **integrity** within the context of the **Web of Trust**. Step 11 explains this process of signing someone else's Public Key.

Step 9: Weaving the Web of Trust—Signing someone else's Public Key

Here is a comment from a respected member of the Public Key Encryption community (Nick Andriash) in response to a request he received to sign a cyberfriend's Public Key. "With respect to signing each other's Public Keys," Nick replied, "I have already done so with a **non-exportable** signature, because we have been in constant communication, and I obtained your Public Key from your web site; I am confident enough in knowing the messages are coming from the same person at the same address... I just don't know **who** that person is, and that is why I cannot sign your Public Key with an **exportable** signature, where it will always travel with the Public Key. For that, I insist on **face to face meetings**, along with an **exchange of photo ID**, **etc**., as this is **the only way to maintain the integrity of one's own Web of Trust**. All of **the people who have signed my Key**, I have **met personally**, and that is **as it should always be**, unless we are introduced to each other by a **Trusted Introducer** whose signature appears on both our Public Keys."

When you sign someone else's Public Key, you are verifying that it belongs to the person who claims to own it. You are stating that you know this individual and that the key really belongs to him or her. As it states in the PGP dialog box for signing a key: "By signing the selected user ID(s), you are certifying based on your own direct first-hand knowledge that the key(s) and attached user ID(s) actually belong to the identified user(s)." Then, before signing, you're asked to remember if you received the key in a secure manner (you know where it came from) or if you have verified the fingerprint with the owner. The dialog box includes the owner's fingerprint so you could, if you wanted to, go over the fingerprint with the owner in person ideally, or at the very least over the phone, just to make sure everything's kosher.

In this way, you are able to give a key greater authenticity. Under normal circumstances, you may think it unnecessary to validate someone else's key in this way. You might even think it seems like overkill. But suppose someone were to masquerade as someone else (say, as you) and put a Public

Key in that person's (or your) name on an internationally available certificate server. Then suppose that other people were to encrypt messages using that Public Key, thinking the message could be decrypted and read only by the person they THINK they're sending it to (say, you). All the masquerader has to do now is intercept those messages and easily decrypt them because the masquerader has the Passphrase and corresponding Private Key.

As Nick points out above, there are **two ways** to sign someone else's Public Key. There is a **non-exportable signature**, which is **good for communication between familiar friends** who already know and trust each other informally. Then there is an **exportable signature**, based on **careful, if necessary face-to-face identification and verification**, which is **a much stronger form of reassurance about the integrity of the owner of the Public Key**.

The important rule of thumb is this: **Never, ever sign someone else's Public Key** with an **exportable signature** UNLESS you are able to say categorically that you know who he or she is and have a strong assurance that he or she will not belie your trust. If you follow this rule of thumb, you will be able, over time, to build up **your own personal Web of Trust** while extending the larger, global **Public Key encryption Web of Trust**. The GNU Privacy Handbook has an excellent section on Trust, Validity and the concept behind the Web of Trust.

Here then are the simple steps to sign someone else's Public Key.

First as a **non-exportable signature**:

- **Open PGP Desktop** by selecting **Start/Programs/PGP/PGP Desktop** or by clicking on the **PGP Desktop** icon in the lower right corner of your screen and selecting **PGP Desktop** in the pop up menu.
- In the list of keys in the PGP Desktop window, **right click** on the **key you wish to sign**.
- In the pop up menu, select the item **Sign....** Immediately PGP presents a dialog box which lists the **key you wish to sign**, along with its **fingerprint** (a long string of hexadecimal characters). The text in the dialog box advises you to ensure that the key you are about to sign was given to you in a secure manner, and if you're not absolutely sure, **you should verify the fingerprint with the owner of the Public Key**. At the very least, unless you are quite sure the key belongs to the person who owns it, you should phone the individual and have them repeat to you the characters of the fingerprint by way of validation.
- You'll notice a small check box next to "**Allow signature to be exported**" and you are advised that "**others may rely upon your signature.**" **DON'T check this box** if all you want to do is add a **non-exportable signature** to the Public Key.
- Click on OK to complete the **non-exportable** signing of the Public Key.

Then as an **exportable signature**:

- **Open PGP Desktop** by selecting **Start/Programs/PGP/PGP Desktop** or by clicking on the **PGP Desktop** icon in the lower right corner of your screen and selecting **PGP Desktop** in the pop up menu.
- In the list of keys in the PGP Desktop window, **right click** on the **key you wish to sign**.
- In the pop up menu, select the item **Sign....** Immediately PGP presents a dialog box which lists the **key you wish to sign**, along with its **fingerprint** (a long string of hexadecimal characters). The text in the dialog box advises you to ensure that the key you are about to sign was given to you in a secure manner, and if you're not absolutely sure, **you should verify the fingerprint with the owner of the Public Key**. For an exportable signature, this means literally meeting with the individual face-to-face and verbally and/or visually validating that the Public Key you wish to sign with an exportable signature really and truly

belongs to the person to whom you believe it belongs. This might sound like overkill, but the fact is that **an exportable signature has absolutely no value without this face-to-face guarantee**.

- You'll notice a small check box next to "**Allow signature to be exported**" and you are advised that "**others may rely upon your signature.**" For an exportable signature, **check this box** before you click **OK** to complete to **exportable** signature of the Public Key.

Step 10: Using the PGP encryption software to protect (encrypt) your personal documents

On your computer in the office or at home, you may well have private documents that you do not want others to be able to read. You can use your own Public Key to encrypt these documents. You can easily and quickly encrypt a single file or a set of files. To decrypt the files, you simply reverse the process that follows by selecting the option to Decrypt instead of Encrypt from the PGP menu. Here are the steps to follow to encrypt a single file or document:

- **Right click** on the **Start** menu in the lower left corner of your Windows screen, select the **Explore** option in the pop-up menu, then in the **left hand** column of the Explore window select the **C drive**, for example, and you'll see the contents of your C drive listed in the **right hand side** of the Exploring window.
- **Right click** on any document you have listed there (in the right hand side of the Exploring window) and you'll see a new item (**PGP**) in the pop-up menu.
- Select **PGP** in the pop-up menu and then you'll see the sub-menu option to **Encrypt** the document you've highlighted. Click on **Encrypt**.
- Now you're presented with the **Key Selection dialog box**. **Double click** on your own **Public Key** (or drag it down to the **Recipients** box below) and click on **OK**. PGP has now created a second, encrypted, version of the document with a **.pgp** extension.
- All you need do now is **delete the original**, **non-encrypted document**, so that all you have left on your disk is the encrypted file which only you can read. Do this right away by **right clicking** on the **original** and selecting **Delete** from the pop-up menu.

And here are the steps to follow to encrypt a selected set of files or all the files or documents in a folder:

- **Right click** on the **Start** menu in the lower left corner of your Windows screen, select the **Explore** option in the pop-up menu, then in the **left hand** column of the Explore window select the **C drive**, for example, and you'll see the contents of your C drive listed in the **right hand side** of the Exploring window.
- If necessary, **open the folder** in which you have saved the files you want to encrypt, and either **drag across them all** to select them as a group, or **click to select the first file** in the list, and hold down the **shift** key while you **click on the last of the files** you want to encrypt.
- Now **Right click** on any document you have highlighted in the list of files you selected (in the right hand side of the Exploring window) and you'll see the new item (**PGP**) in the pop-up menu.
- Select **PGP** in the pop-up menu and then you'll see the sub-menu option to **Encrypt** the document(s) you've highlighted. Click on **Encrypt**.
- Now you're presented with the **Key Selection dialog box**. **Double click** on your own **Public Key** (or drag it down to the **Recipients** box below) and click on **OK**. PGP will now go ahead and create a second, encrypted, version of each of the files or documents you selected.

- All you need do now is **delete the original**, **non-encrypted documents**, so that all you have left on your disk are the encrypted files which only you can read. Do this right away. The **original documents** still should be selected as a block, though if they aren't, just click on the **Type** header at the top of the Explore window to sort the files as encypted and non-encrypted. Now, with all the **originals** selected (**highlighted**), **right click** on any one of them, then select **Delete** from the pop-up menu.

You can also encrypt and decrypt the entire contents of a folder by simply right clicking on the folder and selecting Encrypt from the PGP sub menu. But this is not as convenient as opening the folder first and selecting the files as a list before encrypting them since, after PGP has finished the encryption process, you'll have to delete the original files one by one.

Deleting files on your disks raises another issue, which you can learn about in the next section...

Step 11: Using PGP to Wipe files from your disks

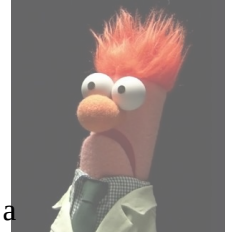
When you delete a file, is the data it contains removed from your disk? Answer: No! You may not be able to see the name of the file anymore if you list the contents of your disk, but someone who knows what they're doing can easily resurrect it and, if it's not encrypted, read it. When you delete a file, all you're doing is removing the link to it from the disk's index of files. It's like a card catalog in a library. Every book in the library has a card in the catalog which helps you find it on the shelves. If you remove the card from the catalog, you'll have a problem finding the book—but it's still out there on the shelves. When you delete a file on your disk, it's like removing the card from the catalog. The file's still there on the disk, even though you can't easily get to it. To remove it completely, you must **Wipe** that part of the disk clean, and this is what the PGP Wipe function does for you. Let's try it for practice.

- Use your word processor to create a dummy file and save it with the name **Dummy**. Put any old garbage in it, since you're going to **Wipe** it off your disk in a minute.
- Now locate the **Dummy** document using the **Explore** option in the **Start** menu (as you did just now in Step 12).
- Right click on the **Dummy** document and select the option in the pop-up menu to **Wipe** the file. Simple as that. PGP writes a bunch of random data to the place on your disk where the Dummy file was saved, effectively removing all trace of the original data. Neat, huh?

Step 12: Useful PGP Options you should know about

We'll be adding explanations for more PGP Options. For now, here is an explanation of how you can tweak the time frame of the cache that PGP uses to remember your Passphrase. You'll also find out here how to Purge your Passphrase cache, a simple task which is very important to remember to do when you leave your computer unattended. Finally, for your convenience, we've added a table listing the hotkeys available in PGP.

As mentioned above in Step 8, every time PGP needs access to the Private Key (to Decrypt an Encrypted Message or Sign an Outgoing Message or someone's Public Key) the corresponding Passphrase will need to be re-entered. By default, PGP will remember—i.e. **cache**—your Passphrase for **two minutes** so that you do not have to re-enter it if needed more than once within this time frame. A cache (which means "hidden" or "hiding place" in French) is a small area on your disk used by the computer to store data it needs to access quickly and frequently. PGP's Passphrase caches are used to save you time by temporarily holding your Passphrases (you may have more than one) after



you've typed them a first time in a session at the computer. Unfortunately, two minutes is too short a time frame for most users, with the result that it's usually necessary to re-enter the Passphrase every time. This is no problem if your Passphrase is short and easy to enter; but a short, simple Passphrase defeats the purpose of PGP which encourages the use of suitably large and complex Passphrases in order to foil attempts at cracking them, as explained above in Step 3 above.

Altering the time that PGP keeps your Passphrase in the cache

This will save you having to repeatedly re-enter your Passphrase every time you need access to the Private Key. Just remember, before you leave your machine unattended, to tell PGP to forget the Passphrase [empty the Cache]. Here are the simple steps to extend the time that PGP keeps your Passphrase in the cache:

- Click on the **PGP Desktop** icon in the lower right corner of your screen and in the PGP Desktop window select **Tools menu > Options...**.
- Make sure the **General** tab is selected in the Options dialog box and notice the Passphrase caching options related to **My Passphrase**.
- The first option: **Save my passphrase for the current Windows session only** speaks for itself.
- The second option: **Save my passphrase for…** You might want to increase the default amount of time you want your Passphrase cached. If you normally are at your computer for an hour or more, you might increase the time to one hour, for example.
- The third option: **Do not save my passphrase**, also speaks for itself.

Acknowledgements

We are grateful to the following folks who have kindly reviewed the tutorial and/or offered suggestions for improving it: Daniel Alvarez, Nick Andriash, Nathaniel Borenstein, Karen Coyle, Jim Davis, Steven Dickenson, John M. Dwyer, Harry Hochheiser, Herb Kanner, Steve Kinney, Pranav Lal, Tom McCune, Peter Meyns, Erik Nilsson, Charles Parlier, Steve Teicher, and Jacques Therrien. If you have further suggestions to help us do a better job, please drop a line to Pranav, Netiva, Bob, or Bernie.