PGP INSTALLATION AND USE FOR DUMMIES

Quick Background

ATTENTION: **This manual was written specifically for PGP Version 5.5.3i, which was the best version available at the time the manual was written. I just checked out the US freeware PGP Version 6.5.1, and it seems to be the best choice to use at this time. This manual is still pretty darned good for 6.5.1, however, some of the instructions are a little off. I don't think you'll have any trouble figuring it out, though. Go ahead and try to install and use 6.5.1, but if you have trouble, you can always uninstall it and download version 5.5.3i, for which this manual was specifically written.**

My time is extremely short right now (8/11/99), and I don't anticipate being able to tailor the manual to 6.5.1 until November at the earliest. You can always e-mail me with questions, and I'll try to help as time permits. Let me know if any links are dead and I will at least update those.

OINK!!

****

PGP (Pretty Good Privacy) is a military grade encryption program that is used to scramble (encrypt) and unscramble (decrypt) data so that it can only be read by those intended to read it. You can encrypt e-mail you send to others and decrypt mail sent to you. You can encrypt and decrypt files on your computer that you don't want others to read. PGP is the best way to protect data that is available to the general public. There is currently a war going on right now between the US government and privacy advocates on the use of powerful encryption. The government claims they cannot break PGP and that it is an impediment to law enforcement agencies. One of the government's propositions is to have easy access to everyone's keys and store them in a large database (typically referred to as key escrow) so that they can decrypt messages when THEY determine there is a reason to. This system is flawed in many ways and we will not go into detail here, but it is important to note that encryption has several legitimate uses such as protecting sensitive data from industrial espionage, conducting financial transactions, talking about intimate issues in a therapy group, securely storing tax information, keeping a diary private, etc.. We encourage everyone to download PGP and even get into the debate. You can find the political information at www.crypto.org.

How It Works

PGP is a public key cryptosystem (although it uses conventional encryption as well). That means that it uses 2 different keys for encrypting and decrypting data. This seems to be the most confusing part that most people have trouble with. Every user will have their own key pair (2 keys). One is called a "secret key", which is used with a secret password to decrypt all your encrypted messages and files. The other is your "public key", and this is given out to the friends and associates you wish to communicate with. They use your public key to ENCRYPT a message to you and you will then use your secret key to DECRYPT it. You also use your own public key to encrypt your own files, then use your secret key to decrypt them. Security is NOT compromised by giving out your public key and that is the beauty of the whole thing. In fact, you must give out your public key to anyone who wants to encrypt a message to you. It does not matter if an adversary gains access to your public key, because all they can do with it is encrypt messages that only you will be able to decrypt. The PGP program is designed so that you cannot accidentally give out your

secret key. PGP automatically brings up your secret key when it needs to so you will never have to worry about it after it is created—there is no need to select a secret key to use for decryption. All you need to do is generate a key pair and give out a copy of your public key to all your contacts. You will also be collecting the public keys of all your contacts as well and they will be stored on your PGP keyring.

Downloading and Installing

There are several versions of PGP to choose from and we won't go into them all here, but in our opinion the best freeware version at the time this page was last updated is 5.5.3i and can be downloaded at www.pgpi.org. The reason we like it is that it has the capability of generating and using both types of public keys (RSA and DH/DSS). The source code has been examined and it has not been shown to have any back doors or other security breaches.

1) To download PGP 5.5.3i go to www.pgpi.org. Select your operating system and click "Show Download Sites".

2) Choose one of the sites and you will then be prompted to save it to a file or open it (depending on your browser type). Choose "Save to File" and begin downloading it into the file of your choice. The file is just over 6.7mb so it might take a while to download.

3) Double click on the file and open it. Follow the steps for installation.

> a) When it asks for registration of name and company, we are privacy freaks so we don't use our real names. You can put whatever you want.
>
> b) It will prompt you to choose a directory. Just stick with the default directory to make it easy.
>
> c) It will ask if you want to install the Eudora/Exchange/Outlook plug ins. If you have any of these e-mail programs then make sure all 3 boxes are selected. If not, then just make sure the PGP program box is selected but it won't hurt if they are all checked.
>
> d) It will ask if you have existing keyrings to use. If you have another version of PGP and you want to use that version's keyrings, then enter the paths here. But since this is the dummies guide to PGP you probably don't so just go with the default and continue.
>
> e) The last option it asks is if you want to run PGP keys and/or view the Read Me file. Uncheck these options because they will just confuse you at this point. Then click finish and you are done.

Configuring and Creating a Key Pair

After the installation is complete, you will notice that you have a small key and envelope icon (which will be referred to as the "PGP icon") in your taskbar (the bar with the START button on the far left and the time of day on the far right—the icon will be to the near left of the clock).

1) Right click on the PGP icon and click "PGP Preferences".

2) In the "General" tab:

a) Uncheck "Cache Decryption Passphrases".

b) Uncheck "Faster key generation". This is optional for added security. Unfortunately, this will greatly increase the amount of time it takes to generate your key pair due to the prime number generation process. You might think the program is not working correctly because nothing happens for a few minutes. Just be patient, because generating prime numbers is a slow process. The program is working fine.

3) In the "Advanced" tab, uncheck "CAST" and "Triple DES" and leave the "IDEA" box checked. IDEA should also appear in the "Preferred Algorithm" box. After that, click "OK".

4) To generate your key pair...right click on the PGP icon once again and click on "Launch PGP Keys".

5) In the box that opens, click on "Keys" and then "New Key" and follow the directions. When you "Launch PGP Keys" for the first time, it MAY automatically begin the keypair generation wizard.

a) You will be asked to enter your name and e-mail address. Care should be taken when you enter this information as it will be attached to your public key and visible to those who have it. If you don't want your e-mail address visible to whoever might obtain a copy of your public key, then do not enter an e-mail address. Presumably anybody you give your key to will know your e-mail address. The e-mail address is NOT needed for PGP to work, but will be convenient for people to reference if they have a hard time remembering e-mail addresses. Those who value their privacy will enter an alias for their name and no e-mail address. However, this can be confusing to people who have your key, as if they don't use it frequently they may forget who "pickle" is if that is not the usual alias you use. The choice is yours.

b) Next you will be prompted to select a key type. Your options are DH/DSS or RSA. There are compatibility considerations. Your version (5.5.3i) can read both keys but other versions may only be able to read one or the other. Choose which ever one you like, as both are considered quite secure. Eventually you may wish to generate both types of keys, because many people have PGP versions which are able to use only RSA or DH/DSS, but not both, so you will need both types of keys on hand to communicate with those people.

c) If you chose RSA then click on the "2048" size. If you chose DH/DSS then click on "Custom" and type in "4096".

d) Next you will be prompted to enter an expiration date. For now, just click "Key pair never expires".

e) Next you will be prompted for a passphrase to enter. A good passphrase should be as equally strong as the message it is trying to protect. Otherwise, the passphrase becomes the weak link in the chain. PGP was made to be military grade encryption. Using a passphrase easier to crack than the encryption simply does not make sense. For a quick way to create a random passphrase, use a dictionary with at least 50,000 words and randomly select 9 words from it. String these words together as your passphrase. Throwing in a few odd symbols such as "!@#$%^&*()_-+={[}]|\:;"'<,>.?/." will help make it even more secure. You can omit the spaces. Once you become more familiar with

the program, check out http://www.stack.nl/~galactus/remailers/passphrase-faq.html for more detailed information on passphrases. IT IS EXTREMELY IMPORTANT THAT YOU REMEMBER YOUR PASSPHRASE. If you forget it, then you will not EVER be able to decrypt your files and messages. If you forget your passphrase, you will need to generate a new keypair with a new passphrase, then distribute your new public key to all the people you communicate with.

f) Once your keys have been generated, you have the option of sending your key to the servers. Until you learn more about this, just leave this box unchecked.

g) Click next or finish and your key will be ready and will appear in your keyring box.

Sending Your Public Key to Others

There are 2 ways to do this:

1) Sending the key as text---this is probably the easiest method for beginners, and will also let you see what your public key looks like.

a) Launch PGP Keys (right click on the PGP icon and click "Launch PGP keys"), then right click on your key, then select "Copy".

b) Use your normal e-mail program, whether it be Netscape, Outlook Express or even Hotmail, and paste the key into the message text box by clicking the right mouse button and selecting "Paste". E-mail it to the person you want to give your key to.

2) Sending the key as an .asc file.

a) Launch PGP Keys, right click on your key, then select "Export". You will be prompted what to call the file and where to save it.

b) Send the file to somebody via an attachment on e-mail, ICQ, etc..

Adding Others' Public Keys to your Keyring

There are 2 ways to add others people's public keys to your keyring.

1) Get the key from a text message (including e-mail text) or bulletin board. This is the most common method.

a) Copy the key to your Windows 95 clipboard. To do this, hold down the left button on your mouse while dragging the cursor over the entire key, including ALL of the leading and ending dashes, until the entire key is highlighted. After everything is highlighted, release the left mouse button, then click the right mouse button, and select "Copy".

b) Right click on your PGP icon.

c) Click on "Add Key from Clipboard". It will show you whose key you are adding.

d) Click "Import".

2) Get the key from an .asc file.

a) Right click on your PGP icon.

b) Click on "Launch PGP keys".

c) Click on "Keys" and then "Import". You then need to show PGP where the key file (extension .asc) of the person is and click "Open". It will ask if that is the key you want to import and you agree.

Encrypting Mail

1) Type your message in a text program, e-mail, or bulletin board.

2) Copy the message to the Windows 95 clipboard. To do this, hold down the left button on your mouse while dragging the cursor over the entire message you want to encrypt until the entire message is highlighted. After everything is highlighted, release the left mouse button, then click the right mouse button, and select "COPY".

3) Right click on your PGP icon and click on "Encrypt Clipboard". There is no need to also "Sign" the message. There is a use for signing messages, but it will only confuse you at this point.

4) You are then prompted to choose the key of the recipient. Simply left click on the key you wish to use to encrypt the message (the recipient's key) and drag it down to the lower box, then release the left mouse button. Then click "OK". (Note: you can encrypt a message to more than one person and/or yourself also). PGP will then encrypt the clipboard.

5) Paste the clipboard into the e-mail, word processor, bulletin board, etc., by clicking your right mouse button and selecting "PASTE".

Decrypting Mail

1) Highlight the ENTIRE message, including ALL the leading and ending dashes, and copy it to your Windows 95 clipboard as described in the "Encrypting Mail" section.

2) Right click on your PGP icon and click on "Decrypt/Verify Clipboard". Enter your passphrase and click "OK". The decrypted message will then appear in a text window. You can read the message, and if you want to save it, then click "Copy to Clipboard" and then paste it into another file, message, etc.. If not, just close the window.

IMPORTANT HELPFUL HINT

Some of the free e-mail services such as Hotmail, Yahoo, etc., create problems when attempting to decrypt messages. If you experience problems decrypting messages with these services, set your Hotmail or Yahoo e-mail preferences so that when you use the REPLY or FORWARD messages option, no characters such as ">" are inserted into the text being replied to or forwarded. When you receive an encrypted message, click on REPLY or FORWARD, and then highlight and copy the text to your clipboard, and decrypt as described above.

Encrypting Files

You can encrypt any kind of file—text files, picture files, etc.—anything. You can even encrypt entire folders using the same method described below.

1) Bring up the icon of the file (or folder) you wish to encrypt.

2) Right click on the file's icon.

3) Select "PGP", then "Encrypt".

4) Select the key you wish to use to encrypt the file—this will usually be your own key—and drag it to the box below, and release it.

5) Click "OK". The file is now encrypted and will be saved in the directory where the original file was.

6) Delete the original unencrypted file. (Before you do this, make sure you are able to decrypt the encrypted file you just created).

Decrypting Files

1) Bring up the icon of the file you wish to decrypt.

2) Right click on the file's icon.

3) Select "PGP", then "Decrypt".

4) Type your passphrase, then select "OK".

5) Save the file.

6) Click on the file to open it.

Encrypting Files to Several Recipients

If you plan to encrypt messages to the same group of friends often you can create a "group" to make the process much easier.

1) Right click on your PGP icon and click "Launch PGP keys".

2) Click on "Groups" and then "New group".

3) Enter the name and description of the group and click "OK"

4) Now click on "Group" again and be sure that "Show groups" is checked and you will be able to see your group under your keys.

5) Drag and drop all the keys of the contacts that you want in the group down to the group name icon.

6) When encrypting to the group next time, simply click on the group name and drag it to the encryption box like you would with any other key and the file encrypted will only be able to be read by that group. (Note: the more participants you have in your group, the longer the messages will get, and the longer it will take to encrypt and decrypt the messages).

That's it. Trust us, we made this as simple as we possibly could. If anybody has any questions or suggestions as to how to improve this manual, please e-mail Pig Vomit. The key to getting proficient is practice. You can practice by encrypting text messages to yourself and then decrypting them. Give it a try, and you'll figure it out pretty quick. If you get stuck, there is a Help manual in the program.

Good luck!