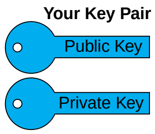
Overview

The PGPmail™ program performs fast, high-security, public-key *encrypting* (with optional compression), *decrypting*, and *authenticating* of electronic messages and files. The program can be used with most popular email, word processing, and spreadsheet programs to exchange secure information with colleagues who also use the PGPmail program, or any PGP program version 2.4 or later. It can also be used to secure files on your local computer or network server.

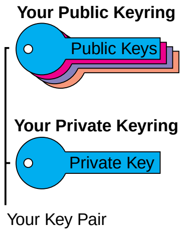
The program comes in two versions, both packaged together: A 32-bit version for Windows® 95 or Windows NT 4.x, and a 16-bit version for Windows 3.1x. The 32-bit version also ships with *email plug-ins* for seamless integration into the Netscape Navigator™ 3.0 and Eudora Pro™ 3.0 (or later) email programs. The PGP Web site will offer additional plug-ins and updates as they become available.

The PGPmail program maintains privacy and assures authentication. *Privacy* means that only recipients intended to read a message can actually read it. *Authentication* means that messages appearing to be from a particular person can only have originated from that person. The program is also convenient to use; its Rivest-Shamir-Adleman (RSA) public-key cryptographic technology lets you exchange secure information *without* the need for secure communication channels.

Keys



In public-key cryptosystems, like the PGPmail program, each communicating colleague maintains a pair of complimentary digital *keys*: a *Public Key* and a *Private Key*. Each key in the pair unlocks the code that the other key makes. Knowing a colleague's public key does not help anyone discover the corresponding private key. Your public key can be widely disseminated to colleagues or strangers. Your private key should be kept secret, known only to you. You only need one key pair, but you can have more.

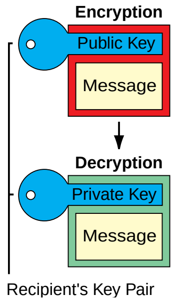


Your public keys—your own and your colleagues'—are stored in a *Public Keyring* file. Your private key is stored in a *Private Keyring* file.

Each key pair has a *User ID* (such as the owner's name and email address) so that you and your colleagues can identify the owners of keys. Each private key also has a *Pass Phrase* that protects it, like a password.

After installation, the first thing to do is generate a key pair for yourself. Then, you send your public key to the colleagues with whom you want to exchange secure information. They do the same: they generate their own key pair and send you their public key.

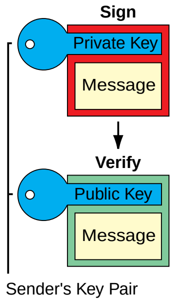
Encryption and Decryption



To send a secure message, you encrypt it using a copy of the recipient's public key. The message can be sent over any type of communication channel; no security is needed in the channel itself. The recipient decrypts the message using his or her private key. Since the recipient is the only person who has that private key, he or she is the only person who can decrypt the message.

Encrypting a message scrambles it in a complicated way, rendering it unreadable to anyone except the intended recipient. Before encrypting the message, the PGPmail program optionally compresses it using the ZIP algorithm, if the message is not already compressed. Compression saves modem transmission time and disk space, and it strengthens the cryptographic security of the encryption.

Signing and Verifying Signatures



Keys are also used to digitally *sign* a message or file and to *verify* a signature. When you sign a message, the PGPmail program uses your private key to create a digital signature that is unique to both the contents of the message and your private key. Anyone can use your public key to verify your signature.

Signatures allow *authentication* of messages. Verifying a signature proves that the message was actually sent by the signer, and that the message has not been subsequently altered by anyone else. The signer, alone, possesses the private key that created that signature. Forgery of a signed message is computationally infeasible.

Summary of Key Usage

The table below summarizes the functions for which public and private keys are used when sending and receiving messages. When keys are used to secure files stored on your computer or local network server, you are both the "sender" (the person who saves the file) and the "recipient" (the person who opens the file).

	Recipient's		Sender's	
	Private Key	Public Key	Private Key	Public Key
Sender ***Encrypts*** with:		**X**		
Sender ***Signs*** with:			**X**	
Recipient ***Decrypts*** with:	**X**			
Recipient ***Verifies Signature*** with:				**X**

Setup

Installing The Software

1. **Start Windows.**
2. **Insert Disk #1 into your floppy drive.**
3. **Run the *Setup* program.**
   - *Windows 95 or Windows NT:* In the Taskbar, select *Start>Run*, and enter **a:setup**.
   - *Windows 3.1:* In the Program Manager, select *File>Run* and enter **a:setup**.

Setup.exe

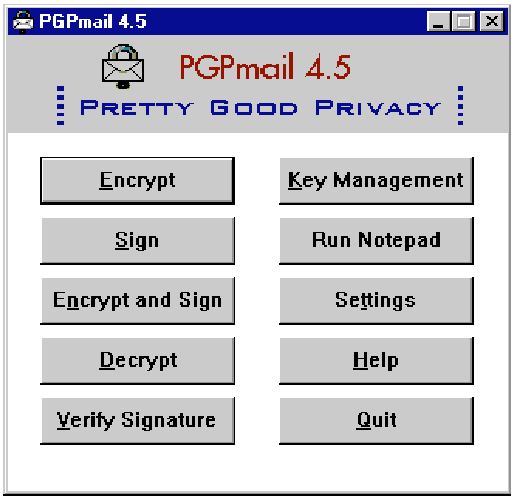
4. **Follow the On-Screen Prompts.**

   This procedure installs the PGPmail program, the Enclyptor toolbar, and (optionally) the plug-ins for Netscape Navigator™ (3.0 or later) and Eudora Pro™ (3.0 or later). If you answer *"Yes"* to *"Add the Enclyptor to your Windows StartUp folder?"* the toolbar will appear on your desktop whenever you start your computer.

Running the Program

- *Windows 95 or Windows NT:* In the Taskbar, select *Start>Programs>***PGPmail**.
- *Windows 3.1:* In the Program Manager, double-click the **PGPmail** icon.

The Main Menu appears:

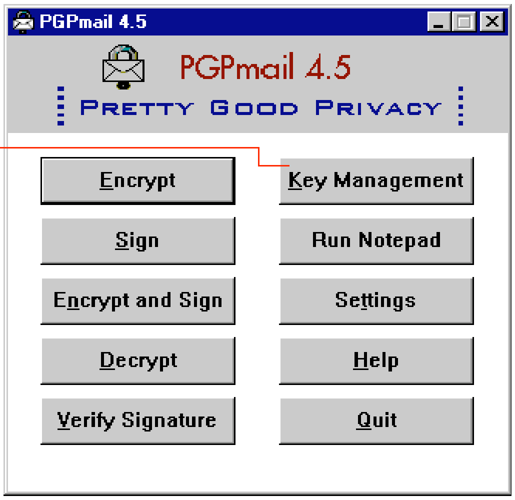


Generating A Key Pair

The first thing to do is generate your own public and private keys (i.e., your *key pair*). You need only one pair, but you can generate additional pairs if you wish.

To Generate A Key Pair:

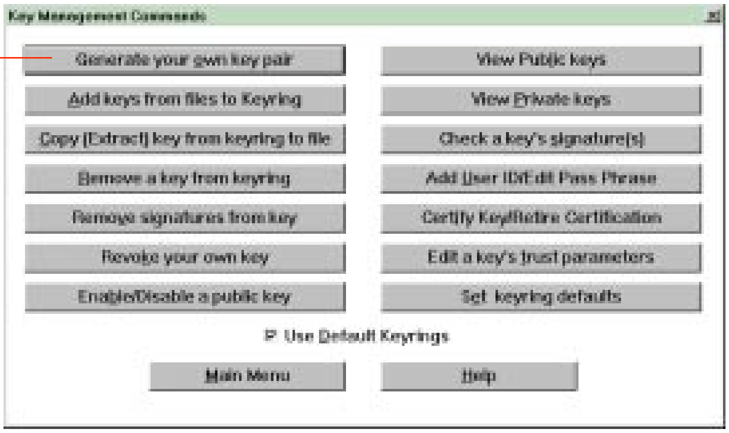
1. **Click the *Key Management* Button on the Main Menu.**



Key Management

The *Key Management Commands* menu appears.

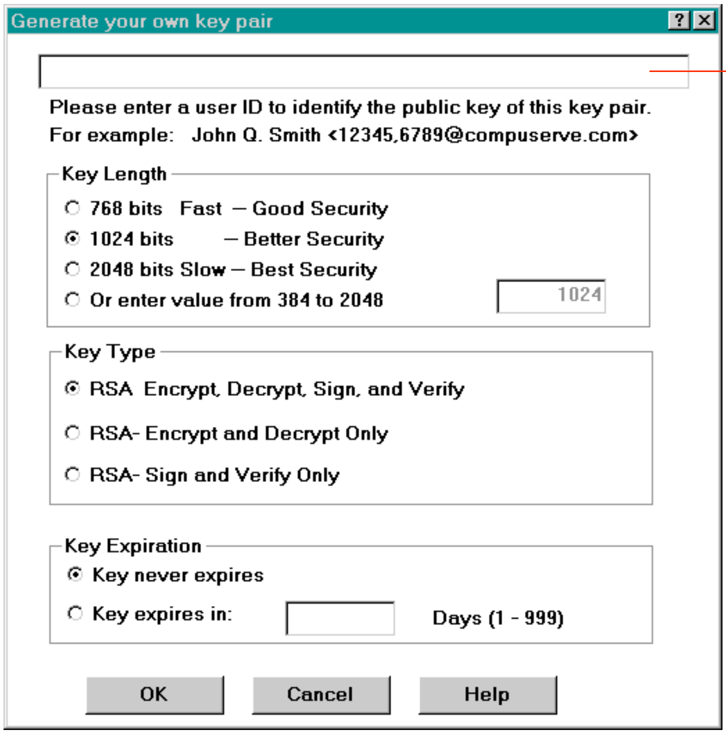
2. **Click the *Generate your own key pair* Button.**


Key Management Commands
Generate your own key pair
View Public keys
Add keys from files to Keyring
View Private keys
Copy (Extract) key from keyring to file
Check a key's signature(s)
Remove a key from keyring
Add User ID/Edit Pass Phrase
Remove signatures from key
Certify Key/Retire Certification
Revoke your own key
Edit a key's trust parameters
Enable/Disable a public key
Set keyring defaults
☑ Use Default Keyrings
Main Menu
Help

Generate your own key pair

The *Generate your own key pair* dialog box appears.

3. **Enter a *User ID* and (optionally) Key Type and Expiration.**



Generate your own key pair

Please enter a user ID to identify the public key of this key pair.
For example: John Q. Smith <12345,6789@compuserve.com>

Key Length

○ 768 bits Fast — Good Security
● 1024 bits — Better Security
○ 2048 bits Slow — Best Security
○ Or enter value from 384 to 2048 1024

Key Type

● RSA Encrypt, Decrypt, Sign, and Verify
○ RSA- Encrypt and Decrypt Only
○ RSA- Sign and Verify Only

Key Expiration

● Key never expires
○ Key expires in: Days (1 - 999)

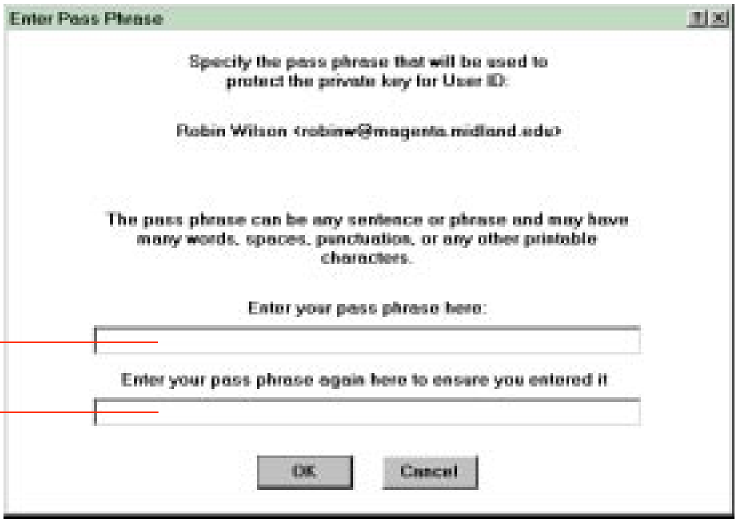
Enter User ID

Enter a *User ID* for the key-pair in the top field. For example, enter your full name and email address so that colleagues can easily identify your public key. Blank spaces and punctuation characters are allowed.

The other fields on the form can be left at their default values, although the accompanying *Reference Manual* explains these values if you want to modify them.

Click the **OK** button. The *Enter Pass Phrase* dialog box appears.

4. **Enter a Pass Phrase.**



Enter Pass Phrase

Specify the pass phrase that will be used to protect the private key for User ID:

Robin Wilson <robinw@magenta.midland.edu>

The pass phrase can be any sentence or phrase and may have many words, spaces, punctuation, or any other printable characters.

Enter your pass phrase here:

Enter your pass phrase again here to ensure you entered it

Enter Pass Phrase

Repeat Pass Phrase

Enter the phrase in the upper field (it will not be visible), then repeat it in the lower field. The phrase is case-sensitive; blank spaces and punctuation characters are allowed.

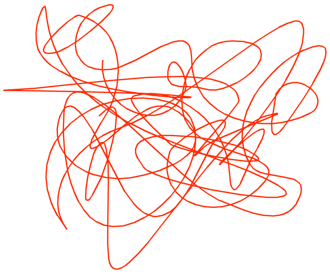
A *Pass Phrase* works like a password. It protects the privacy of your private key. If you generate more than one key pair, you can use the same or different Pass Phrases for each.

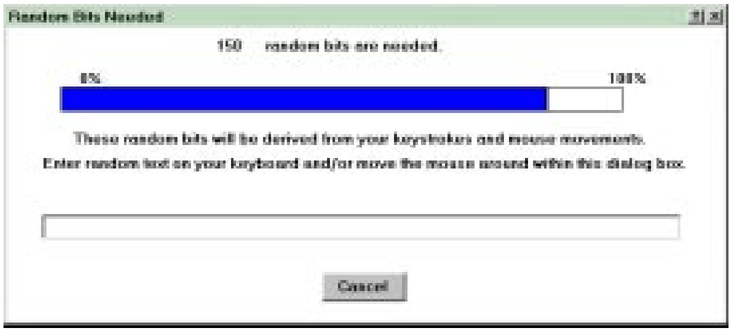
You will be asked to enter the Pass Phrase whenever you decrypt or sign a message or file. *Keep the phrase secret, and don't lose it!* There is no way to recover it if you lose it, and you will no longer be able to decrypt or sign messages except by generating a new key pair and distributing the public key to your colleagues again.

Click the **OK** button. The *Random Bits Needed* dialog box appears.

5. **Move Your Mouse Randomly and Press Some Keys.**

Move Your Mouse Randomly





Random Bits Needed

150 random bits are needed.

These random bits will be derived from your keystrokes and mouse movements.
Enter random text on your keyboard and/or move the mouse around within this dialog box.