When the “**Always encrypt to default key**” setting is checked, all e-mail messages or file attachments you encrypt with a recipient’s public key will also be encrypted to you using your default public key. It is useful to have this setting turned on so that you have the option of decrypting the contents of any e-mail you have previously sent.

When **Always use PGP/MIME encryption** is checked, you do not have to go through the trouble of explicitly turning on the PGP/MIME feature every time you send out e-mail. For instance, if you are using Eudora, and you turn this setting on, all of your e-mail messages and file attachments will automatically be encrypted to the intended recipient. This setting has no effect on other encryptions you perform from the clipboard or for Windows Explorer and should not be used if you intend on sending e-mail to recipients who are not using e-mail applications that support the PGP/MIME standard.

The **Private Key Ring File** shows the current location and name of the file where the PGP program expects to find your Private keyring file. If you plan on storing your private keys in a file with a different name or in some other location, then you will need to specify this information here..

By checking the “**Faster key generation**” setting, you can decrease the amount of time it takes to generate a new set of DSS/Diffie-Hellman keys.

The **Public Key Ring File** shows the current location and name of the file where the PGP program expects to find your Public keyring file. If you plan on storing your public keys in a file with a different name or in some other location, then you specify this information here. Some users like to keep their private keyring on a floppy and then only insert this disk when they need to sign or decrypt mail. You can use the browse button to search through your files rather than having to explicitly type in the path.

The **Cache encryption passphrase for [ ] seconds** setting specifies the amount of time (in seconds) that your encryption passphrase is stored in your computer's memory. If you regularly compose or read several e-mail messages in secession, then you may want to increase the amount of time your passphrase is cached so you don't have to enter your passphrase over and over again to get through all of your mail. However, you should be aware that the longer your passphrase is stored in your computers memory, the more time a sophisticated snooper has to get hold of this highly compromising bit of information. By default, this setting is set to 120 seconds which is probably sufficient to perform most of your PGP chores without having to enter your passphrase too many times but not for someone to determine your passphrase.

Your passphrase should contain multiple words and may include spaces, numbers, and other printable characters. Choose something that you can remember easily but that others will not be able to guess and keep in mind that the passphrase is case-sensitive. The longer your passphrase, and the wider variety of characters it contains, the more secure it is. Try to include equal numbers of upper and lower case alphabetic characters, numbers, punctuation marks and so on.

When **Use PGP/MIME signing** is checked, you do not have to go through the trouble of explicitly turning on the PGP/MIME feature every time you send e-mail with an e-mail application that supports this standard. For instance, if you are using Eudora, and you turn this setting on, all of your e-mail messages and file attachments will automatically include your digital signature. This setting has no effect on other signatures you add from the clipboard or for Windows Explorer and should not be used if you

The **Word wrap clear-signed messages at column [ ]** setting allows you to specify the column number where a hard carriage return should be used to wrap the text in your digital signature to the next line. This feature is necessary since all applications do not handle word wrapping in the same way which could cause the lines in you digital signature to be broken up in a way that cannot be read properly. By default, this setting is set to 78, which prevents any problems with most applications.

When checked, your typing will not display.

Select **Create** after all the fields on the New Master Key Screen have been completed to create a new key.

Enter your user name.

Enter your key size here. Key size ranges from 768-3072 bits. A standard key size is 1024 bits A larger key size provides more security, but also takes longer to perform encryption and decryption functions.

Select your key type:

- RSA used for older versions of PGP
- DSS/Diffie-Hellman for use with PGP version 5.0 or above
  Note: The person you are exchanging mail with must use version 5.0 of PGP to receive mail using the DSA key.

Select to set your key to never expire.

Enter the number of days for your key to expire.

A unique identifying number associated with each key. This number distinguishes between two keys with the same user name and e-mail address.

Displays the date the key was created.

The key type - Either RSA or DSS/Diffie-Hellman.

The date the key expires. The owner specifies this date when a key is created. The value is usually set to never. However, if the owner only wants a key used for a limited period of time, the key can be set to expire on a specific date.

Indicates the validity of the key, based on its certification and the level of trust you have in the owner to vouch for the authenticity of someone else's public key. Set the trust level by sliding the bar to the appropriate level (complete, marginal, or untrustworthy).

This bar indicates the level of confidence that the key actually belongs to the purported owner. The validity is based on who has certified the key and how well you trust the signer to vouch for the authenticity of a key

Displays the level of trust.

Key trust slider.

This bar indicates the level of trust you have granted to the owner of a key to serve as an introducer for the public keys of others. This trust comes into play when you are unable to verify the validity of someone's public key for yourself and instead choose to rely on the judgment of other users who have certified the key in the past.

A unique identification number generated when the key is created. This is the primary means for checking the authenticity of a key. The optimum way to check a fingerprint is to have the owner read their fingerprint over the phone and then compare it to the fingerprint on your copy of their public key. You can also check the authenticity of someone's key by comparing the fingerprint on your copy to the one listed on a public key server, since it is assumed the owner periodically checks to make sure the fingerprint remains valid.

Indicates whether or not the key is currently enabled. When a key is disabled, it is dimmed out in the PGPkeys window and is not be available for performing any PGP functions. However, the key remains on your keyring where it can later be enabled if necessary. To enable or disable a key, use this box, or select Enable or Disable from the **Keys** pull-down menu.

Allows you to change the passphrase for a private key.

When selected, automatically sets the highest level of trust.

When checked, your typing will not display.

When checked, messages are automatically encrypted.

When checked, messages are automatically signed.

By default, this setting is set to 120 seconds which is probably sufficient to perform most of your PGP chores without having to enter your passphrase too many times but not for someone to determine your passphrase.

Allows you to select the file where your private keyring files are stored.

Allows you to select the file where your public keyring files are stored.

Closes this dialog box and save any changes you have made.

Closes this dialog box without saving any changes you have made.

Type your passphrase here. If the Hide Typing box is checked, your passphrase will not display.

Type your current passphrase.

Type your new passphrase here. Your passphrase must be at least 8 characters.

Confirm your new passphrase by typing it again and then click **OK**.

The minimum validity bar indicates the minimum level of confidence that the public keys in the Recipient list are valid. This validity is based on the certification and validity associated with the key and those who have signed it.

If you are adding your signature to the encrypted file and would like the signature stored in a separate file, then you can place a check in the **Separate Signature File** check box.

You can also check the **Text Output checkbox** if you want the output of the encrypted file saved in a text format that can be handled by all e-mail applications. You should note that this option will add to the size of the file.

Place the names of the users who are to receive a copy of the encrypted e-mail message in the Recipients list box by dragging the user name to the Recipient list box.

This box displays the user names and their public keys. Click on and drag each of the public keys for those who are to receive a copy of the encrypted e-mail message to the Recipient list box.

Yes, delete this key.

Yes, delete all the selected private/public keys.

No, don't delete this key. (The next key will display if more than one key was selected.)

Cancels deletion of keys and closes this dialog box.

This setting, when checked, allows you to specify the column number where a hard carriage return should be used to wrap the text in your digital signature to the next line. This feature is necessary since all applications do not handle word wrapping in the same way which could cause the lines in you digital signature to be broken up in a way that cannot be read properly. By default, this setting is set to 78, which prevents any problems with most applications.

Create Dialog

Create a new set of keys.

Enter your new mail address in this field.

Check this box to specify the agent.

The Key Wizard

The Key Wizard will lead you through the steps required to create a key pair. Follow the instructions presented on each screen and click on the appropriate Help buttons for more detailed information.

For complete instructions which you can read while creating your key, see the following topic:

PGP Key Wizard

User Name

Enter your name on the first line and your e-mail address on the second line. It’s not absolutely necessary to enter your real name or even your e-mail address. However, using your real name makes it easier for others to identify you as the owner of your public key. Also, by using your correct e-mail address, you and others can take advantage of one of the plug-in features that automatically calls the appropriate key when you address mail to a particular recipient.

Key Type

Select a key type, either DSS/Diffie-Hellman or RSA

Earlier versions of PGP use an older technology referred to as RSA to generate keys. Beginning with this version of PGP, you have the option of creating a new type of key based on the newer DSS/Diffie-Hellman technology.

- If you plan to correspond with individuals who are still using the older RSA keys, you will probably want to generate an RSA key pair that is compatible with older versions of the program.
- If you plan to correspond with individuals who have the latest version of PGP, you can take advantage of the new technology and generate a pair of DSS/Diffie-Hellman keys.
- If you want to be able to exchange e-mail with all PGP users, you should make a pair of RSA keys and a pair of DSS/Diffie-Hellman keys and then use the appropriate set depending on the public key used by the recipient.

Key Size

Select a key size (from 768 to 3072) or enter any key size from (from 768 to 4096).

The key size corresponds to the number of bits used to construct your digital key. The larger the key, the less chance that someone will ever be able to crack it, but the longer it will take to perform the decryption and encryption process. You will need to strike a balance between the convenience of performing PGP functions quickly with a smaller key and the increased level of security provided by a larger key. Unless you are exchanging extremely sensitive information that is of enough interest that someone would be willing to mount an expensive and time consuming cryptographic attack in order to read it, you are probably safe using a key composed of 1024 bits.

Expiration Date

Indicate when you want your keys to expire.

You can either go with the default selection which is “never”, or you can enter a specific number of days after which the keys will expire.

Once you create a key pair and have distributed your public key to the world, you will probably continue to use the same keys from that point on. However, under certain conditions, you may want to create a special set of keys that you plan to use for a limited period of time. In this case, when the public key expires it can no longer be used by someone to encrypt mail for you but it can still be used to verify your digital signature. Similarly, when your private key expires, it can still be used to decrypt mail that was sent to you before your public key expired but can no longer be used to sign mail for others.

Passphrase

In the “Passphrase” entry box, enter the string of characters or words you want to use to gain exclusive access to your private keys. To confirm your entry, press the **Tab** key to advance to the next line, then enter the same passphrase again.

Normally, as an added level of security, the characters you enter for the passphrase do not appear on the screen. However, if you are sure that no one is watching over your shoulder, and you would like to see the characters of your passphrase as you type, clear the “Hide Typing” check box.

TIP: Your passphrase should contain multiple words and may include spaces, numbers, and other printable characters. Choose something that you can remember easily but that others won’t be able to guess, and keep in mind that the passphrase is case sensitive. The longer your passphrase, and the wider the variety of characters it contains, the more secure it is. Try to include equal numbers of upper and lowercase alphabetic characters, numbers, punctuation marks and so on.

Random Data Generation

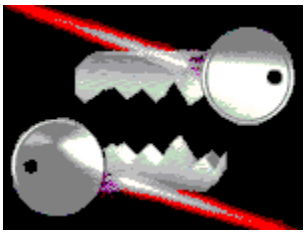
If there is not enough random information upon which to build the key, the PGP Random Data dialog box appears. As instructed on the screen, move your mouse around and enter a series of random keystrokes until the progress bar in the dialog box is completely filled in. Your mouse movements and keystrokes generate random information that is needed to generate a unique key pair.

Key Generation Process

The Key Generation Wizard indicates that it is busy generating your key.

If you have entered an inadequate passphrase, a warning message appears before the keys are generated and you have the choice of accepting the bad passphrase or entering a more secure one before continuing.

After the key generation process begins, it may take several minutes to generate the keys.



Eventually, the Key Generation Wizard indicates that the key generation process has completed.

Sign New Key With Old

If you have created a new key pair using the same user name and e-mail address as another key pair, you may elect to sign the new key with your old key. This will allow anyone who has previously designated your older key as trustworthy to be able to trust that your new key belongs to you.

Send Key To Key Server

The Key Generation Wizard indicates that you have successfully generated a new key pair and that it is about to send your public key to the public key server.

Specify whether you want your new public key to be sent to the key server by checking the check box. By sending your public key to the key server, anyone will be able to get a copy of your key when they need it. See the section on distributing your public key presented later in this chapter for complete details.

Sending Key To Server

This message indicates that your new public key is being sent to a server where other PGP users can easily get a copy so that they can send you encrypted email and verify your digital signature.

Key Generation Completed

When the Key Generation process completes a pair of keys representing your newly created keys appears in the PGPkeys window. You will notice that the older RSA keys are blue and the newer DSS/Diffie-Hellman keys are yellow. At this point you can examine your keys by checking their properties and the values associated with them; you may also want to add other user names or e-mail addresses.

Possibly Corrupted Keyring File

PGP has detected a possible problem with one or more of your keyring files. You are given the choice of using a previous backup of the kekyring files or you can select new keyring files.

Select Signing Key

Allows you to select the appropriate key to sign with.

Text Output Option

You can also check the **Text Output checkbox** if you want the output of the encrypted file saved in a text format that can be handled by all e-mail applications. You should note that this option will add to the size of the file.

Sign Cache Enable

Specifies the amount of time (in seconds) that your encryption passphrase is stored in your computer's memory. If you regularly compose or read several e-mail messages in secession, then you may want to increase the amount of time your passphrase is cached so you don't have to enter your passphrase over and over again to get through all of your mail. However, you should be aware that the longer your passphrase is stored in your computers memory, the more time a sophisticated snooper has to get hold of this highly compromising bit of information. By default, this setting is set to 120 seconds which is probably sufficient to perform most of your PGP chores without having to enter your passphrase too many times but not for someone to determine your passphrase

Sign Cache Seconds

By default, this setting is set to 120 seconds which is probably sufficient to perform most of your PGP chores without having to enter your passphrase too many times but not for someone to determine your passphrase

Warn When Using Marginaly Trusted Keys

When the **Warn When Using Marginally Trusted Keys** is checked, you will be warned whenever you attempt to use a public key that is not considered completely valid.

Send Signature To Server

By checking this checkbox, you can send the selected public key along with your signature to the public server where it will replace any previous versions of the key. By signing someone's public key, you are stating to all other PGP users that you are vouching for the validity of the key and that you are absolutely confident that the key does indeed belong to the purported owner. Out of courtesy, you should probably check with the owner of the key before appending your signature to their public key.

Specifies the address for the public key server that is used by PGP to send and retrieve public keys. You should not change this unless you have a different location.

The port address for the public key server.

When this setting is selected, even unknown keys will be retrieved from the public key server.

Reverts to the default server name and port number settings for the key server.

Overview

With PGP[a] for Personal Privacy, Version 5.0 you can easily protect the privacy of your e-mail messages and file attachments by encrypting them so that only those with the proper authority can decipher the information. You can also digitally sign the messages and files you exchange, which ensures that they have come from the person who allegedly sent them and that the information has not been tampered with in any way while in transit.

The most convenient way to use PGP is through one of the popular e-mail applications supported by the plug-ins. This allows you to encrypt and sign as well as decrypt and verify your messages while you are composing and reading your mail. In addition, if you are communicating with another PGP user who is using an e-mail application that adheres to the PGP/MIME standard, you can perform all of the PGP functions on both your messages and any file attachments by simply clicking a button when sending or receiving your e-mail.

If you are using an e-mail application that is not supported by the plug-ins, you can easily transfer the text of your e-mail messages to the clipboard and perform the necessary functions from there. In addition, if you need to encrypt or decrypt entire file attachments, you can do so directly from the Windows Explorer by choosing the appropriate menu option.

Here are some of the features offered by PGP:

- Widely-trusted encryption and decryption incorporating maximum-strength cryptographic technologies
- Digital signature and verification for certifying messages and files
- Quick access to all functions from easily selectable menu items
- Integrated plug-in support for popular e-mail applications
- Implementation of PGP/MIME for quick encryption and decryption of messages and file attachments when sending and receiving e-mail
- Simple key generations with up to 4096-bit keys and support for multiple key formats (RSA and DSS/Diffie-Hellman)
- Sophisticated key management with graphical representations of key properties
- Integrated support for distributing and retrieving keys from public key servers

Using PGP

Using PGP From Supported Mail Applications

Performing PGP Functions from the Windows Clipboard

Performing PGP Functions from Windows Explorer

Using PGP

PGP is based on a widely accepted encryption technology known as "public key cryptography" in which two complementary keys are used to maintain secure communications. One of the keys is a private key to which only you have access and the other is a public key which you freely exchange with other PGP users. Both, your private and your public keys are stored in keyring files which are accessible from the PGPkeys window in which you perform all your key management functions.

To send someone a private e-mail message, you use a copy of that person's public key to encrypt the information, which only they can decipher by using their private key. Conversely, when someone wants to send you encrypted mail, they use a copy of your public key to encrypt the data, which only you can decipher by using a copy of your private key.

You also use your private key to sign the e-mail you send to others. The recipients can then use their copy of your public key to determine if you really sent the e-mail and whether it has been altered while in transit. When someone sends you e-mail with their digital signature, you use a copy of their public key to check the digital signature and to make sure that no one has tampered with the contents.

With the PGP program you can easily create and manage your keys and access all of the functions for encrypting and signing as well as decrypting and verifying your e-mail messages and file attachments.

The following section provides a quick run-through of the procedures you normally follow in the course of using PGP. For details concerning any of these procedures, refer to the appropriate chapters in this book where they are fully explained.

Create a Private and Public Key Pair

Before you can begin using PGP, you need to generate a key pair consisting of a private key to which only you have access and a public key that you can copy and make freely available to everyone with whom you exchange e-mail. You have the option of creating a new key pair immediately after you have finished the PGP installation procedure or you can do so at any time by opening the PGPkeys window.

Exchange Public Keys with Others

After you have created a key pair, you can begin corresponding with other PGP users. To do so, you will need a copy of their public key and they will need a copy of your public key. Since your public key is just a block of text, it is really quite easy to trade keys with someone. You can either include your public key in an e-mail message, copy it to a file or you can post it on a public key server where anyone can get a copy when they need it.

Certify and Validate Your Keys

Once you have a copy of someone's public key, you can add it to your public keyring. You should then check to make sure that the key has not been tampered with and that it really belongs to the purported owner. You do this by comparing the unique "fingerprint" on your copy of someone's public key to the fingerprint on their original key. When you are sure that you have a valid public key, you sign it to indicate that you feel the key is safe to use. In addition, you can grant the owner of the key a level of trust indicating how much confidence you have in them to vouch for the authenticity of someone else's public key.

Encrypt and Sign Your E-mail

After you have generated your key pair and have exchanged public keys, you can begin encrypting and signing e-mail messages and file attachments.

- If you are using an e-mail application supported by the plug-ins, you can encrypt and sign your messages by selecting the appropriate options from your application's tool bar. In addition, if you are communicating with other PGP users who are using an e-mail application such as PGP which adheres to the PGP/MIME standard, you can encrypt and sign messages as well as file attachments

automatically when you send your mail.

- If your e-mail application is not supported by the plug-ins, you can copy the message to the clipboard and perform the appropriate functions from there. If you want to include any file attachments, you can encrypt and sign them from the Windows Explorer before attaching them to your e-mail.

Decrypt and verify your e-mail

When someone sends you encrypted e-mail, you can unscramble its contents and verify any appended signature to make sure that the data originated with the alleged sender and that its contents have not been altered.

- If you are using an e-mail application that is supported by the plug-ins, you can decrypt and verify your messages by selecting the appropriate options from your application's tool bar. In addition, if your e-mail application supports the PGP/MIME standard, you can decrypt and verify messages and file attachments sent using this format by clicking on an icon when reading your mail.
- If your e-mail application is not supported by the plug-ins, you can copy the message to the clipboard and perform the appropriate functions from there. If you want to decrypt and verify file attachments, you can do so from the Windows Explorer.

Generate a Private and Public Key pair

Before you begin using PGP, you must generate a set of keys:

- A private key that only you posses
- A public key that you copy and give to others in order to exchange secure and certified e-mail.

You generate a new key pair from the PGPkeys window using the PGP Key Wizard that guides you through the process.

Making a New Set of Keys

Protecting your Keys

Verifying the Authenticity of a Key

Exchanging Keys With Others

PGP is based on a widely accepted and highly trusted "public key encryption" system by which you and other PGP users generate a key pair consisting of a private key and a public key. As its name implies, only you have access to your private key, but in order to correspond with other PGP users you need a copy of their public key and they need a copy of your public key. You use your private key to sign the e-mail messages and file attachments you send to others and to decrypt the messages and files they send to you. Conversely, you use the public keys of others to send them encrypted mail and to verify their digital signatures.

NOTE:

> Without going into too much technical detail, you might be interested to know that it is not actually the content of the e-mail that is encrypted using the public key encryption scheme. Instead, the data is encrypted using a much faster single-key algorithm, and it is this single key that is actually encrypted using the recipients public key. The recipient then uses their private key to decrypt this key, which allows them to decipher the encrypted data.

Your private key is also used to sign the contents of a given e-mail message or file attachment. Anyone who has a copy of your public key can check your digital signature to confirm that you are the originator of the mail and that the contents have not been altered in any way during transit. In the same way, if you want to verify somebody else's digital signature or check the integrity of the e-mail they send to you, then you need a copy of their public key to do so.

This version of PGP supports two distinct types of keys -- the traditional RSA key used in older versions of PGP and a new type of key called DSS/Diffie-Hellman which is based on the latest advancements in cryptographic technologies. If you plan to exchange e-mail with someone who has PGP or later, then you can take advantage of the new DSS/Diffie-Hellman keys. However, if you are corresponding with someone who is using a previous version of PGP, you have to use the traditional RSA keys to communicate with them.

NOTE:

> If you are upgrading from an earlier version of PGP, you have probably already generated a private key and have distributed its matching public key to those with whom you correspond. In this case you don't have to make a new key pair (as described in the next section) because your old keys are automatically extracted from the files where they were previously stored and are immediately available for your use.

Distributing Your Public Key

Obtaining the Public Keys of Others

Verifying the Authenticity of a Key

Protecting your Keys

Distributing Your Public Key

After you create your keys, you need to make them available to others so that they can send you encrypted e-mail and verify your digital signature. You have several alternatives for distributing your public key:

- Make your public key available through a public key server
- Include your public key in an e-mail message
- Export your public key or copy it to a text file

Since your public key is basically composed of a block of text, it is really quite easy to make it available through a public key server, include it in an e-mail message or export or copy it to a file. The recipient can then use whatever method is most convenient to add your public key to their public keyring.After creating a set of keys, you need to make them available to others so they can send you encrypted e-mail and verify your digital signature.

Make your key available through a public key server

Including your public key to an e-mail message

Export your public key to a text file

Obtaining the Public Keys of Others

Just as you need to distribute your public key to those who want to send you encrypted mail or to verify your digital signature, you need to obtain the public keys of others so you can send them encrypted mail or verify their digital signatures. You have several alternatives for obtaining someone's public key:

- Get the key from a public key server
- Add the public key directly from an e-mail message
- Import the public key from a file

Since public keys are really just blocks of text, it is really quite easy to add keys to your keyring by importing them from a file or by copying them from an e-mail message or a key server and then pasting them into your public keyring. Here are the alternatives for obtaining someone's public key:

Get the key from a public key server

Add the public key directly from an e-mail message

Import a Public Key from a File

Protecting your Keys

Once you have generated a key pair, it is wise to create a spare set and put them in a safe place in case something happens to the originals. In fact, when you close the PGPkeys window after creating a new key pair, you are prompted to save a backup copy.

Your private keys and your public keys are stored in separate keyring files, which you can copy just like any other files to another location on your hard drive or to a floppy disk. By default, the private keyring (secring.pgp) and the public keyring (pubring.pgp) are stored along with the other program files in the PGP file directory, but you can save your backups in any location you like.

When you specify that you want to save a backup copy of your keys, the "Select Backup Destination" dialog box appears asking you to specify the location of the private keyring file that is to be backed up.

Besides making backup copies of your keys, you should be especially careful about where you store your private key. Even though your private key is protected by a passphrase that only you should know, it is possible that someone could discover your passphrase and then use your private key to decipher your e-mail or forge your digital signature. For instance, somebody could look over your shoulder and watch the keystrokes you enter or intercept them on the network or even over the airwaves.

To prevent anyone who might happen to get hold of your passphrase from being able to use your private key, you should only store it on your own computer. If your computer is attached to a network, you should also make sure that your files are not automatically included in a system-wide backup where others might gain access to your private key. Given the ease with which computers are accessible over today's networks, if you are working with extremely sensitive information, you may want to keep your private key on a floppy disk which you can insert like an old fashioned key whenever you want to read or sign your private mail.

As another security precaution, consider assigning a different name to your private keyring file and then storing it somewhere other than in the default PGP file directory. where it will not be so easy to locate. You use the PGPkeys Preferences dialog box to specify a name and location for your private and public key ring files.

Verifying the Authenticity of a Key

When you exchange keys with someone, it is sometimes hard to tell if the key really belongs to that person. PGP provides a number of safeguards by allowing you to check a key's authenticity, to vouch for its integrity. The PGP program will also warn you when you attempt to use a key that is not completely trusted.

One of the major vulnerabilities of public key enrcryption systems is the ability of some eavesdropper to mount a "man-in-the-middle" attack by replacing someone's public key with one of their own. In this way they can intercept any encrypted e-mail intended for that person, decrypt it using their own key, then encrypt it again with the person's real key and send it on to them as if nothing had ever happened. In fact, this could all be done automatically through a sophisticated computer program that stands in the middle and deciphers all of your correspondence.

Based on this scenario, you and those with whom you exchange mail need a way to determine whether you do indeed have legitimate copies of each others keys. The only way to be completely sure that a public key actually belongs to a particular person is to have the owner copy it to a diskette and then physically hand it to you. Since you are not always within close enough proximity to personally hand a disk to someone, you will generally exchange public keys via e-mail or get them from a public key server.

Even though these are somewhat less secure methods of exchanging tamper-proof keys, you can still determine if a key really belongs to a particular person by checking its digital fingerprint, a unique series of numbers generated when the key is created. By comparing the fingerprint on your copy of someone's public key against the fingerprint on their original key, you can be relatively sure that you do in fact have a valid copy of their key.

The most definitive way to check a a key's fingerprint is to call the person and have them read their fingerprint over the phone. When you get a key from a public key server, you don't have to go through this exercise but can instead access the fingerprint information for the key while you are on-line. Of course, you do this with the expectation that the person periodically checks their key to make sure that no one has switched keys.

Once you are absolutely convinced that you have a legitimate copy of someone's public key, you can then sign their key. By signing someone's *public key* with your *private key,* you are signifying to the world that you are sure the key belongs to the alleged user. For instance, when you create a new key, it is autonomically certified with your own digital signature, since it is a reasonably safe assumption that the person creating the key is in fact the true owner. The reason for signing your own key is to prevent anyone from modifying it which would immediately invalidate your signature.

PGP users often have other trusted users sign their public keys to further attest to their authenticity. For instance, you might send a trusted colleague a copy of your public key with a request that they certify and return it so you can include their signature when you post your key on a public key server. Now, when someone gets a copy of your public key, they don't necessarily have to check the key's authenticity themselves, but can instead rely on how well they trust the person who signed your key. PGP provides the means for establishing this level of trust for each of the public keys you add to your public keyring and shows the level of trust associated with each key in the PGPkeys window. This means that when you get a key from someone whose key is signed by a trusted introducer, you can be fairly sure that the key belongs to the purported user.

Encrypt and Sign Data

The quickest and easiest way to encrypt and sign e-mail is with an application supported by the PGP plug-ins. Although the procedure varies slightly between different e-mail applications, you perform the encryption and signing process by clicking the appropriate buttons in the application's toolbar. In addition, if you are using an application such as Eudora, that supports the PGP/MIME standard, you can encrypt and sign your e-mail messages as well as any file attachments when you send or receive your e-mail.

If you are using an e-mail application that is not supported by the PGP plug-ins, you can encrypt and sign your e-mail messages via the Windows clipboard. To include any file attachments, you encrypt the files from the Windows Explorer before attaching them. Click on the appropriate topic below for more information:

Selecting Recipients

To Encrypt and Sign with Eudora

To Encrypt and Sign from the Clipboard

To Encrypt and Sign from Windows Explorer

Decrypt and Verify Data

The quickest and easiest way to decrypt and verify the e-mail sent to you is with an application supported by the PGP plug-ins. Although the procedure varies slightly between different email applications, when you are using an e-mail application supported by the plugins, you can perform the decryption and verification process by clicking a button in your application's toolbar. In addition, if you are using an application such as Eudora, that supports the PGP/MIME standard, you can decrypt and verify your e-mail messages as well as any file attachments by just clicking an icon attached to your e-mail.

If you are using an e-mail application that is not supported by the PGP plug-ins, you will decrypt and verify your e-mail messages via the Windows clipboard. Also, if your e-mail includes encrypted file attachments, you must decrypt them separately from the Windows Explorer. See the appropriate topic below for further information:

Decrypting and Verifying Within Your Mail Application (Eudora)

Decrypting and Verifying Signatures Via the Clipboard

Decrypting and Verifying from Windows Explorer

Using PGP from Supported E-mail Applications

If you have one of the popular e-mail applications supported by the PGP plug-ins, you can access the necessary PGP functions by clicking the appropriate buttons in your application's toolbar. For example, if you are using Eudora, you click the lock icon to indicate that you want to encrypt your message and the quill icon to indicate that you want to sign it. When you are ready to send your message, you click the PGP button to initiate the encryption and signatory functions and then send the scrambled text to the intended recipient.

When you receive e-mail from another PGP user, you decrypt the message and verify the person's digital signature by clicking the open lock.

You can also access the PGPkeys window at any time while composing or retrieving your mail by clicking the double keys button.

To make things even simpler, if you are exchanging e-mail with another party who is also using PGP and Eudora (or some other e-mail application which adheres to the PGP/MIME standard), both of you can automatically encrypt and decrypt your e-mail messages and any attached files when you send or retrieve your mail. All you have to do is turn on the PGP/MIME encryption and signatory functions from the PGP Preferences dialog box.

When you receive e-mail from someone who uses the PGP/MIME feature, the mail arrives with an attached icon indicating that it is PGP/MIME encoded.

When you receive PGP/MIME encapsulated mail, all you need do to decrypt its contents and verify any digital signatures is to double-click the key icon.

Opening the PGPkeys Window

Accessing PGP From the Windows Clipboard

Accessing PGP from Windows Explorer

PGP Encrypt and Sign

PGP Decrypt and Verify

Performing PGP Functions from the Windows Clipboard

If you are using a mail application that is not supported by the PGP plug-ins, or are working with text generated by another application, you perform your encryption/decryption and signature verification functions via the Windows clipboard.

For instance, to encrypt or sign text:

1. Copy the text from your application to the clipboard.
2. Encrypt and sign it using the appropriate PGP functions.
3. Copy and paste it back into your application.
4. Send it to the desired recipient.

When you receive an encrypted or signed e-mail message, reverse the process and copy the ciphertext from your application to the clipboard, decrypt and verify the information, then view the contents and, if applicable, save it to a file.

To access the PGP functions from the Windows clipboard, place your cursor on the **key and lock** icon in the corner of the window and press the right mouse button.

There are selections for encrypting and signing and for decrypting and verifying the contents of the clipboard, depending on whether you are sending or retrieving your mail. There are also options for editing or viewing the contents of the clipboard and for accessing the PGP Preferences dialog box, where you specify settings that affect how PGP is configured.

To Encrypt and Sign Via the Clipboard (procedures for AOL)

Decrypting and Verifying Signatures Via the Clipboard

Performing PGP Functions from Windows Explorer

If you want to encrypt and sign or decrypt and verify files such as word processing documents, spreadsheets, or even entire programs, you can do so directly from Windows Explorer. If you are not using an e-mail application such as Eudora, you will have to use this method for attachments to e-mail messages. In some cases, you may want to encrypt and decrypt files that you store on your computer in order to prevent others access to them. To access PGP functions from Windows Explorer, select the appropriate options from the **File** menu.

The options that display depend on the current state of the selected file. You can also send the file directly by choosing the Encrypt and Send option.

To Encrypt and Sign from Windows Explorer

To Decrypt and Verify from Windows Explorer

Managing Keys

The keys you create as well as those you obtain from others are stored in digital keyrings, which are essentially files stored on your hard drive or a floppy disk. Your private keys are normally stored in the file named secring.pgp and your public keys in the file pubring.pgp. Both are usually located in the same program directory as the other PGP program files.

NOTE:

> If you have more than one set of keys, or you are not comfortable storing your keys in the usual place, you can choose a different file name or location. (See: Establishing your Preferences)

You may occasionally want to examine or change the attributes associated with your keys. For instance, when you obtain someone's public key, you might want to identify its type (either RSA or El/Gamal), check its fingerprint, or determine its validity based on any digital signatures included with the key. You may also want to sign someone's public key to indicate you believe it is valid, assign a level of trust to the key's owner, or even change a passphrase for your private key.

You perform all of these key management functions from the **PGPkeys window** .

About Keys and Keyrings

Adding a New User Name or Address

Changing your Passphrase

Checking a Keys Fingerprint

Deleting a Key or Signature

Disabling and Enabling Keys

Examining a Key's Properties

Exchanging Keys With Others

Granting Trust for Key Validations

Revoking Keys

Protecting your Keys

Signing Someone's Public Key

Specifying a Default Key Pair

Verifying the Authenticity of a Key

Importing and Exporting Keys

In addition to distributing public keys by cutting and pasting the key text from a public key server, you can also exchange keys by importing and exporting them as separate text files. This allows you to distribute public keys on a disk on over an FTP server.

To import a key from a file:

1. Select and highlight the key you want to import to a file.
2. Choose **Import** from the **Keys** menu. The **Select File Containing Key** dialog box appears.
3. Locate the file containing the key you want to import, then click the **Open** button.

   The imported key displays in the PGPkeys window and is available for use.

To export a key to a file:

1. Select the icon representing your key pair from the PGPkeys window, then choose Export from the Keys menu. The Export Key to File dialog box appears.
2. Enter the name of the file where you want the key to be exported and click Save.

   The exported key is saved to the named file in the specified directory location.

The PGPkeys Window

All key management functions are performed from the PGPkeys Window.

1. To open the PGPkeys window, click the **lock and key icon** in the System tray and choose **Launch PGPkeys**.The PGPKeys window displays the keys you have created for yourself plus any public keys you have added to your public keyring. A double set of keys represents the private and public key pairs you have created for yourself. Single keys represent the public keys you have obtained from others. RSA type keys are blue and DSS/Diffie-Hellman keys are gold.

2. Double click on any key icon to view the user ID and e-mail addresses. Double click on a figure icon to view the signatures of any users who have certified the key (as represented by the quill icon). You can also select several keys and choose the Expand Selection option from the Edit pull-down menu.

The captions at the top of the window correspond to the following attributes associated with each key:

Keys

Displays an icon representation of the key, plus the name and e-mail address of the owner.

Validity

This bar indicates the level of confidence that the key actually belongs to the purported owner. The validity is based on who has certified the key and how well you trust the signer to vouch for the authenticity of a key. The public keys you certify yourself have the highest level of validity, based on the assumption that you only sign someone's key if you are convinced it is valid. The validity of keys that you have not personally certified depends on the level of trust you have granted to any other users who have certified the key. If there are no certifications associated with the key, the key is not considered valid and a message indicating this fact displays whenever you use the key.

Trust

This bar indicates the level of trust you have granted to the owner of a key to serve as an introducer for the public keys of others. This trust comes into play when you are unable to verify the validity of someone's public key for yourself and instead choose to rely on the judgement of other users who have certified the key in the past. When you receive a public key that has been certified by some other key on your public keyring, the level of authenticity is based on the trust you have granted to the owner of that key. When you create a set of keys, they are considered implicitly trustworthy as represented by the striping in the trust and validity bars. Use the Properties dialog box to assign a level of trust (select complete, marginal, or untrustworthy) to someone's public key.

Creation

Shows the date a key was originally created. You can sometimes make assumptions about the validity of a key based on how long it has been in circulation. If a key has been in use for a while, it is less likely that someone will try to replace it since there are many other copies in circulation.

Size

Indicates the number of bits used to construct the key. Generally, the larger the key, the less chance it will be compromised. However, larger keys require more time to encrypt and decrypt data than smaller keys. When you create a DSS/Diffie-Hellman key, there is one number for the DSS portion and another number for the Diffie-Hellman portion.

Examining a Key's Properties

In addition to the general attributes shown in the PGPkeys window, you can also examine and change other key properties. To access the properties for a particular key, select and highlight the key, then select **Key Properties** from the **Keys** menu.

The Key Properties dialog box displays the following elements:

Key ID

A unique identifying number associated with each key. This number distinguishes between two keys with the same user name and e-mail address.

Created

Date the key was created.

Key Type

The key type - Either RSA or DSS/Diffie-Hellman.

Expires

The date the key expires. The owner specifies this date when a key is created. The value is usually set to never. However, if the owner only wants a key used for a limited period of time, the key can be set to expire on a specific date.

Trust Model

Indicates the validity of the key, based on its certification and the level of trust you have in the owner to vouch for the authenticity of someone else's public key. Set the trust level by sliding the bar to the appropriate level (complete, marginal, or untrustworthy).

Fingerprint

A unique identification number generated when the key is created. This is the primary means for checking the authenticity of a key. The optimum way to check a fingerprint is to have the owner read their fingerprint over the phone and then compare it to the fingerprint on your copy of their public key. You can also check the authenticity of someone's key by comparing the fingerprint on your copy to the one listed on a public key server, since it is assumed the owner periodically checks to make sure the fingerprint remains valid.

Enabled

Indicates whether or not the key is currently enabled. When a key is disabled, it is dimmed out in the PGPkeys window and is not be available for performing any PGP functions. However, the key remains on your keyring where it can later be enabled if necessary. To enable or disable a key, use this box, or select Enable or Disable from the **Keys** pull-down menu.

Change Passphrase

Allows you to change the passphrase for a private key. Some security experts suggest changing your passphrase on a regular basis, but this can cause problems for people who are prone to losing things like their secret passphrases. However, if you decide your passphrase is no longer a secret (perhaps you caught someone looking over your shoulder), select the Change Passpharase button to specify a new passphrase.

Specifying a Default Key Pair

Each time you create a set of keys, the keys are designated as your default keys and are automatically selected when you perform certain PGP functions. For instance, your default key pair is used when you sign a message or someone's public key. If you have more than one set of keys, you can designate one pair as your default set.

To specify your default key pair:

1. Select and highlight the set of keys you want designated as your default set.
2. Choose **Set As Default** from the **Keys** menu.

   Notice the selected keys are now bold faced, indicating they are your default keys.

Adding a New User Name or Address

You can have more than one user name or e-mail address for the same set of keys. After creating a new set of keys, you can add these alternate names and addresses.

To add a new user name or address to an existing key:

1. Select the key pair for which you want to add another user name or address.
2. Choose **New Key** from the **Keys** pull-down menu. The PGP New User Name dialog box appears. Enter the new name and address.
3. Click **OK**. The PGP Enter Passphrase dialog box appears.
4. Enter your passphrase, then click **OK**.

   The new name replaces the previous name, and if you expand the view you see that the old name has moved down a level.

Making a New Set of Keys

Unless you have already done so while using another version of PGP, the first thing you need to do before sending or receiving encrypted and certified e-mail is create a new key pair. A key pair consists of two keys: a private key that only you possess and a public key that you freely distribute to those with whom you correspond.

You generate a new key pair from the **PGPkeys** window using the **PGP Key Wizard** which guides you through the process.

PGP Key Wizard

Saving Your Public Key to a File

Another method of distributing your public key is to copy it to a file and then make this file available to the person with whom you want to communicate. There are several ways to copy your public key to a file:

- Select the icon representing your key pair from the PGPkeys window, then choose **Export** from the "Keys" menu and enter the name of the file where you want the key to be saved.
- Drag the icon representing your key pair from the PGPkeys window and drop it into the desired location in the Windows Explorer window.
- Select the icon representing your key pair in the PGPkeys window, choose **Copy** from the "Edit" menu and then choose **Paste** to insert the key information into a text document.

Including Your Public Key in an E-mail Message

Another convenient method of delivering your public key to someone is to include it along with your e-mail message.

1. Open the PGPkeys window by clicking on the lock and key icon in the Win95 tray, or click the **Start** button and choose **PGPkeys** from the PGP submenu of the Programs menu.
2. Select your key pair and then choose **Copy** from the "Edit" menu.
3. Open the editor you use to compose your e-mail messages, place the cursor in the desired area, and then choose **Paste** from the "Edit" menu. In some e-mail applications, you can simply drag your key from the PGPkeys window into the text of your e-mail message to transfer the key information.

   When you send someone your public key, be sure to sign the e-mail. That way, the recipient can verify your signature and be sure that no one has tampered with the information along the way.

Making Your Public Key Available Through a Server

Probably the best long-term and hassle-free method for making your public key available is to place it on a public key server where anyone can access it. By storing your public key on a key server, people can send you e-mail without having to explicitly request a copy of your key. It also relieves you and others from having to maintain a large number of public keys that you rarely use.

There are a number of key servers, such as those offered by PGP, Inc. where you can make your public key available for anyone to access. It doesn't really matter which key server you use to initially submit your public key, because once you submit your key to one server it is automatically propagated to all the other major servers in the world.

To Send your Public Key to a Key Server

1. Open the PGPkeys window by clicking on the lock and key icon in the Win95 tray, or click the **Start** button and choose **PGPkeys** from the **PGP** submenu of the **Programs** menu.
2. Select the icon that represents the public key you want to post on the key server.
3. Choose **Send Selected Keys** from the "Keyserver" submenu of the "Keys" menu. As an alternative, you can click the right mouse button and select this option from the pop-up menu.

After placing a copy of your public key on a key server, it will be available to any other PGP user who wants to send you encrypted mail or verify your digital signature. They can also get a copy of your key by accessing any PGP key server by searching for your name or e-mail address. Many people include the Web address for their public key in the footer of their of their e-mail messages; in many cases the recipient can just double-click the address to access a copy of your key on the server.

If you ever need to change your e-mail address or you acquire new signatures, all you have to do to replace you old key is send a new copy to the server and the information is automatically updated. If your key is ever compromised, you can revoke your key which tells the world to no longer trust that version of your key.

Adding Public Keys from E-mail Messages

One convenient way to get a copy of someone's public key is to have them include it when they send you encrypted e-mail. If you have an e-mail applications that is supported by the PGP plug-in, then adding the senders public key to your public key ring can be accomplished by simply clicking a button. For example, if you are using Eudora, and a mail message arrives with a block of text containing someone's public key, click the key and envelope button to have the key stored on your public keyring.

If you are using an e-mail application that is not supported by the plug-ins, you can copy the block of text that represents the public key and paste it into the PGPkeys window and thus add the key to your public keyring.

Import a Public Key from a File

Another method of obtaining someone's public key is to have them save it to a file from which you can import it or copy and paste it into your public keyring. There are several methods of extracting someone's public key and adding it to your public keyring.

- Choose **Import** from the "Keys" menu and then enter the name of the file where the public key is stored.
- Drag the file containing the public key from the Windows Explorer window onto the PGPkeys window.
- Open the text document where the public key is stored, select the block of text representing the key, then choose **Copy** from the "Edit" menu. Then, go to the PGPkeys window and choose **Paste** from the "Edit" menu to copy the key. The key will then show up as an icon in the PGPkeys window.

Getting Public Keys from a Public Key Server

If the person to whom you want to send encrypted mail is an experienced PGP user, chances are that they have placed a copy of their public key on a key server. This makes it very convenient for you to get a copy of their most up-to-date key whenever you want to send them mail and also relieves you from having to store a lot of keys on your public key ring.

There are a number of public key servers, such as the one maintained by PGP, Inc., where you can locate the keys of most PGP users. If the recipient has not pointed you to the Web address where their public key is stored, you can access any key server and do a search for the user's name or e-mail address, since all key servers are regularly updated to include the keys stored on all the other servers. In fact, when using PGP, you can quickly locate a specific user's key when you are sending e-mail or managing your keys from the PGPkeys window.

To Get Someone's Public Key from a Key Server

1. Open the PGPkeys window by clicking on the lock and key icon in the Win95 tray, or click the **Start** button and choose **PGPkeys** from the **PGP** submenu of the **Programs** menu.
2. Choose Find New Key from the "Keyserver" submenu of the "Keys" menu.
3. The "Find Key" dialog box appears.
4. Enter the e-mail address or user name to locate the users public key.
5. If a public key for the specified user is found, you are asked whether you want to add it to your public keyring. When you add a public key to your keyring, the keys will show up in the PGPkeys window where you can examine it to make sure that it is valid.

To Encrypt and Sign with Eudora

Here are the steps you should follow when you are sending encrypted and signed e-mail to those using a PGP/MIME compliant e-mail application:

To Encrypt and Sign with Eudora

1. Use Eudora to compose your e-mail message just as you normally would.
2. When you have finished composing the text of your e-mail message, specify whether you want to encrypt and sign the text of your message by clicking the lock and quill buttons.If you you are communicating with another PGP user who is using an e-mail application that adheres to the PGP/MIME standard, click on and depress the PGP/MIME button. When you click one of these buttons, they remain indented to indicate the operations you want to perform.
3. Send your e-mail message as you normally do. If you have elected to sign the encrypted data, the Passphrase dialog box appears requesting your passphrase before the mail is sent.
4. Enter your passphrase and then click **OK**. As long as you have a copy of the public keys for every one of the recipients, the appropriate keys are used. However, if you specify a recipient for whom there is no corresponding public key, the PGP Key Selection dialog box appears so you can specify the correct key.
5. Drag the public keys for those who are to receive a copy of the encrypted email message into the "Recipients" list box. You can also double-click on any of the keys to move them from one area of the screen to the other. The "Validity" bar indicates the minimum level of confidence that the public keys in the Recipient list are valid. This validity is based on the signatures associated with the key and the trust indicates how well you can rely on the owner of the key to vouch for the authenticity of another users key. (See chapter 5 for more details).
6. Click **OK** to send your mail.

   Note:

   If you are communicating with someone who is using an e-mail application that supports PGP/MIME, you can turn the PGP/MIME feature on from the Preferences dialog box. In this case, you do not have to click the PGP (do it) button to encrypt and sign your message or any file attachments. Instead, these operation are performed automatically when you send your e-mail

   If you are not using PGP/MIME, you must encrypt any files you want to send as attachments from the Windows Explorer before sending it.

To Encrypt and Sign with Exchange

Here are the steps you should follow to send encrypted and signed email from within the Exchange email application.

To Encrypt and Sign with Exchange

1. Use Exchange to compose your e-mail message just as you normally would.
2. When you have finished composing the text of your e-mail message, specify whether you want to encrypt and sign the text of your message by clicking the lock and quill buttons. When you click one of these buttons, they remain indented to indicate the operations you want to perform.
3. Send your e-mail message as you normally do. If you have elected to sign the encrypted data, the Passphrase dialog box appears requesting your passphrase before the mail is sent.
4. Enter your passphrase and then click **OK**. As long as you have a copy of the public keys for every one of the recipients, the appropriate keys are used. However, if you specify a recipient for whom there is no corresponding public key, the PGP Key Selection dialog box appears so you can specify the correct key.
5. Drag the public keys for those who are to receive a copy of the encrypted email message into the "Recipients" list box. You can also double-click on any of the keys to move them from one area of the screen to the other. The "Validity" bar indicates the minimum level of confidence that the public keys in the Recipient list are valid. This validity is based on the signatures associated with the key and the trust indicates how well you can rely on the owner of the key to vouch for the authenticity of another users key. (See chapter 5 for more details).
6. Click **OK** to send your mail.

   If you to send any encrypted and signed files as attachments, you need to encrypt and sign them from the Windows Explorer before sending them.

To Encrypt and Sign Without PGP/MIME

If you are using Eudora to send encrypted and signed e-mail to someone whom is not using an e-mail application that supports the PGP/MIME standard; here are the steps you should follow:

1. Use Eudora to compose your e-mail message just as you normally would.
2. When you are through composing the text of your e-mail message, select the **Message Plugins** menu option from the **Edit** menu and the select **PGP Encrypt & Sign**.
3. Send your message to the intended recipients. As long as you have a copy of the public keys for every one of the recipients, then the appropriate keys will be used. However, if you specify a recipient for whom there is no corresponding public key, the Recipients dialog box appears so you can specify the correct key.
4. If you have elected to sign the encrypted data, then the passphrase dialog box appears requesting your passphrase before the mail is sent.

   Note:

   If you want to include an encrypted attachment with your email message, you will need to encrypt the file from through the Windows Explorer before sending it.

To Encrypt and Sign Via the Clipboard

If you are using an e-mail application that is not yet supported by the PGP plug-ins (such as the one supplied with AOL), you must encrypt and sign your e-mail via the Windows clipboard. Essentially, you copy the contents of your message to the clipboard, encrypt and/or sign its contents, then paste it into your email editor before sending it. If you plan to attach any files with your message, you must encrypt them from the Windows Explorer before attaching them. Here is the procedure for encrypting and signing an e-mail message using the clipboard:

1. Use the editor supplied with your email application or your favorite word processing program to compose the message you want to send.
2. When you are ready to send the message, select the are of text you want to encrypt or choose **Select All** from the "Edit" menu available in most applications.
3. Choose **Copy** from the "Edit" menu to copy the contents of your message to the clipboard.
4. You should note that any time you copy or cut text in your application, it is temporarily stored on the clipboard.
5. Click the lock and key icon in the System tray and choose either **Encrypt Clipboard**, **Sign Clipboard** or **Encrypt/Sign Clipboard** depending on the operation you want to perform.
6. If you indicate that you want to encrypt the contents of the clipboard, the PGP Key Selection Dialog box appears:
7. Drag the public keys for those who are to receive a copy of the encrypted email message into the "Recipients" list box.
8. The "Validity" bar indicates the minimum level of confidence that the public keys in the Recipient list are valid. This validity is based on the signatures associated with the key and the trust indicates how well you can rely on the owner of the key to vouch for the authenticity of another users key. (See chapter 5 for more details)
9. Click **OK**.
10. If you elect to sign the message, the PGP Signing Passphrase dialog box appears requesting your personal passphrase for your default private key.
11. Enter your passphrase and then click **OK**.
12. Return to your email application and choose the **Paste** command from the "Edit" pull-down menu. This will copy the encrypted message back into your email application.
13. Send your email to the intended recipient(s).

To Encrypt and Sign from Windows Explorer

If you plan to send an encrypted file as an attachment with your e-mail message, or if you just want to encrypt a file to protect it on your own computer, you do so from the Windows File Explorer. Here are the steps you will follow when encrypting and/or signing a file from the Windows Explorer:

1. Open the Windows Explorer from the **Start** menu.
2. Select the file or files that you want to encrypt.
3. You can select multiple files but you must encrypt and sign each of them individually.
4. Choose the desired option from the “File” menu or from the pop-up menu, which you access by pressing the right mouse button.The “Key Selection Dialog” box appears in which you can select the recipient’s public keys for the file you are encrypting or signing. If you are adding your signature to the encrypted file and would like the signature stored in a separate file, select the “Separate Signature File” check box. If you want the output of the encrytped file saved in a text format that can be handled by all e-mail applications, select the **Text Out** checkbox. You should note that selecting this option increases the size of the file by about 30 percent.
5. Select the public keys by dragging them to the recipients list and then click **OK**. The “Save Encrypted File As”dialog box appears:
6. Specify the location and enter the name of the file where you want to save the encrypted version of the file. The.pgp extension is automatically appended to the file name unless you have turned on the ASCII Armor option in which case the.asc extension is used.
7. Click **Save** to save the file to the specified location.
8. If you look in the directory where you saved the file, you will find a file with the specified name represented by the PGP icon.

To Decrypt and Verify from within Eudora

If you are communicating with other PGP users, and they have encrypted and signed their mail using the PGP/MIME standard, a lock icon will appear when you open your e-mail.

In this case, you can decrypt and verify the message and any attached files by simply double-clicking this icon.

If you are receiving e-mail from someone who is not using a PGP/MIME-compliant e-mail application, you will decrypt the e-mail messages by clicking the choosing the appropriate menu option. If there are any encrypted file attachments, you will decrypt them from the Windows Explorer.

1. Open your e-mail message as you normally do.You will see a block of unintelligible ciphertext in the body of your e-mail message.
2. To decrypt and verify the contents of the e-mail message, click the open lock icon in your application's toolbar. The PGP Enter Passphrase dialog box appears requesting that you enter your passphrase.
3. Enter your passphrase and then click **OK**. The message is decrypted and, an if the message is signed, a message indicates whether it is valid.
4. At this point you can save the message in its decrypted state, or you can save the original encrypted version so that it remains secure.

To Decrypt and Verify from within Exchange

1. Open your e-mail message as you normally do.You will see a block of unintelligible ciphertext in the body of your e-mail message.
2. To decrypt and verify the contents of the e-mail message, click the open lock icon in your application's toolbar. The PGP Enter Passphrase dialog box appears requesting that you enter your passphrase.
3. Enter your passphrase and then click **OK**. The message is decrypted and, an if the message is signed, a message indicates whether it is valid.
4. At this point you can save the message in its decrypted state, or you can save the original encrypted version so that it remains secure.

To Decrypt and Verify With PGP/MIME

If you are communicating with other PGP users, and they have encrypted and signed their mail using the PGP/MIME standard, a lock icon will appear when you open your e-mail.

In this case, you can decrypt and verify the message and any attached files by simply double-clicking this icon.

If you are receiving e-mail from someone who is not using a PGP/MIME-compliant e-mail application, you will decrypt the e-mail messages by choosing the appropriate menu option. If there are any encrypted file attachments, you will decrypt them from the Windows Explorer.

To decrypt and verify from within Eudora

1. Open your e-mail message as you normally do.
2. You will see a block of unintelligible text in the body of your e-mail message.
3. Click on the open lock icon in your application's toolbar. You will be asked for your personal passphrase:
4. Enter your passphrase and then click **OK**.
5. The message and any attachments will be decrypted. If there are any signatures, an attempt is made to verify the signature and a message indicates whether the signature is valid or not.
6. At this point, you can save the message in its encrypted state, or you can save the original encrypted version so it remains secure.

To Decrypt and Verify Without PGP/MIME

If you are using Eudora to read mail sent by someone using an e-mail application that does not adhere to the PGP/MIME standard, then here are the steps you should follow:

1. Open your mail message as you normally do. You will see a block of unintelligible text:
2. To decrypt and verify the contents of the e-mail message, select the **Message Plugins>PGP Decrypt & Verify** option from the **Edit** menu.The passphrase dialog box appears requesting that you enter your passphrase.
3. Enter your passphrase and then click **OK**. The message and any attachments will be decrypted. If there are any signatures, an attempt is made to verify the signature and a message indicates that the signature is valid.

   At this point, you can save the message in its encrypted state, or you can save the original encrypted version so it remains secure.

To Decrypt and Verify Via the Clipboard

If your e-mail application is not supported by the PGP plug-ins, you must copy the contents of your message to the clipboard in order to decrypt it or to verify any digital signatures. If the e-mail contains file attachments, you decrypt and verify them through the Windows Explorer.

1. In the editor supplied with your email application, select the encrypted text and then copy it to the clipboard. In most applications, choose **Copy** from the “Edit” menu to copy the text to the Windows clipboard.

2. Using the right mouse button, click the lock and key icon in the System Tray to open the PGP pop-up menu. Choose **Decrypt/Verify Clipboard** to initiate the decryption and verification process.The PGP Enter Passphrase dialog box appears requesting that you enter your passphrase.

3. Enter your passphrase and then click **OK**. The message is decrypted. If there are any signatures, an attempt is made to verify the signature and a message appears indicating whether the signature is valid.

4. To view the contents of the deciphered email message, choose **Edit Clipboard Text** or **Launch Associated Viewer** from the PGP pop-up menu. You can then copy the contents back to your text editor and save it if you like.

To Decrypt and Verify from the Windows Explorer

If the email you receive has file attachments, you must decrypt them from the Windows Explorer.

1. Open the Windows Explorer from the **Start** menu.
2. Select the file or files that you want to decrypt and verify. You can select multiple files, but you must go through the process of decrypting and verifying each individual file.
3. Choose the **Decrypt/Verify** from the PGP submenu of the File menu or press the right mouse button to open the pop-up menu and then choose **Decrypt/Verify**. The “Save Encrypted File As”dialog box appears.
4. Specify the location and enter the name of the file where you want to save the decrypted version of the file. If you do not explicitly enter a name, then the original name is used.
5. Click the **Save** button to save the file. The passphrase dialog box appears requesting that you enter your passphrase.
6. Enter your passphrase and then click **OK**.

   The decrypted file is saved in the specified location. If there are any signatures, an attempt is made to verify the signature and a message appears indicating whether the signature is valid.

About Keys and Keyrings

PGP is based on a widely accepted and highly trusted "public key encryption" system by which you and other PGP users generate a key pair consisting of a private key and a public key. As its name implies, only you have access to your private key, but in order to correspond with other PGP users you need a copy of their public key and they need a copy of your public key. You use your private key to sign the e-mail messages and file attachments you send to others and to decrypt the messages and files they send to you. Conversely, you use the public keys of others to send them encrypted mail and to verify their digital signatures.

Your private key is also used to sign the contents of a given e-mail message or file attachment. Anyone who has a copy of your public key can check your digital signature to confirm that you are the originator of the mail and that the contents have not been altered in any way during transit. In the same way, if you want to verify somebody else's digital signature or check the integrity of the e-mail they send to you, then you need a copy of their public key to do so.

This version of PGP supports two distinct types of keys -- the traditional RSA key used in older versions of PGP and a new type of key called DSS/Diffie-Hellman which is based on the latest advancements in cryptographic technologies. If you plan to exchange e-mail with someone who has a newer version of PGP, you can take advantage of the new DSS/Diffie-Hellman keys. However, if you are corresponding with someone who is using a previous version of PGP, you will need to use the traditional RSA keys to communicate with them.

The keys you create as well as those you collect from others are stored on digital keyrings, which are essentially files stored on your hard drive or on a floppy disk. Normally your private keys are stored in a file named "secring.skr" and your public keys are stored in another file named "pubring.pkr". These files are usually located in the same program directory as the other PGP program files.

On occasion you may want to examine or change the attributes associated with your keys. For instance, when you obtain someone's public key, you might want to identify its type (either RSA or DSS/Diffie-Hellman), check its fingerprint, or determine its validity based on any digital signatures included with the key. You may also want to sign someone's public key to indicate that you believe it is valid, assign a level of trust to the key's owner or change a passphrase for your private key. You perform all of these key-management functions from the PGPkeys window.

Although the details of your private key are hidden, each public key has a set of attributes associated with it indicating its type (either RSA or DSS/Diffie-Hellman), the associated user name and e-mail address, when it was created and, if applicable, when the key expires. Keys often have digital certificates associated with them, which basically represent the signatures of those who have verified that the key does in fact belong to the person who allegedly generated it. For those keys you personally sign, the key is considered completely trustworthy while the trustworthiness of keys signed by others is based on the level of confidence you have granted to the signers.

PGP Preferences Dialog Box

Checking a Key's Fingerprint

It is often difficult be certain that a key belongs to a particular person unless that person physically hands their key to you on a floppy disk. Since this is not always possible, each key is associated with a unique fingerprint that can be used to verify that a key belongs to a specific person.

There are several ways to verify a fingerprint. The safest method is to call the person and have them read the fingerprint to you over the phone.

You can also verify a fingerprint by comparing your version to the version shown for the key on a public key server.

To check a key's fingerprint:

1. Select the key for the fingerprint you want to check.
2. Choose **Key Properties** from the **Keys** menu.
3. Compare the fingerprint to one you have received over the phone or from a public key server.

Signing Someone's Public Key

When you create a set of keys, they are automatically signed using your public key. Similarly, once you are sure that a key belongs to the proper individual, then you can sign their public key, indicating you are certain it is a valid key.

To sign someone's public key:

1. Select the key you want to sign.
2. Choose **Sign** from the **Keys** menu. The PGPkeys alert box appears.
3. Click **Yes** to indicate you are certain the key belongs to the purported owner.

   Notice that a quill icon associated with your user name is now included with the public key.

Granting Trust for Key Validations

In addition to certifying that a key belongs to a specific person, you can also assign a level of trust to the user of the keys, indicating how well you trust them to act as an introducer to others whose key you may get in the future. This means that if you get a key from someone that has been signed by an individual that you certified his or her key would be considered valid even though you have not done the check yourself.

To change the trust level for the owner of a particular key:

1. Select the key for which you want to change the trust level.
2. Choose **Key Properties** from the **Keys** menu. The Properties dialog box displays.
3. Use the **Trust Level** sliding bar to choose the appropriate level of trust for the key. You have a choice of **Untrusted**, **Marginal** or **Complete**.
4. Click **OK** to accept the new setting.

Disabling and Enabling Keys

You can temporarily disable a key so that it does not show up in your recipients' list. The ability to disable keys is useful when you want to retain a public key for future use, but don't want it included in your recipient list every time you send mail.

To disable a key:

1. Select and highlight the key you want to disable.
2. Choose **Disable** from the **Keys** menu.

   The key is dimmed and is temporarily unavailable for use.

To enable a key:

1. Select and highlight the key you want to enable.
2. Choose **Enable** from the **Keys** menu.

   The key is becomes visible and can be used as before.

Deleting a Key or Signature

If you no longer want to store a particular key on your keyring or you want to remove your signature from someone's public key, you can delete the key or the signature.

To delete an item from the PGPkeys window:

1. Select the key or signature you want to delete.
2. Choose **Delete** from the Edit menu.

Changing your Passphrase

To change your passphrase for a specific set of keys:

1. Select and highlight the key pair for which you want to change the passphrase.
2. Select **Key Properties** from the **Keys** menu. The Properties dialog box appears.
3. Click **Change Passphrase**. The Change Passphrase dialog box displays.
4. Enter your old passphrase in the top portion of the dialog box. Press **Tab** to advance to the next field.
5. Enter your new passphrase in the center dialog field and Press **Tab**.
6. Confirm your entry by re-entering your new passphrase.
7. Click **OK**.

Revoking Keys

If you can no longer trust your personal key pair, you can issue a revocation that tells everyone to stop using your public key. The best way to circulate a revoked key is to place it on a public key server.

To revoke your keys:

1. Select and highlight the key pair you want to revoke.
2. Choose **Revoke** from the **Keys** menu.
3. Enter your passphrase and click **OK**.

   A revoked key displays crossed out with a red line to indicate it is no longer valid.

In the event you lost or forgot your passphrase, you would not be able to use your key and you would have no way of invalidating your old key when you create a new one. To safeguard against this possibility, you can create a revocation key to be used in case you ever lose or forget your passphrase. To do so, make a copy of your key pair, revoking one copy, then putting the revoked key in a safe place. Be very careful where you store the revoked version of your key. If someone finds the revoked key, they can revoke your key and replace it with one of their own.

Protecting Your Keys

Once you have generated a key pair, it is wise to create a spare set and put them in a safe place just in case something happens to the originals. In fact, when you close the PGPkeys window after creating a new key pair, you are prompted to save a backup copy of your keys.

Both, your private key(s) and your public keys are stored in separate keyring files which you can copy just like any other files to another location on your hard drive or to an external floppy disk. By default, the private keyring (prv.pgp) and the public keyring (pub.pgp) are stored along with the other program files in the PGP file directory.

Besides making backup copies of your keys, you should be especially careful about where you store your private key. Even though your private key is protected by a passphrase that only you should know, it is possible that someone could discover your passphrase and then use your private key to decipher your e-mail or forge your digital signature. For instance, somebody could look over your shoulder and watch the keystrokes you enter or intercept them on the network or even over the airwaves.

To thwart anyone, who might happen to get hold of your passphrase from being able to use your private key, you should only store it on your own computer. You should also make sure that, if your computer is attached to a network, your files are not automatically included in a system wide backup where others might gain access to your private key. Given the ease with which your computer is accessible over today's networks, if you are working with extremely sensitive information, you may just want to keep your private key on a floppy disk. You can then insert this floppy like an old fashioned key whenever you want to read or sign your private mail.

As another security precaution, you might want to consider assigning a different name to your private keyring file and then storing it somewhere other than in the default PGP file directory where it will not be so easy to locate. You have the option of specifying which name to use for your private keyring and where it should be located through the PGPkeys main key dialog box.

Making a Backup Copy of Your Keys

When you specify that you want to save a backup copy of your keys, the **Select Backup Destination** dialog box appears where you specify the location to store a backup of your private keyring file.

Establishing PGP Preferences

While PGP is configured to accommodate the needs of most users, you have the option of adjusting some of the settings to suit your particular computing environment. You specify these settings through the PGP Preferences dialog box that you access by clicking the right mouse button on the key and lock icon and then selecting the **Preferences** menu option. You can also access the Preferences dialog box by selecting the **Preferences** option from the **Edit** pull-down menu.

General Preferences

Key Files Preferences

E-mail Preferences

Key Server Preferences

General Preferences

You specify general encryption settings from the General pane.

Always encrypt to default key

When this setting is selected, all the e-mail messages or file attachments you encrypt with a recipient's public key are also encrypted to you using your default public key. It is useful to leave this setting turned on so that you have the option of decrypting the contents of any e-mail you have previously sent.

Cache decryption passphrase for [] seconds

This setting specifies the amount of time (in seconds) that your encryption passphrase is stored in your computer's memory. If you regularly compose or read several e-mail messages in succession, you may want to increase the amount of time your passphrase is cached so you don't have to enter your passphrase over and over again to get through all of your mail. However, you should be aware that the longer your passphrase is stored in your computers memory, the more time a sophisticated snooper has to get hold of this highly compromising bit of information. By default, this setting is set to 120 seconds, which is probably sufficient to perform most of your PGP chores without having to enter your passphrase too many times, but not long enough for someone to determine your passphrase.

Cache signing passphrase for [] seconds

This setting specifies the amount of time (in seconds) that your signature passphrase is stored in your computer's memory. If you regularly compose or read several e-mail messages in succession, you may want to increase the amount of time your passphrase is cached so you don't have to enter your passphrase over and over again to get through all of your mail.

Show recipients when encrypting to marginally valid keys

This setting specifies that you should be warned whenever you are encrypting to a recipient for which the validity is only marginally established.

Faster key generation

When this setting is selected, it requires less time to generate a new DSS/Diffie-Hellman key pair. Using a precalculated set of prime numbers rather than going through the time-consuming process each time a new key is generated speeds up this process. Although it is extremely unlikely that anyone could ever crack your key based on their knowledge of these canned prime numbers, it may be prudent to spend the extra time to create a set of keys with the maximum level of security.

Key Files Preferences

Click the Key Files tab to advance to the pane where you specify the location of the keyrings used to store your private and public keys.

Public Key Ring File

The **Public Key Ring File** shows the current location and name of the file where the PGP program expects to find your Public keyring file. If you plan on storing your public keys in a file with a different name or in some other location, then you specify this information here. Some users like to keep their private keyring on a floppy and then only insert this disk when they need to sign or decrypt mail. You can use the browse button to search through your files rather than having to explicitly type in the path.

Private Key Ring File

The **Private Key Ring File** shows the current location and name of the file where the PGP program expects to find your Private keyring file. If you plan on storing your private keys in a file with a different name or in some other location, then you will need to specify this information here.

E-mail Preferences

Click the **Email** tab to advance to the pane where you specify preferences that affect the way PGP functions are implemented for your particular e-mail application.

Use PGP/MIME when sending email

When **Use PGP/MIME encryption** is checked, you do not have to go through the trouble of explicitly turning on the PGP/MIME feature every time you send out e-mail. For instance, if you are using Eudora, and you turn this setting on, all of your e-mail messages and file attachments will automatically be encrypted to the intended recipient. This setting has no effect on other encryptions you perform from the clipboard or for Windows Explorer and should not be used if you intend on sending e-mail to recipients who are not using e-mail applications that support the PGP/MIME standard.

Word wrap clear-signed messages at column [ ]

The **Word wrap clear-signed messages at column [ ]** setting allows you to specify the column number where a hard carriage return should be used to wrap the text in your digital signature to the next line. This feature is necessary since all applications do not handle word wrapping in the same way which could cause the lines in you digital signature to be broken up in a way that cannot be read properly. By default, this setting is set to 78, which prevents any problems with most applications.

Encrypt new messages by default

Leaves the encryption function turned on for your e-mail application. The lock icon will remain indented to indicate the encryption function is turned on.

Sign new messages by default

Leaves the signature function turned on for your e-mail application. The quill icon will remain indented to indicate the signatory function is turned on.

Key Server Preferences

Click the Key Server tab to advance to the pane where you specify settings for the key server you are using.

Server

Specifies the address for the public key server that is used by PGP to send and retrieve public keys. You should not change this unless you have a different location.

Port

The port address for the public key server.

Automatically Retrieve Unknown Keys

When this setting is selected, even unknown keys will be retrieved from the public key server.

Key Size

Key size ranges from 768-3072. The key size corresponds to the number of bits used to construct your digital key. The larger the key, the less chance someone will ever be able to crack it but the longer it will take to perform the decryption and encryption process. You will need to strike a balance between the convenience of performing PGP functions quickly with a smaller key and the increased level of security provided by a larger key. Unless you are exchanging extremely sensitive information which is of enough interest that someone would be willing to mount an expensive and time consuming cryptographic attack in order to read it, you are probably safe using a key composed of 1024 bits.

Passphrase

Your passphrase should contain multiple words and may include spaces, numbers, and other printable characters. Choose something that you can remember easily but that others will not be able to guess and keep in mind that the passphrase is case-sensitive. The longer your passphrase, and the wider variety of characters it contains, the more secure it is. Try to include equal numbers of upper and lower case alphabetic characters, numbers, punctuation marks and so on.

Hide Typing Check Box

Check this box if you do not want your passphrase to display on the screen when entered.

RSA or DSS/Diffie-Hellman

There are two distinct types of keys supported by this version of PGP. One is the traditional RSA key used in older versions of PGP and the other is a new type of key called DSS/Diffie-Hellman which are based on the latest advancements in cryptographic technologies.

- If you plan to correspond with individuals who are still using the older RSA keys, you will probably want to generate an RSA key pair that is compatible with older versions of the program.
- If you plan to correspond with individuals who have the latest version of PGP, you can take advantage of the new technology and generate a pair of DSS/Diffie-Hellman keys.
- If you want to be able to exchange e-mail with all PGP users, you should make a pair of RSA keys and a pair of DSS/Diffie-Hellman keys and then use the appropriate set depending on the public key used by the recipient.

Key Size

Key size ranges from 768-3072. The key size corresponds to the number of bits used to construct your digital key. The larger the key, the less chance someone will ever be able to crack it but the longer it will take to perform the decryption and encryption process. You will need to strike a balance between the convenience of performing PGP functions quickly with a smaller key and the increased level of security provided by a larger key. Unless you are exchanging extremely sensitive information which is of enough interest that someone would be willing to mount an expensive and time consuming cryptographic attack in order to read it, you are probably safe using a key composed of 1024 bits.

Note: When creating a DSS/Diffie-Hellman keys, the size of the DSS portion of the key is increased in fixed increments and is less than the size of the Diffie-Hellman portion of the key:
3072 Diffie-Hellman ----> 1024 DSS
3072-4095 Diffie-Hellman ----> 1536 DSS
4096 Diffie-Hellman ----> 2048 DSS

Passphrase

Your passphrase should contain multiple words and may include spaces, numbers, and other printable characters and must be at least eight characters. Choose something that you can remember easily but that others will not be able to guess and keep in mind that the passphrase is case-sensitive. The longer your passphrase, and the wider variety of characters it contains, the more secure it is. Try to include equal numbers of upper and lower case alphabetic characters, numbers, punctuation marks and so on.

Private Key

Only you have access to your private key. Your private key is also used to generate a unique digital signature based on the contents of a given e-mail message or file attachment.

Public Key

Anyone who has a copy of your public key can check your digital signature to confirm that you were the originator of the mail and that the contents have not been altered in any way during transit.

Opening the PGPkeys Window

By choosing the **Launch PGPkeys** option from the PGP pop-up menu, you open the PGPkeys window which shows the private and public key pairs you have created for yourself as well as any public keys you have added to your public keyring. (If you have not already created a new key pair, the PGP Key Wizard leads you through the steps necessary to create a new key pair.)

From the PGPkeys window you can create new key pairs and manage all of your other keys. For instance, this is where you examine the attributes associated with a particular key, specify how confident you are that the key actually belongs to the alleged owner, and indicate how well you trust that person to vouch for the authenticity of other user's keys.

The PGPkeys Window

Managing Keys

Selecting Recipients

When you send e-mail to someone whose e-mail application is supported by the PGP plug-ins, the recipient's email address determines which keys to use when encrypting the contents. However, if you enter a user name or e-mail address that does not correspond to any of the keys on your public keyring or if you are encrypting from the clipboard or the Windows Explorer, you must manually select the recipient's public key from the PGP Key Selection Dialog box.

To select a recipients public key:

Drag the icon representing their key into the Recipient's list box and then click OK.

Decrypt and Verify Data

Encrypt and Sign Data

PGP Key Wizard

To Create a New Key Pair

1. Click the **Start** button and choose **PGPkeys** from the PGP submenu of the Programs menu, or click the **lock and key icon** in the System tray and choose **Launch PGPkeys**. You can also open this window by clicking the double keys icon located in your e-mail application's toolbar.The PGPkeys window opens:
2. Choose **New Key** option from the **Keys** menu.The Key Generation Wizard provides some introductory information on the first screen.
3. When you are through reading this information, click **Next** to advance to the next dialog box.The Key Generation Wizard then asks you to enter your user name and e-mail address.
4. Enter your name on the first line and your e-mail address on the second line.
5. Click **Next** to advance to the next dialog box. The Key Generation Wizard then asks you to choose a key type.
6. Select a **key type** , either DSS/Diffie-Hellman or RSA.
7. Click **Next** to advance to the next dialog box. The Key Generation Wizard asks you to specify a size for your new keys.
8. Select a **key size** (from 768 to 3072) or enter any key size from (from 768 to 4096).
9. Click **Next** to advance to the next dialog box. The Key Generation Wizard asks you to indicate when the key pair should expire.
10. Indicate when you want your **keys to expire**. You can either go with the default selection, which is "never", or you can enter a specific number of days after which the keys will expire.
11. Click **Next** to advance to the next dialog box. The Key Generation Wizard asks you enter a passphrase.
12. In the "**Passphrase** " entry box, enter the string of characters or words you want to use to gain exclusive access to your private keys. To confirm your entry, press the Tab key to advance to the next line, then enter the same passphrase again. Normally, as an added level of security, the characters you enter for the passphrase do not appear on the screen. However, if you are sure that no one is watching over your shoulder, and you would like to see the characters of your passphrase as you type, clear the "Hide Typing" check box.
13. Click **Next** to begin the key generation process. The Key Generation Wizard indicates that it is busy generating your key. If you have entered an inadequate passphrase, a warning message appears before the keys are generated and you have the choice of accepting the bad passphrase or entering a more secure one before continuing. If there is not enough random information upon which to build the key, the PGP Random Data dialog box appears. As instructed on the screen, move your mouse around and enter a series of random keystrokes until the progress bar in the dialog box is completely filled in. Your mouse movements and keystrokes generate random information that is needed to generate a unique key pair. After the key generation process begins, it may take several minutes to generate the keys, as indicated by rotating hands on the clock. Eventually the clock will run down and the Key Generation Wizard indicates that the key generation process has completed.
14. Click **Next** to advance to the next dialog box. The Key Generation Wizard indicates that you have successfully generated a new key pair and that it is about to send your public key to the public key server.
15. Specify whether you want your new public key to be sent to the key server and click **Next**.

By sending your public key to the key server, anyone will be able to get a copy of your key when they need it.

When the Key Generation process completes a pair of keys representing your newly created keys appears in the PGPkeys window. You will notice that the older RSA keys are blue and the newer DSS/Diffie-Hellman keys are gold. At this point you can examine your keys by checking their properties and the values associated with them; you may also want to add other user names or e-mail addresses.

Adding a New User Name or Address

Examining a Key's Properties

Key Selection Dialog Box

You use the Key Selection dialog box to select the recipients for the encrypted data. When you send e-mail to someone with an e-mail application that is supported by the plug-ins, the recipient's email address determines which keys to use when encrypting the contents. However, if you enter a user name or e-mail address that does not correspond to any of the keys on your public keyring, you must manually select the recipient's public key. You must also use the choose your recipients in this way whenever you encrypt data from the clipboard or from the Windows Explorer.

All you need do to select a recipients public key is to drag the icon representing their key into the Recipient's list box and then click **OK**.

If you are encrypting from the Windows Explorer, you have the option of encrypting the contents of the file as text which makes it easier for others do decrypt the file regardless of which application they are using. You also have the option of saving the signature in a separate file if you have elected to both encrypt and sign the file.

Contacting Technical Support

Before contacting Support, please review the following information and follow the appropriate instructions. All support calls will be returned within 8 business hours of the initial call. Business hours are from 8 AM to 5 PM (Pacific time), excluding National holidays. Address changes can be mailed or e-mailed to Customer Service using the information.

E-Mail: pgpsupport@PGP.com

Phone: 503.684.3140

Web: http://www.pgp.com/service/service.cgi

Mail: PGP Inc, 2121 South El Camino Real, San Mateo, CA 94403

If you are the end user of an PGP product that you did not purchase directly from PGP and you need technical assistance, please contact the provider of the software or hardware that included PGP software. If you are part of an enterprise network, please contact your network administrator or Information Services tech support group.

Technical Support Preparation

To ensure quick resolution, please have the following information ready before calling Support.

- PGP product and version
- Computer type, CPU type, clock speed, and bus type
- Network operating system and version
- Content of status or error message displayed on screen
- E-mail application and version