University of Pittsburgh
Computing Services and Systems Development
Pittsburgh, PA 15260
(412) 624-HELP [4357]

Date: July 2000
File name: pgp
Document #: 0700Rev1

Sending Secure Messages with Mulberry 2.0.3 for Windows

Acquiring PGP

Pretty Good Privacy® (PGP) is a program that encrypts e-mail messages so that only the recipient is able to read them. It also allows you to secure and encrypt files that you have stored on your computer.

PGP is available on the Student Toolkit CD, which can be obtained through Software Licensing Services. University of Pittsburgh students, faculty and staff can also download a freeware version of PGP through MIT's Distribution Center for PGP located at **http://web.mit.edu/network/pgp.html**.

Installing PGP

If you are installing PGP from the Student Toolkit CD:

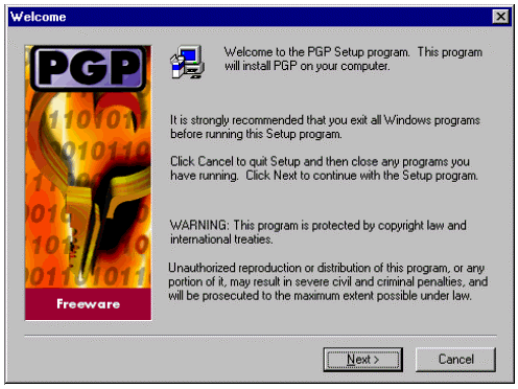
1. Click the **Software** tab.
2. Select **Utilities**.
3. Click **Pretty Good Privacy**.

If you are downloading PGP from MIT's site:

1. Go to **http://web.mit.edu/network/pgp.html**.
2. Click the **Download** link for Windows 95/98/NT/2000 to download the PGP zip file.
3. Use a program such as WinZip to unzip the file.

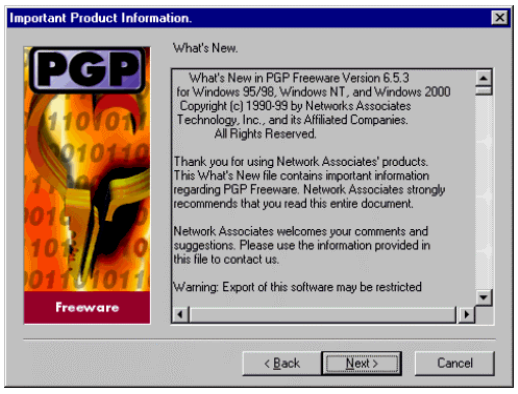
Once you have downloaded PGP, double-click the **PGPfreeware_653.exe** icon from the folder where you unzipped it. The PGP setup wizard begins.

a.) The **Welcome** window appears. Click **Next.**



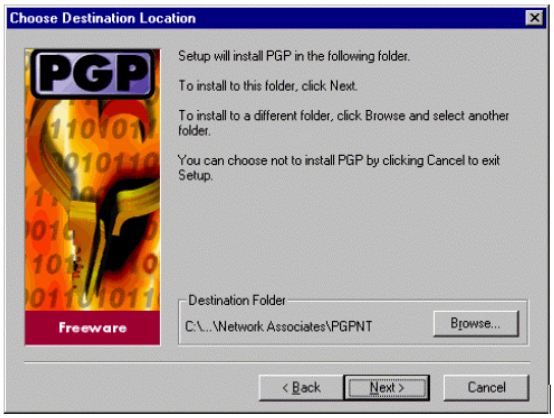
b.) The **Software License Agreement** window appears. Read it carefully and click **Yes.** Clicking **No** will cancel the setup process.

c.) The **Important Product Information** window appears. Read it and click **Yes** to continue.

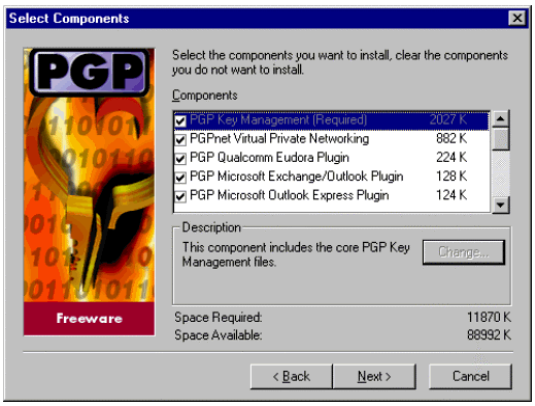


d.) The **User Information** window appears. Enter your name in the **Name:** text box and enter your company or University in the **Company:** text box. Click Next.

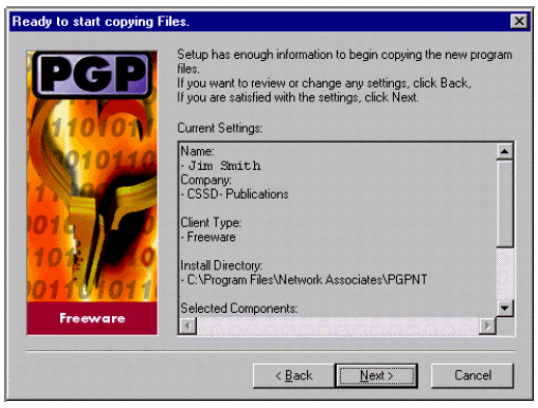
e.) The **Choose Destination Location** box appears. Click **Next** to choose the default location, or you can press the **Browse** button to specify a different location.



f.) The **Select Components** window appears. Click **Next** to accept the default components, or you can specify which components you want installed.

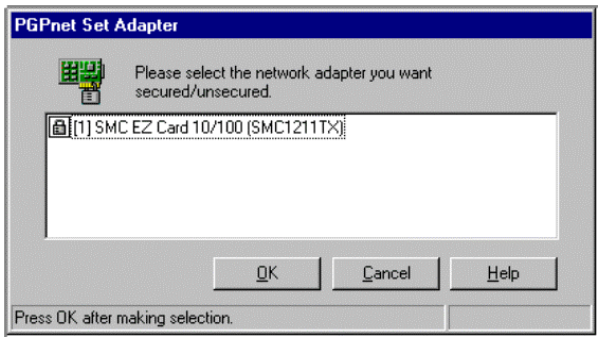


g.) The **Ready to Start Copying Files** window appears. Click **Next** to start the setup process.



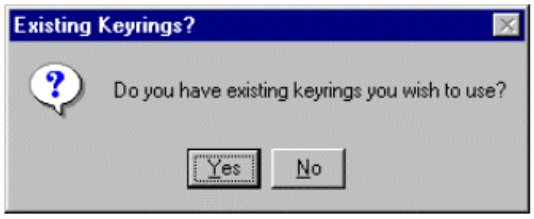
4. Once the setup begins, the **PGPnet Set Adapter** window appears.

h.) Select the network adapter to be secured. A padlock icon appears in the box next to the selected adapter.



i.) Press **OK** . The Binding Configuration process begins and will take a few moments.

j.) The **Existing Keyrings** window appears. Click **Yes** and the **Browse to Your Public Keyring** window appears. Select a file and click **Open**. Click **No** and PGP will setup the default keyrings.



k.) The **Setup Complete** window appears. You must restart your computer in order to start using PGP. Select **Yes, I want to restart my computer now** and click **Finish.** If you choose to restart your computer at a later time, make sure the box is not checked and click **Finish.**

Using Keys

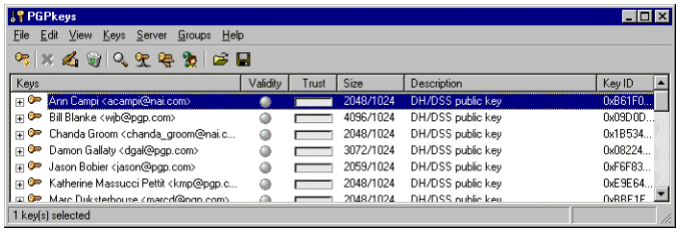
In order to start encrypting and decrypting messages, you must set up a key pair, which is made up of a public and a private key. By making your public key available, people can send you encrypted messages. Your private key is used to decrypt the messages.

Note: Encrypted messages cannot be sent or decrypted unless you have exchanged keys with the people that you will be communicating with through e-mail.

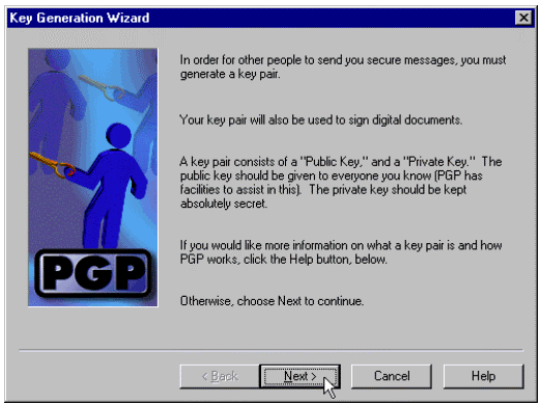
To set up a key pair:

1. Press the **Start** button on the taskbar and select **Programs, PGP**.

2. Select **PGPkeys**. The **PGPkeys** window appears.



3. Select **New Key** from the **Keys** menu. The **Key Generation Wizard** appears.



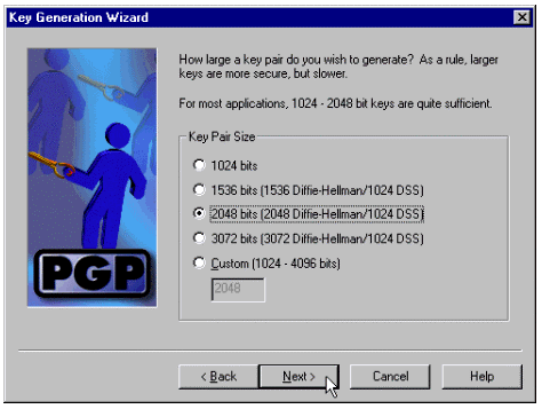
4. Read the information and click **Next**.

5. In the second window, enter the name you would like associated with the key in the **Full Name:** text box.

6. Enter the e-mail address that is to be used with the key in the **Email address:** text box and click **Next**.

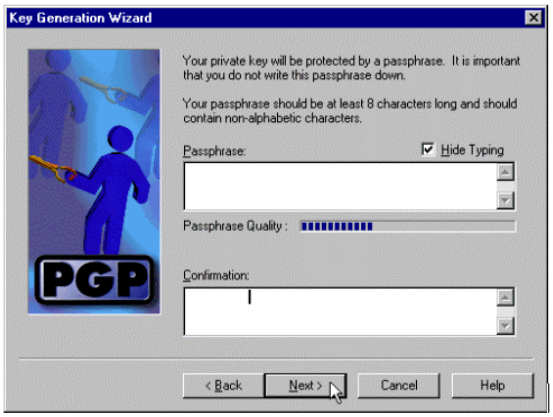
7. In the third window, read the information and select the type of key pair you want. The window explains that if you don't know which type to use, it is recommended you choose **Diffie-Hellman/DSS**. Click **Next**.

8. In the fourth window, select a size for your key pair. Larger keys are slower, but more secure. It is recommended that you use the default size of 2048 bits. Click **Next**.



9. In the fifth window, choose an expiration date. You can select **Key pair never expires**, or select **Key pair expires on** and enter your own date. Click **Next**.

10. The sixth window requires that you enter a password. This will be used when you decrypt your e-mail. Enter a password in the **Passphrase:** text box and re-enter it in the **Confirmation:** box. Click **Next**.



11. Your key pair will be generated and the Wizard lets you know when the process is complete. Click **Next**.

12. You must send your key pair to the root server before you can start encrypting messages. Click **Send my key to the root server now** to have it sent, or you can send it at a later time. Click **Next**.

13. Click **Finish** to end the Wizard.

Exchanging Keys

You can exchange keys with others in three ways:

1. Make keys available through a public certificate server

   Note: If you selected **Send my key to the root server now** in the last window of the **Key Generation Wizard**, then you do not have to resend it. Your key will already be available through a public certificate server.

2. Send keys through e-mail

3. Import and Export keys

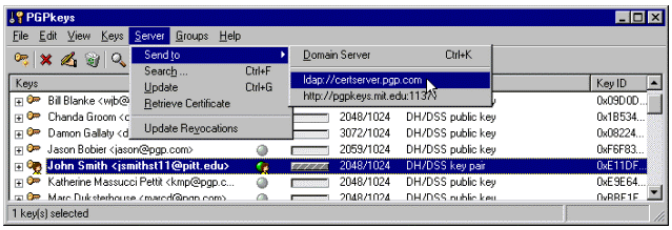
Making your key available through a public certificate server:

1. Press the **Start** button on the taskbar and select **Programs, PGP**.

2. Select **PGPkeys**.

3. Select your key pair by highlighting the name that you entered in the **Key Generation Wizard**.

4. Select **Send To** from the **Server** menu and choose the desired server.



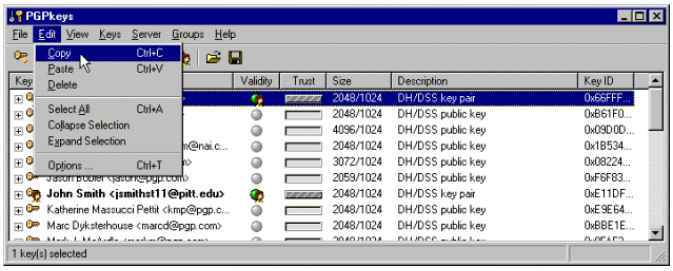
Sending keys through e-mail:

1. Press the **Start** button on the taskbar and select **Programs, PGP**.

2. Select **PGPkeys**.

3. Select your key pair by highlighting the name that you entered in the **Key Generation Wizard**.

4. Choose **Copy** from the **Edit** menu.

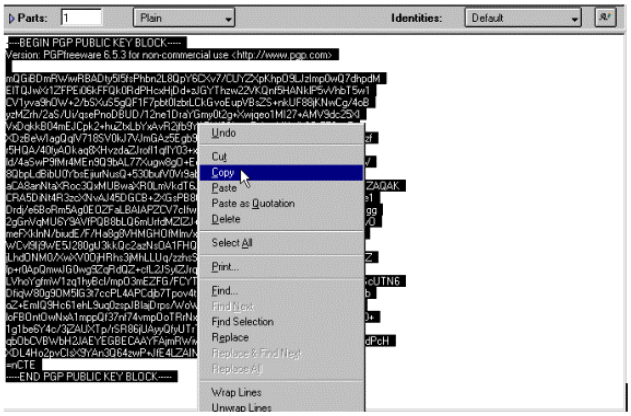


5. Paste the text into an e-mail message and send it.

Importing and Exporting Keys:

If you receive a key in an e-mail message, you can import the key to your public keyring.

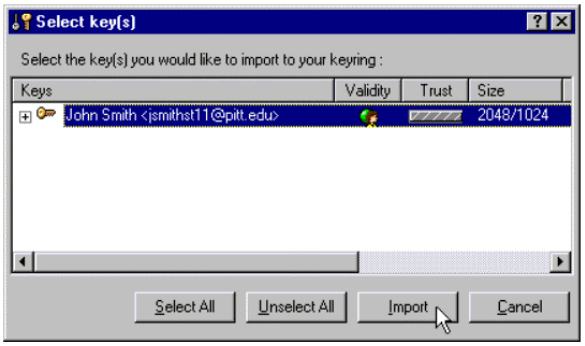
1. Select the text block which represents the key and choose **Copy** from the **Edit** menu, or right-click on the text and select **Copy**.



2. Press the **Start** button on the taskbar and select **Programs, PGP**.

3. Select **PGPkeys**.

4. Choose **Paste** from the **Edit** menu. The **Select Keys** dialog box appears.



5. Select the key you want to import and click the **Import** button.

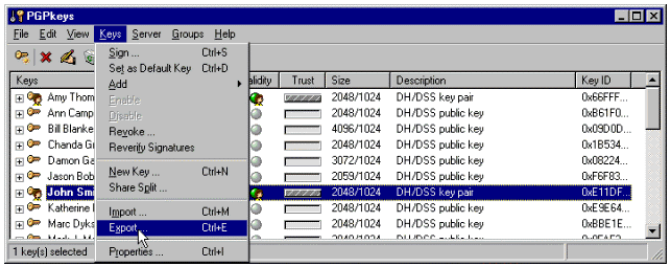
There are three ways to export your key pair.

1. To export your key pair using the **Keys** menu:
   a.) Press the **Start** button on the taskbar and select **Programs, PGP**.

   b.) Select **PGPkeys**.

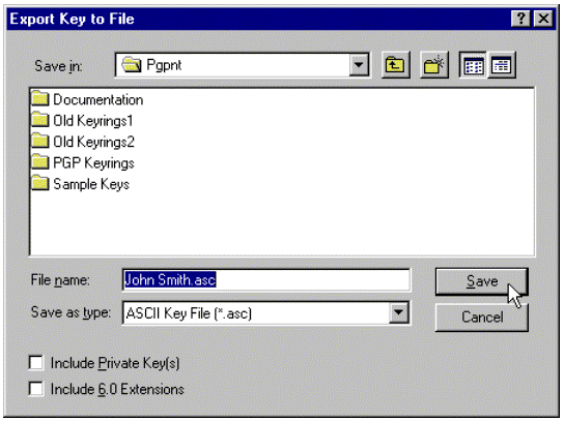
   c.) Select your key pair by highlighting the name that you entered in the **Key Generation Wizard**.

   d.) Click the **Keys** menu and choose **Export**.



   e.) Select the folder where you would like to save your key pair.

   f.) Enter a file name in the **Export Key to File** window and click **Save**.



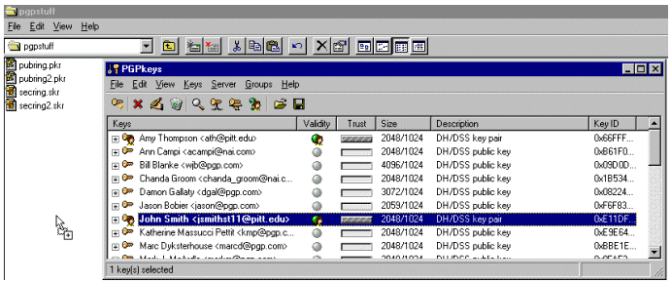
2. To export your key pair using **Drag and Drop**:
   a.) Double-click **My Computer** and select the folder where you would like to save your key pair.

   b.) Press the **Start** button on the taskbar and select **Programs, PGP**.

   c.) Select **PGPkeys**.

   d.) Select your key pair by highlighting the name that you entered in the **Key Generation Wizard**.

   e.) Hold down the mouse button and drag your key pair to the folder that you selected in **My Computer**. Release the mouse button.



3. To export your key pair using **Copy and Paste**:
   a.) Press the **Start** button on the taskbar and select **Programs, PGP**.

   b.) Select **PGPkeys**.

   c.) Select your key pair by highlighting the name that you entered in the **Key Generation Wizard**.

   d.) Choose **Copy** from the **Edit** menu.

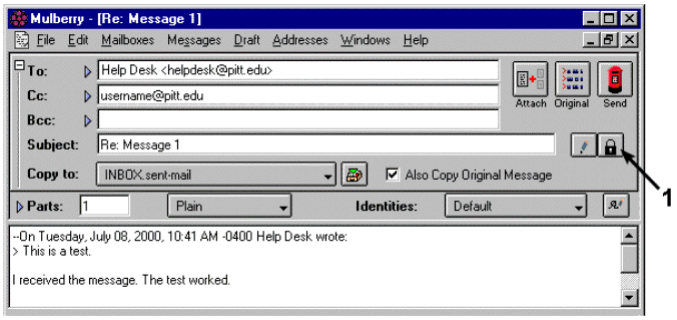
   e.) Paste the text into an e-mail message and send it.

Once you have installed PGP and exchanged keys with others, you can begin encrypting your e-mail messages.

To encrypt an e-mail message using Mulberry:

1. Select **File, New Messages** to compose a new e-mail message, or you can reply to a message.

2. Select the small padlock icon **(1)** to encrypt the message.

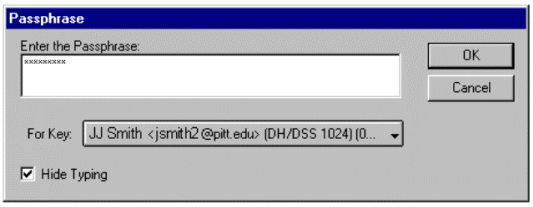


3. Click **Send.**

Note: You will not see the encrypted message on your screen. It is not encrypted until it is sent.

To decrypt an e-mail message using Mulberry:

1. Open the message. The **Passphrase:** window appears.



2. Enter the password you selected using the **Key Generation Wizard** and click **OK**.

Getting Help

Contact the **Help Desk** if you have any questions about installing this program or any other computing-related issue. The Help Desk can be reached by phone at (412) 624-HELP [4357] or via the Web at **http://technology.pitt.edu**. The Help Desk is available 24 hours a day, seven days a week.

Additional information on obtaining and installing Mulberry 2.0.3 is available at **http://technology.pitt.edu.**