Using PGP for Windows 95 or Windows NT

PGP Basics

The first half of this document will introduce you to the basics of using PGP for secure correspondence:

I. Finding someone's public key on the Caltech PGP key server and adding it to your keyring,

II. Sending an encrypted, signed message to someone,

III. Decrypting an encrypted message and verifying its signature.

Getting Started:

Change your passphrase
When PGP is installed, an initial public and private key pair are generated for you, with an assigned passphrase. It is advisable to change this initial passphrase to one that will be easy for you to remember. See page 15 for instructions on changing your passphrase.

Send your public key to the Security Manager
Before using your new PGP key pair for official Caltech correspondence, you must send a signed, encrypted message to the Security Manager, at csmk@caltech.edu. The Security Manager will then make your public key searchable on the Caltech PGP Public Key server. This helps to ensure that no one will start sending you encrypted messages before you've learned to use PGP. For instructions on sending your public key to someone, see page 11.

I. Finding someone's public key on a key server

To exchange encrypted messages or files with other PGP users, you will need to have your correspondents' PGP public key(s) in your keyring file. If the key owner is a member of the Caltech community and has instructed the Security Manager to list the key, you can look up that key on the Caltech public key server. You can also look for a key on one of the public key servers on the Internet, have the key sent to you via email, or obtain it in text form by cutting and pasting it from an already-received document. (Instructions for this last method appear on page 12, "Obtaining public keys from a file or from the text of an email message.") The following example shows how to find the public key component of the Security Manager's Caltech Security Master Key on the Caltech key server.

To look up a user's key on the Caltech key server or another public key server:

1. Launch PGPKeys.
2. From the **SERVER** menu, choose **SEARCH...** or select the  button from the PGPKeys button bar. The PGPKeys Search Window opens, and the Caltech key server, **pgp-server.caltech.edu**, is listed as the default choice in **SEARCH FOR KEYS ON**. To search another key server, select it here from the pull-down menu. (To add a key server to the search menu, see the section on "Recommended Settings" on page 13.)
3. Enter the search criteria to use in locating the user's public key. To narrow your search, click **MORE CHOICES** and specify additional criteria. Find the Caltech Security Master Key by typing in "security" in the search field labeled **USERID** and **CONTAINS**, and then click the **SEARCH** button.
4. Once you have found the public key you want, add it to your keyring by dragging it from the search window and dropping it in the main PGPkeys window.

Updating a key in your keyring:

Because people occasionally make changes to their public keys that require the key to be updated, it is advisable to update your keyring periodically. PGP is set to automatically update the keys in your keyring by searching the key server on a monthly basis. This process can take several minutes depending on the size of your keyring, and a notifier dialog box will appear during the update to allow you to cancel if necessary. If you're unsure whether your keyring copy of a specific key is still current, update the key from the server:

1. Launch PGPKeys, by clicking on the PGPTray icon  in the lower right corner of your screen and selecting **LAUNCH PGPKEYS**. Your keyring will open.
2. Highlight the key to be updated.
3. Click **SERVER** and then **UPDATE**, or click on the  button on the toolbar. A notifier box will pop up showing the key server search and allowing you to cancel.
4. Import the search result by clicking the **IMPORT** button on the search result dialog box.

II. Encrypting and Signing

Attaching vs. encrypting or signing within the text of a message
Encrypted messages can be sent in one of two ways: as the text of a message (which appears as gibberish after encoding) or as an encrypted attachment to a message that itself may or may not be encrypted and/or signed. The decision to use one method or the other is mainly a matter of convenience, depending on the purpose of the encrypted text. Very long text, or a document that needs editing or contains special formatting, might be best sent as an encrypted attachment. For instructions on encrypting files separately or as attachments, see "Signing or Encrypting a Document" on page 4.

Signing or encrypting the text of an email message
Signing provides an electronic validation that the message has not been altered or tampered with after it was sent by its originator. ITS recommends digitally signing any file that is considered confidential enough to encrypt. A document or message can also be signed but left in unencrypted "clear text" form if the contents are not confidential.

NOTE: although PGP adds buttons to the toolbar of Eudora 4.x, ITS recommends against using these buttons for encrypting or signing email messages, due to a slight incompatibility between the two programs. Outgoing messages encrypted and signed using the PGP buttons in Eudora 4.x are not stored properly in the Eudora Outbox. The method given below for encrypting and signing email results in a correct Outbox copy of the message.

To sign, or encrypt and sign, the text of an email message:

1. Start a new message in Eudora and address it as usual.

2. Type in your message.

3. Hit **<ctrl a>** or choose **SELECT ALL** from the **EDIT** menu in Eudora. Next, right-click anywhere in the message window. From the resulting menu, choose **MESSAGE PLUGINS**, then either **PGP SIGN** or **PGP ENCRYPT & SIGN**. Note that if the email address in your message corresponds to a key in your keyring, PGP will *automatically* encrypt the message and prompt you for your passphrase to sign the message. Otherwise, your PGP keyring window will open with keys listed by their associated email addresses, and allow you to select, by drag & drop, the key you wish to encrypt to. After you select the key, PGP will prompt for your passphrase to sign the message.

4. Click the **<send>** button to send the message. An encrypted copy of the message will be retained in Eudora's Outbox, if Eudora is configured to keep copies of outgoing messages.

Encrypting for more than one user
When encrypting, simply select multiple recipient public keys. You may select as many as you wish. The resulting document will be decryptable by each of the recipients. If your email message is addressed to multiple recipients, each of whom appears in your keyring, the message will automatically be encrypted to each recipient.

Signing or encrypting a document
PGP creates a new copy of the target file in the original directory, leaving the original file intact. If you wish to remove the original, unencrypted copy of the file for security reasons, do so as a separate step.

To sign a document (with or without encrypting it):

1. Locate the document under My Computer or in the Windows Explorer file display. Right-click the file and choose **PGP** from the resulting menu. Select **SIGN**, or **ENCRYPT AND SIGN**.

2. To sign the document without encrypting, skip to step 4. If you have chosen to encrypt the file, PGP now opens the keyring window. Select the key(s) you wish to encrypt to.

3. Select key(s) by clicking and dragging them from the keyring in the upper portion of the window to the **RECIPIENTS** list in the bottom portion of the window. Then click **OK**. *Caution: WIPE **IRRETRIEVABLY DESTROYS THE ORIGINAL, UNENCRYPTED COPY OF THE FILE.** Therefore, to guard against possible mishap, ITS recommends **against selecting WIPE** here. More information about WIPE is on page 13.*

4. PGP prompts for your passphrase to sign the encrypted document. If you have more than one key pair, select the appropriate key pair from the pull-down window. (See page 8, "Creating additional key pairs" for more information.) After typing your passphrase, click **OK**.

Signing and Encrypting a document from within Eudora
PGP for Windows allows you to sign or encrypt attachments directly from Eudora:

1. Create your email message in Eudora.

2. Click the attachment button from inside your message.

3. Locate the file to be attached, and then right-click on the file. Choose **PGP** and then **SIGN** or **ENCRYPT AND SIGN** from the resulting menu. Select the recipient(s) and/or type in your passphrase as usual. A new signed or encrypted version of the file will be created in the original file's directory. Attach this new file to your message by double-clicking to select it.

4. Click the **SEND** button to send the message with its signed or encrypted attachment.

Decrypting and Verifying

Decrypting and/or verifying the text of an email message
The same method is used for both decrypting an encrypted message and verifying a digital signature. Note that if the message includes an encrypted attachment, you must decrypt the attachment first, using the instructions on the next page.

To decrypt an email message in Eudora or verify its signature:

1. Open the message in your Eudora mailbox.
2. Click on the PGP Decrypt/Verify button  . If the message was signed, PGP automatically verifies the signature and displays a short paragraph indicating whether the signature appears valid and corresponds to a public key in your keyring. If the signature does not correspond to a key in your keyring, PGP will declare the signer to be "unknown". If the message was encrypted, PGP also prompts you for your passphrase and decrypts the message.
3. When you close the message or attempt to reply to it, Eudora will ask whether to save changes. Answering "no" to this question will retain the message in its encrypted form only. Answering "yes" will save the message in its decrypted, readable form.

Decrypting selected text
To decrypt just selected text, either in an email message or from some other source:

1. Highlight the text you wish to decrypt, starting with the line **-----BEGIN PGP MESSAGE-----** and including the line **-----END PGP MESSAGE-----** at the end of the encrypted text.
2. If you're decrypting part of an email message, right-click on the highlighted text. Choose **MESSAGE PLUGINS** from the resulting menu, then **PGP DECRYPT & VERIFY**. Otherwise, go to step 4 below.
3. If you're decrypting non-email text, type **<ctrl c>** to copy the selected text to the clipboard, then click on the PGPTray icon  in the lower right corner of your screen, and **DECRYPT & VERIFY CLIPBOARD**.
4. Type in your passphrase at the prompt.

Decrypting and/or verifying a document emailed as an encrypted attachment
Messages with encrypted attachments can appear in one of two forms, depending on what method the sender used. Messages encrypted using the PGP plug-in buttons for some email programs will result in a single encrypted file with the subject of the message as its name, and a **.ems** filename extension. The **.ems** file contains the message text, if any, as well as the attachment. Messages in which the file attachment was encrypted separately, and whose text may or may not be encrypted, will display as regular email messages containing text (either encrypted or not) and displaying an icon for the attached file at the bottom of the message. The attached file's name will be its original filename with **.pgp** or **.asc** (text-output encryption) as the filename extension.

In either case, single-clicking the icon of the attached file will decrypt it. The result will be slightly different depending on which type of encrypted attachment is decrypted, as discussed below.

To decrypt and verify an attachment with a **.ems** filename extension  :

1. Single-click on the **.ems** file's icon in the email message.

2. Enter your passphrase at the resulting prompt (note that if the document was signed but not encrypted, you will not be prompted for a passphrase.)

3. The file decrypts and the text of the message (if any), a block of text indicating the validity of the digital signature, and an icon for the file attachment display.

4. Open the attached file by double-clicking its icon from within Eudora, or locate the file in Eudora's attachments folder and move, or double-click, it from there.

To decrypt and/or verify an attachment with a **.pgp**  or **.asc**  filename extension:

1. Single-click on the **.pgp** or **.asc** file icon that appears in the email message. Do this BEFORE decrypting any accompanying encrypted message text.

2. Enter your passphrase at the resulting prompt (note that if the document was signed but not encrypted, you will not be prompted for a passphrase.)

3. A PGPLog window will open displaying the validity of the digital signature.

4. A decrypted version of the attached file will appear in the Eudora attachment folder, with the same name minus the **.pgp** or **.asc** filename extension.

Decrypting and/or verifying a file outside of email

Note that this method will also work for **.pgp**  and **.asc**  files sent as email attachments.

To decrypt an encrypted file:

1. Right-click on the icon of the file to be decrypted and/or verified.

2. Choose **PGP** and then **DECRYPT & VERIFY** from the resulting menu. Type in your passphrase at the prompt (note that if the document was signed but not encrypted, you will not be prompted for a passphrase).

3. The decrypted version of the file will appear as a second file in the same folder as the encrypted version, with the same name minus the **.pgp** or **.asc** filename extension.

Using PGP: Additional Information

Adding a user name or email address to a key pair

The user name and email address associated with a key pair are used when looking up a public key on the key server. They also display when someone encrypts a document for you, or verifies a document you signed with your key. It is important that they be correct. If you have more than one email address and would like them all associated with your same key pair, or if your key is for official use only and you want users to be able to search for you by your department name or title, you will need to associate additional user names or email addresses with your key pair. Existing names and email addresses associated with a key pair cannot be changed or deleted.

To add a user name or email address to a key pair:

1. Launch PGPKeys.

2. Click to select the key pair for which you wish to add a user name or address.

3. From the menu bar, select **KEYS**, then **ADD**, and then **NAME**. Enter the new name and email address to be associated with the key pair.

4. At the prompt, enter your passphrase.

5. Note that whenever a new name and/or email address is added, **you must send the updated key to the Caltech Security Manager** and to any correspondents who do not have access to the Caltech server. See page 11, "Distributing your public key" for instructions.

Creating additional key pairs

Some users may want additional key pairs, either to maintain encrypted or signed correspondence for more than one department, or to have separate key pairs for personal correspondence and official departmental correspondence. To create an additional key pair in PGP 6.x for Windows 95/NT:

1. Launch PGP Keys.
2. From the Keys menu item, choose **NEW…** (or click the "shiny key"  button on the PGPKeys button bar). Click **NEXT** from the initial key-generation screen.
3. Type in your full name as it should appear in association with your key – this is the name that will appear when documents you encrypt or sign are decrypted or verified. It is also the name that will appear in any public key servers that list your key. Type in the email address that should be associated with this key. Click **NEXT**.
4. Select a size for this key pair. Bigger key sizes are safer from certain kinds of computer attacks, but require more time for encryption/decryption; ITS recommends a 2048-bit PGP key pair in PGP. Click **NEXT** to accept this recommendation and continue.
5. Choose whether the key should expire. Expired keys can still decrypt and verify, but can no longer sign or encrypt documents. If this key is intended for short-term use only, an expiration date may be appropriate. ITS currently recommends selecting **NEVER**. Click **NEXT** to accept this and continue.
6. The next three screens are informational screens about your new key's properties. The first screen indicates that your key has an Additional Decryption Key associated with it, the Caltech Security Master Key. This means that whenever you encrypt something for someone else, or someone encrypts something for you, the Caltech Security Master Key will also have the ability to decrypt that file. The second screen indicates that the Caltech Security Master Key is a trusted "corporate signer," meaning that any key signed by the CSMK will be considered by PGP to be "valid" and "trusted." The third screen indicates that the Caltech Security Master Key is a Designated Revoker for your key (see page 10, "Revoking your key" for more information). Click **NEXT** to continue past each screen.
7. Enter a passphrase for this new key pair. This passphrase will be required for signing and encrypting/decrypting documents. You will be typing it often. Pick a passphrase you will remember, and *do not write it down.* As long as your passphrase remains secure, you can use the same passphrase for multiple key pairs, each of which will still be unique. Click **NEXT** to continue.
8. PGP may ask you to move the mouse around in order to help generate a random number. You will be notified when the new key pair has been generated. Click **NEXT** to continue, and **NEXT** again to avoid attempting to automatically submit the key pair to a server (Caltech's key server is maintained directly by the Security Manager). Click **FINISH**.
9. Your new key will display in your PGPKeys keyring window, with the "key-with-face" icon  to indicate that it is a key pair.
10. If this is an official key, to be listed on the Caltech PGP key server, **your new public key must be sent to the Caltech Security Manager**. Distribute the key to any correspondents who do not have access to the Caltech public key server. See page 11, "Distributing your public key," for more information on sending your public key to others.

Specifying a default key pair
If you have more than one key pair, specify a default signing key:

1. Launch PGPKeys.

2. Highlight the key pair you wish to set as the default.

3. From the **KEYS** menu, choose **SET DEFAULT**. The default key will appear in your keyring in bold.

Sign-only keys
In some situations, it is useful to have a key pair that is used only to sign documents. PGP allows a key pair to be set as a "sign-only" key. Such a key can neither encrypt nor decrypt any messages. **This choice is not reversible**. You cannot restore encryption capability to a sign-only key.

To set a key pair to allow it to sign, but not encrypt, documents or email:

1. Launch PGPKeys.

2. Highlight the key pair you wish to change; click the green "question mark"  on the PGPKeys button bar, or select **KEYS** from the menu bar and then **PROPERTIES**.

3. Click on the **SUBKEYS** tab. There usually will be only one subkey listed here, with **VALID FROM**, **EXPIRES**, and **SIZE** entries. This is the component of your key that allows encryption.

4. Highlight the displayed subkey and click **REMOVE**. You will be warned that if the encryption subkey is removed, this key will automatically become a sign-only key. Click **YES** for **ARE YOU SURE YOU WANT TO DO THIS?** Key pairs that have had all encryption subkeys removed are automatically sign-only keys.

The final step to making a sign-only key, or to making any other changes to a key aside from changing its passphrase, is to send the public key portion of the newly-modified key pair to the Security Manager so that the Caltech key server can be updated. See page 11, "Distributing your public key," for more information on sending your public key to the Security Manager or to others.

Deleting a key
Occasionally you may want to delete a public key or a public/private key pair from your keyring, perhaps because it is outdated or no longer used. If you delete a key pair, any files already encrypted to that key will no longer be decryptable. As a precaution, PGP asks "**ARE YOU SURE YOU WANT TO DELETE YOUR PUBLIC/PRIVATE KEY PAIR**?" before deleting a key pair from your keyring.

To delete a public key from your keyring, simply highlight the key and hit the "delete" button on your computer.

Before deleting a key pair, revoke it from any key servers that list it, so that no new correspondent will use it. Use the instructions below.

Revoking your key
To revoke or disable a key pair, you must first generate a revoked copy of your public key, and send this to the Caltech Security Manager and to any non-Caltech public key servers that list your key. If you no longer have access to the public and private components and the passphrase of the key pair to be revoked, you will not be able to generate a revoked copy of your public key yourself.

Because the **private key and passphrase are required** in order to revoke a key, PGP allows a key to be assigned an additional revoker. The Caltech Security Master Key is automatically a designated revoker of all official Caltech keys. If you are unable to generate a revoked copy of your key, call the Security Manager from your own telephone extension, or visit him in person to have the key revoked and a new key pair created for you.

To revoke a key pair yourself, assuming you have a working copy of the key pair and your passphrase:

1. Launch PGPkeys.

2. Select the key pair you want to revoke.

3. From the **KEYS** menu, choose **REVOKE**, or click the "red X" button  on the PGPKeys button bar. The Revocation Confirmation dialog box appears.

4. Click **OK** to confirm your intent to revoke the selected key.

5. Enter your passphrase, then click **OK**. Once the key has been revoked, it will appear in your keyring with a red X to indicate that it is no longer valid.

6. **Send a new copy of your revoked key to the Security Manager.** Use the instructions for sending a copy of your public key given below in "Distributing your public key." If your key is listed on non-Caltech key servers, send a copy of your revoked key to the appropriate key servers as well.

Distributing your public key
Email is the simplest way to give someone a copy of your key. Instructions are given below. See "Exporting a copy of your public key into a file," in the section after this one, for instructions on copying your public key to a text file, which you can then cut and paste into your UNIX account .plan, upload to a non-Caltech public key server, or save to a floppy that you send to your correspondent.

Sending out a copy of your public key in an email message

1. Create and address your email message in Eudora as usual.

2. Launch PGPKeys.

3. Click and drag your key from the keyring window into the Eudora message window. Drop the key anywhere within the body of your message. A lengthy chunk of garbled text will appear, prefaced with **-----BEGIN PGP PUBLIC KEY BLOCK-----** and ending with **-----END PGP PUBLIC KEY BLOCK-----**. Your message, if any, must be typed outside the BEGIN and END markers of the PGP Public Key Block. If you want to sign or encrypt the message that contains your key, do so as usual in accordance with the instructions on page 3 of this document, "Signing or encrypting the text of an email message."

4. Click **SEND** to send your message.

Exporting a copy of your public key into a file
If you want to create a file containing your public key, you must **export** a copy of your key from your keyring:

1. Launch PGPKeys.
2. Highlight your key, and click on the "floppy disk"  button on the PGPKeys button bar, or select **KEYS** from the menu bar, and then **EXPORT…**.

3. Give the export file a name and location. ITS recommends leaving the option **USE 6.0 EXTENSIONS** *unselected* in case your correspondent does not use version 6.0 of PGP. SECURITY NOTE: You must leave **INCLUDE PRIVATE KEY** *unselected*, or you will export your private and public keys as a working pair that can be used on another computer.

4. Click **SAVE**.

Obtaining public keys from a file or from the text of an email message
To acquire the public key of someone not listed on an available key server, either cut and paste their key from an email message or other text containing the key, or import it from a file.

To import a key into your keyring from text that you can cut and paste:

1. Copy any text containing the public key onto your Windows clipboard: Highlight the text (or type **<ctrl a>** to select the entire text), then type **<ctrl c>** to copy the text. PGP ignores extraneous text, and looks for that portion of the text that contains the public key(s).

2. Launch PGPKeys.

3. Click anywhere in the PGPKeys window and type **<ctrl v>** to paste the contents of the clipboard into the keyring. The key or keys will be automatically imported into your keyring. If there is extraneous text in addition to the key itself, PGP may open a window listing the key or keys found and verifying that this is what you wish to import. Click the **IMPORT** button to complete this step.

To import one or more keys into your keyring from a file that is emailed as an attachment or provided on floppy disk:

1. Launch PGPKeys.

2. Click and drag the file containing the key(s) and drop it on your keyring. PGP will automatically ask for your passphrase to decrypt the file if it was encrypted, and then ask if you want to import the key(s) into your keyring.

3. Click the **IMPORT** button to import the key(s).

Signing a non-Caltech key to make it valid
Note that if you import a non-Caltech public key, it will not automatically be listed as "trusted" or "valid" in your keyring because it will not have been signed by the Caltech Security Master Key. Such keys are still usable, but when you encrypt to them, PGP will give an error message saying "Some recipient keys are not valid. Please verify that these recipients are correct." and requiring you to manually select the invalid keys from your keyring.

To avoid this error message, make the non-Caltech key valid by signing it:

1. Launch PGPkeys.
2. Highlight the key to be signed and click on the "pencil" button  from the menu bar, or select **KEYS** and **SIGN…**. A box will pop up reminding you to be certain that this key really belongs to the person whose name is on it. Click **OK**.

3. Type in your passphrase to sign the key. The "validity" bullet next to the key in your keyring will turn green to indicate that this key is now valid.

The WIPE command
This PGP security feature allows you to delete a file by overwriting it so that it cannot be retrieved even using a file-retrieval utility such as Norton Utilities. WIPE should be considered permanent, complete, and irreversible. Therefore, ITS strongly recommends using this powerful feature with care. We do not recommend selecting **WIPE** as part of the process of encrypting a file, on the small chance that something goes wrong during the encryption and you are unable to retrieve your original file. Instead, to irretrievably destroy the unencrypted original of a file, first encrypt it and make sure that the file has encrypted properly and is decryptable. Next:

1. Right-click on the file to be removed.

2. Select **PGP**, then **WIPE** from the pull-down menu. Click **YES** at the prompt "are you really sure you want to secure delete these files?" The file will be irretrievably deleted.

Recommended settings
PGP is preconfigured by ITS with recommended settings, viewable in PGPKeys under **EDIT** and **PREFERENCES**. Under the **GENERAL** tab, **ALWAYS ENCRYPT TO DEFAULT KEY** causes your own key to be added to the list of encryption keys for each message or file you encrypt, so that you can always decrypt the result. Otherwise, you would be unable to decrypt an item you have encrypted.

If you are using PGP heavily, ITS recommends **caching** the decryption and signing passphrase so that you don't have to continually retype the passphrase. The recommended length of time before you would have to retype the passphrase varies, depending on the security of your work area. If you are not located in a public area and need not be concerned that an unauthorized person will take advantage of your absence, ITS recommends caching your decryption passphrase for **5 minutes** and your signing passphrase for **30 minutes**. However, shorten these times or uncheck the cache checkboxes if your work area is easily accessible and you are frequently away from your desk.

The **FILES** tab lists the locations of your keyring files. Do not change these settings after your initial installation.

The **EMAIL** tab tells PGP how to behave when used with email. Leave **USE PGP/MIME WHEN SENDING EMAIL** unchecked. Leaving the **WORD WRAP** setting at **60** prevents a problem caused by mailers that wrap the text of incoming signed messages at a shorter length, thereby "altering" the message and rendering the signature invalid.

The **SERVER** tab lists available key servers and gives information about the default key server (Caltech's key server should always be your default) and when to search for keys. We recommend leaving these checkboxes blank in order to avoid lengthy automatic searches. See the next page for instructions on adding a new key server to your list.

Adding a public key server to the Server list
To add a PGP public key server to the preconfigured Caltech and third-party servers:

1. Launch PGPKeys.

2. From the **EDIT** menu, select **PREFERENCES**, and then the **SERVERS** tab.

3. Click **NEW** and then type in the address for the new key server to be added to the list. Leave **PORT** blank unless the server uses an unusual port for this service. If the server uses the HTTP protocol instead of the default LDAP protocol, you will probably need to contact the server administrator to learn the correct port number.

4. Click **OK** to add the server to the list.

Encryption options
When you encrypt a file using PGP for the PC, the Recipients window allows you to set some options. One is **CONVENTIONAL ENCRYPTION**, explained below. The **TEXT OUTPUT** option is useful if your correspondent is using an older email program, or a mail server that can't handle modern email encoding methods. If you're sending mail to a Caltech user, **TEXT OUTPUT** should be unnecessary.

Uses of conventional encryption instead of public key encryption
To encrypt a file for storage on your hard drive, or for a recipient whose public key is unknown to you, select "conventional" (also known as "private key") encryption. This will create a file that PGP can decrypt by using a special password or passphrase that you assign to that file. No public key is used. This can be useful for encrypting confidential files that are stored on a shared hard drive, or for a file that may be distributed to an unknown number of people. If it is encrypted with a password rather than to a person's public key, the file can be decrypted by any PGP user who has the password. While similar to the password protection feature of applications such as Word, Excel, and FileMaker Pro, this method is more secure. NOTE: *if the password is forgotten, there will be no way to decrypt the file.* Use this feature with **extreme caution**.

To encrypt a file with a password or passphrase only:

1. Locate the document in Windows Explorer file or by clicking on the My Computer icon.

2. Highlight the file to be signed or encrypted; right-click and choose PGP from the resulting menu, then select **ENCRYPT** from the pull-down menu.

3. PGP opens the key-ring window. Click the **USE CONVENTIONAL ENCRYPTION** checkbox, then click **OK**. Note: To guard against a possible mishap, do not select **WIPE** (see "The WIPE Command" on page 13) at this time, as it irretrievably destroys the original, unencrypted copy of the file.

4. Type in a word or phrase as a "conventional" passphrase for encrypting this document, and again at the confirmation box, and then click **OK**.

5. If you are using conventional encryption as a method of secure storage, delete or **WIPE** the original, unencrypted, document. See "The WIPE Command" on page 13 for instructions.

Changing your passphrase
There is no technical reason to change your passphrase, but you may change it often as you wish, either to make it easier to remember, or to replace it in the event that you suspect it has been compromised in some way. To change the passphrase for your key pair:

1. Launch PGPKeys.

2. Select the key pair whose passphrase you wish to change.

3. Select **KEYS** from the menu bar, and then either select **KEY PROPERTIES** or click the  button on the PGPKeys button bar.

4. Select the **GENERAL** tab and click the **CHANGE PASSPHRASE** button.

5. Enter your current passphrase. This requirement helps prevent someone else from sitting at your computer and changing your existing passphrase.

6. Enter the new passphrase. Tab to the confirmation window and type it a second time to check for typos. Click **OK** or hit **<enter>**. A message will display indicating that the passphrase has been changed.

7. Click **CLOSE** to exit this key's **PROPERTIES** window.

A note about remembering your passphrase and keeping keys secure
It is of utmost importance that you choose a passphrase that you will remember. Without your passphrase, you would be unable to use your PGP key pair to encrypt or sign new messages. You would also be unable to decrypt any files or messages that are encrypted to your public key. If you forget your passphrase, you will have to revoke your old public key, create a new one, and then redistribute it to the key server and your correspondents. If your original key pair was configured for Caltech use, your older encrypted messages would be decryptable only by the Security Manager using the Caltech Security Master Key.

Similarly, the private and public components of your key pair, which are stored in files named **secring.pkr** and **pubring.pkr**, must also be kept secure. Loss of these files would prevent you from using your key pair. Anyone who gains access to these files and knows your passphrase would be able to decode your encrypted files, or sign documents with your digital signature.

Because your private and public key files are so critical to the functioning of PGP, the program automatically prompts you to make a backup copy of each file when you exit the program after making a change to your keyring. It's a good idea to allow PGP to do this, in case you accidentally delete a needed key or otherwise inadvertently damage your keyring.

ITS recommends that you select a passphrase that can be remembered without being written down, and that you ensure that your PGP key pair is backed up to a secure backup medium. In the event of a hard-drive failure or other problem with your files, this will preserve your ability to encrypt, sign, and decrypt.

PGPDisk for secure file storage
A reference guide for this feature is forthcoming.

Quick Reference

Quick Reference, cont'd