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

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

Sending Secure Messages with Mulberry 2.0.3 for Macintosh

Acquiring PGP

Pretty Good Privacy® (PGP) is a program that encrypts e-mail messages so that only the recipient is able to read them. PGP 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:

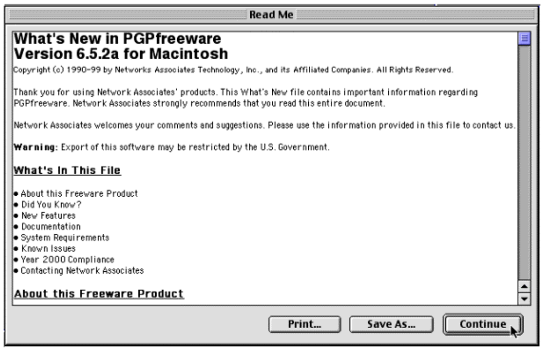
1. Go to **http://web.mit.edu/network/pgp.html**.
2. Click the **Download** link for Mac OS to download the PGP zip file.
3. Use Stuffit Expander to expand the program. This application is usually found in your Web browser's program folder.

Once you have downloaded PGP, double-click the **PGP 6.5.2a** icon from the folder where you expanded it. The PGP setup wizard begins.

PGP 6.5.2a

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

b.) The **ReadMe** window appears. Read it and click **Yes** to continue.



Read Me

What's New in PGPfreeware
Version 6.5.2a for Macintosh

Copyright (c) 1990-99 by Networks Associates Technology, Inc., and its Affiliated Companies. All Rights Reserved.

Thank you for using Network Associates' products. This What's New file contains important information regarding PGPfreeware. Network Associates strongly recommends that you read this entire document.

Network Associates welcomes your comments and suggestions. Please use the information provided in this file to contact us.

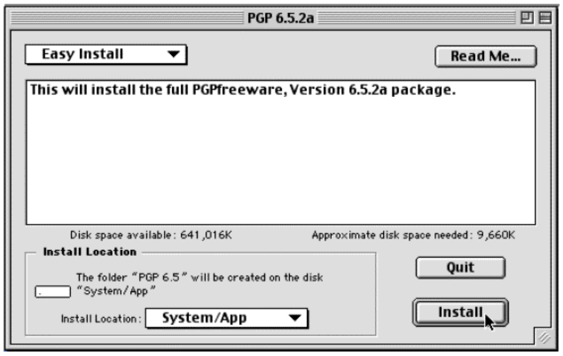
Warning: Export of this software may be restricted by the U.S. Government.

What's In This File

- About this Freeware Product
- Did You Know?
- New Features
- Documentation
- System Requirements
- Known Issues
- Year 2000 Compliance
- Contacting Network Associates

About this Freeware Product

c.) The **PGP 6.5.2a** installation window appears. Click **Install**.



PGP 6.5.2a

Easy Install

This will install the full PGPfreeware, Version 6.5.2a package.

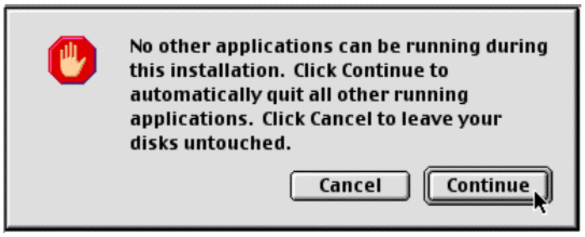
Disk space available: 641,016K
Approximate disk space needed: 9,660K

Install Location

The folder "PGP 6.5" will be created on the disk "System/App"

Install Location: System/App

d.) A warning window appears to let you know that no other applications can be running during PGP installation. Click **Continue**. The installation process begins and will take a few moments.



No other applications can be running during this installation. Click Continue to automatically quit all other running applications. Click Cancel to leave your disks untouched.

e.) If the installation was successful, a window appears, prompting you to restart your computer. Click **Restart.**

Using Keys

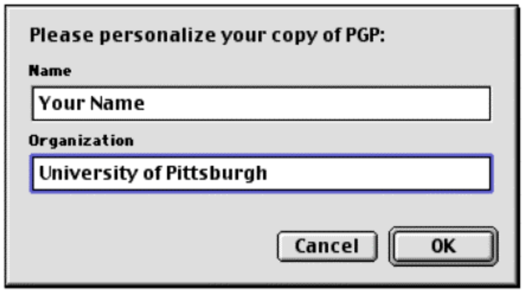
In order to start encrypting and decrypting messages, you must set up a key pair, which is made up of a public and a private key. By making your public key available, people can send you encrypted messages. Your private key is used to decrypt the messages.

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. Open the PGP 6.5 folder from the location where you installed it.

2. Double-click **PGPkeys.** If you don't have any key files, you are prompted to personalize your copy of PGP.



Please personalize your copy of PGP:

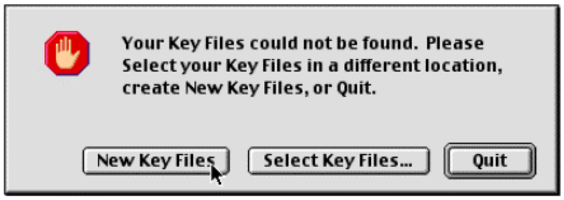
Name

Your Name

Organization

University of Pittsburgh

a.) Enter your name and organization. Click **OK**.
b.) Select **New Key Files**.

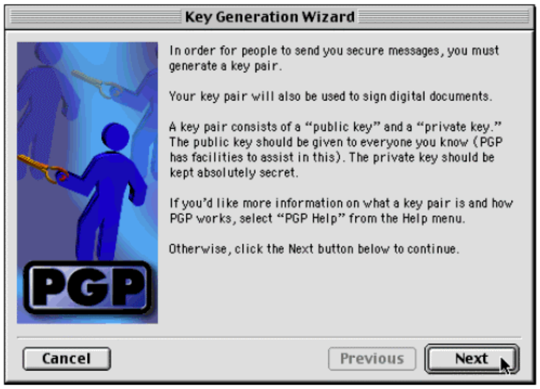


Your Key Files could not be found. Please Select your Key Files in a different location, create New Key Files, or Quit.

If you do not get a window prompting you to personalize PGP, the **PGPkeys** window will appear.

Note: You may want to make an alias for your PGPkeys if you are going to send encrypted messages to many people. Choose **File, Make Alias** and drag the alias to your desktop.

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



Key Generation Wizard

In order for people to send you secure messages, you must generate a key pair.

Your key pair will also be used to sign digital documents.

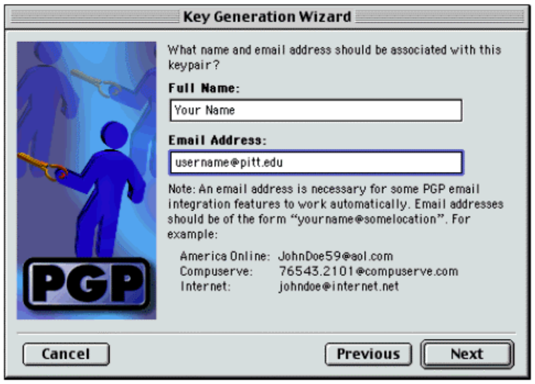
A key pair consists of a "public key" and a "private key." The public key should be given to everyone you know (PGP has facilities to assist in this). The private key should be kept absolutely secret.

If you'd like more information on what a key pair is and how PGP works, select "PGP Help" from the Help menu.

Otherwise, click the Next button below to continue.

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.



Key Generation Wizard

What name and email address should be associated with this keypair?

Full Name:

Your Name

Email Address:

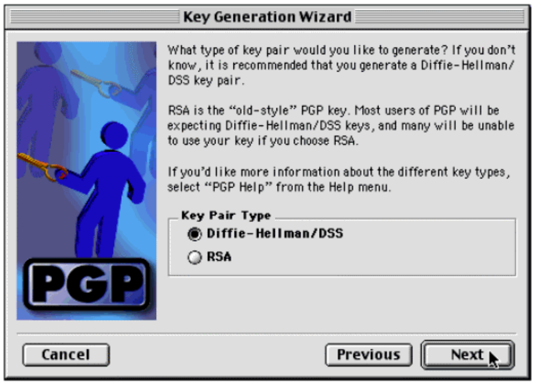
username@pitt.edu

Note: An email address is necessary for some PGP email integration features to work automatically. Email addresses should be of the form "yourname@somelocation". For example:

America Online:	JohnDoe59@aol.com
Compuserve:	76543.2101@compuserve.com
Internet:	johndoe@internet.net

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**.



Key Generation Wizard

What type of key pair would you like to generate? If you don't know, it is recommended that you generate a Diffie-Hellman/DSS key pair.

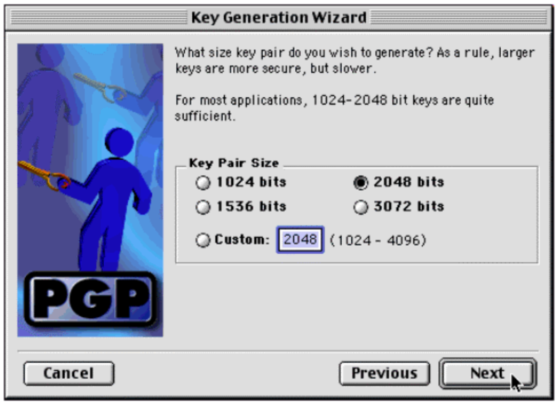
RSA is the "old-style" PGP key. Most users of PGP will be expecting Diffie-Hellman/DSS keys, and many will be unable to use your key if you choose RSA.

If you'd like more information about the different key types, select "PGP Help" from the Help menu.

Key Pair Type

● Diffie-Hellman/DSS
○ RSA

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**.



Key Generation Wizard

What size key pair do you wish to generate? As a rule, larger keys are more secure, but slower.

For most applications, 1024-2048 bit keys are quite sufficient.

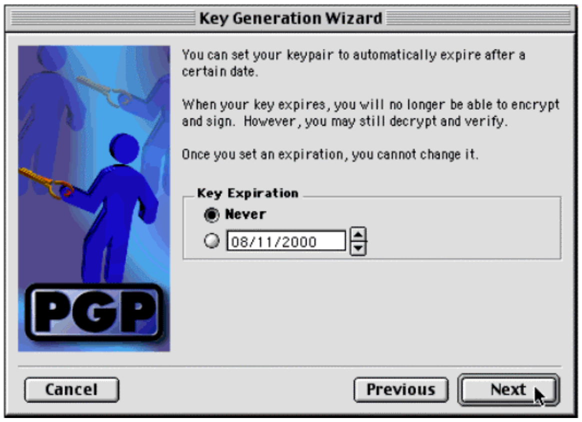
Key Pair Size

○ 1024 bits ● 2048 bits

○ 1536 bits ○ 3072 bits

○ Custom: 2048 (1024 - 4096)

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**.



Key Generation Wizard

You can set your keypair to automatically expire after a certain date.

When your key expires, you will no longer be able to encrypt and sign. However, you may still decrypt and verify.

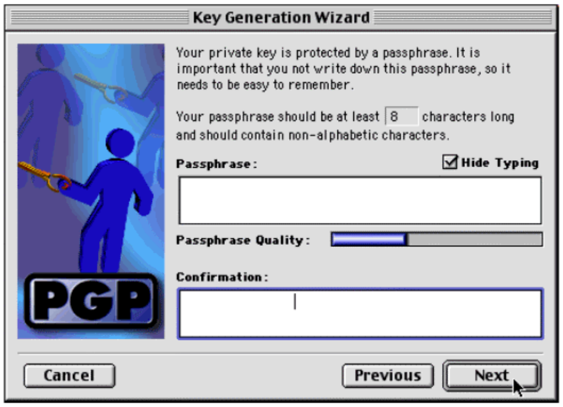
Once you set an expiration, you cannot change it.

Key Expiration

● Never

○ 08/11/2000

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**.



Key Generation Wizard

Your private key is protected by a passphrase. It is important that you not write down this passphrase, so it needs to be easy to remember.

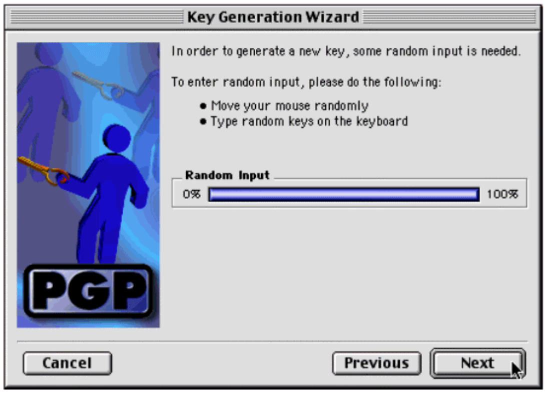
Your passphrase should be at least 8 characters long and should contain non-alphabetic characters.

Passphrase: ☑ Hide Typing

Passphrase Quality:

Confirmation:

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



Key Generation Wizard

In order to generate a new key, some random input is needed.

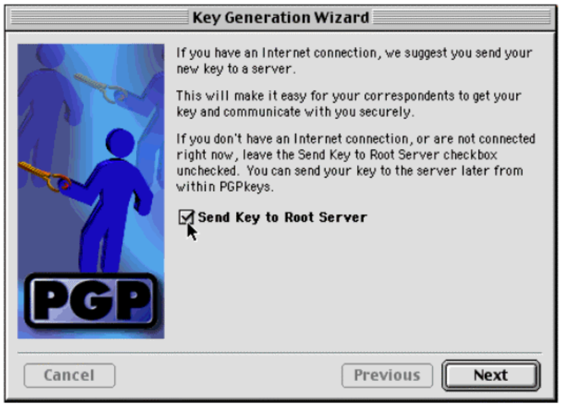
To enter random input, please do the following:

- Move your mouse randomly
- Type random keys on the keyboard

Random Input

0% 100%

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**.



Key Generation Wizard

If you have an Internet connection, we suggest you send your new key to a server.

This will make it easy for your correspondents to get your key and communicate with you securely.

If you don't have an Internet connection, or are not connected right now, leave the Send Key to Root Server checkbox unchecked. You can send your key to the server later from within PGPkeys.

☑ Send Key to Root Server

13. Click **Done** 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

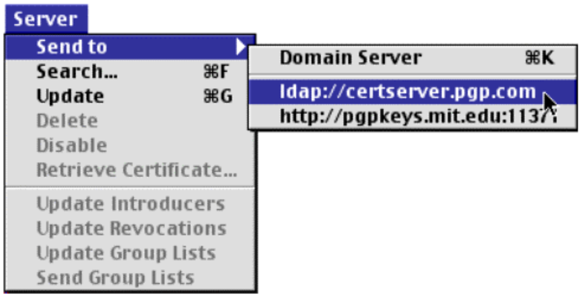
Making your key available through a public certificate server:

1. Open the PGP 6.5 folder from the location where you installed it.

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.



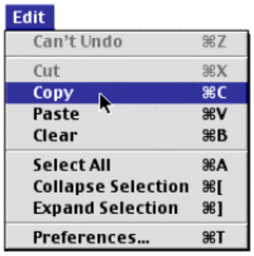
Sending keys through e-mail:

1. Open the PGP 6.5 folder from the location where you installed it.

2. Double-click **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.

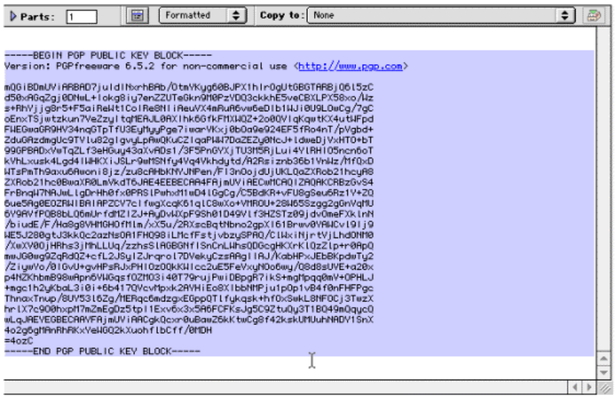


5. Paste the text into an e-mail message and send it.

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.



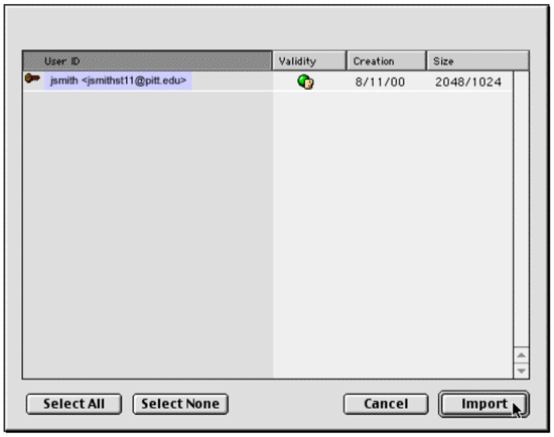
```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.5.2 for non-commercial use <http://www.pgp.com>

mQGiBDmUViARBAD7juldINxrhBAb/OtmYKyg60BJPX1hIr0gUtGBGTARBjQ6l5zC
d50xAGqZgj0DNwL+Iokg8iy7enZZUTeGkn9M0PzYDQ3ckkhE5veCBXLPX58xo/Wz
s+RhYjjg8r5+F5aiReWt1CoIRe8NIiAeuVX4mRuA6vw6eDIb1WJi0U9LOwCg/7gC
oEnxTSjwtzkun7VeZzyItqMEAJL0AXIhk6GfkFMXWQZ+2o0QVIqKqwtKX4utWFpd
FWEGwaGR9HV34nqGTpTfU3EyMyyPge7iwarVKxj0bOa9e924EF5fRo4nT/pVgbd+
ZduGAzdmgUc9TVlu82gIgvyLpAwQKuCZIqaPWW7DaZEZy0NcJ+ldweDjVxHTO+bT
99GPBADxVwTqZLf3eHGuy43aXvADs1/3F5PnGYXjTU3M5RjLui4YlRHIO5ncn6oT
kVhLxusk4Lgd4IWHKXiJSLr9wMSNfy4Vq4Vkhdytd/A2RsiznbZ36b1VnWz/MfQxD
WTsPmTh9axu6Awoni8jz/zu8cAHbKNYJNPen/FI3nOojdUjUKLQaZXRob21hcyA8
ZXRob21hc0BwaXR0LmVkdT6JAE4EEBECAA4FAjmUViAECwMCAQIZAQAKCRBzGvS4
FrBnqW7NAJwLlgDrHh0fx0PRSlPwhxM1wD4lGgCg/C5BdKR+vFU8gSeu6Rz1Y+ZQ
6ue5Ag0EOZRWIBAIAPZCV7cIfwgXcqK61qlC8wXo+VMROU+28W65Szgg2gGnVqMU
6Y9AVfPQB8bLQ6mUrfdMZIZJ+AyDvWXpF9Sh01D49Vlf3HZSTz09jdvOmeFXklnN
/biudE/F/Ha8g8VHMGHOfMlm/xX5u/2RXscBqtNbno2gpXI61Bruv0VAWCvl9Ij9
WE5J280gtJ3kkQc2azNsOA1FHQ98iLMcfFstjvbzySPAQ/ClWxiNjrtVjLhdONM0
/XwXV00jHRhs3jMhLLUq/zzhsSlAGBGNfISnCnLWhsQDGcgHKXrKlQzZlp+r0ApQ
mwJG0wg9ZqRdQZ+cfL2JSyIZJrqrol7DVekyCzsAAgIIAJ/KabHPxJEbBKpdwTy2
/ZiywYo/0IGvU+gvHPsRJxPHIOzOQkKWIcc2uE5FeVxyNOo6wy/Q8d8sUVE+a20x
p4NZKhbm898wApn6VWGqsfOZMO3i40T79rujPwiDBpgR7ikS+mgMpqq0mV+OPHLJ
+mgc1h2yKbaL3i0i+6b417QVcvMpxk2AYHiEo8XIbbNMPju1pOp1vB4f0nFHFPgc
ThnaxTnup/8UY53l6Zg/MERqc6mdzgxEGppQTlfykqsk+hfOxSwkL8NFOCj3TwzX
hrlX7c9O0hxpM7mZmEgDz5tpI1Exv6x3x5A6FCFKsJg5C9ZtuQy3T1BQ49mQqycQ
wLqJAEYEGBECAAYFAjmUViAACgkQcxr0uBawZ6kKtwCg8f42kskUMUuhNADV1SnX
4o2g6gMAnRhRKxYeWGQ2kXuohflbCff/0MDH
=4ozC
-----END PGP PUBLIC KEY BLOCK-----
```

2. Open the PGP 6.5 folder from the location where you installed it.

3. Double-click **PGPkeys**.

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



User ID	Validity	Creation	Size
jsmith <jsmithst11@pitt.edu>	●	8/11/00	2048/1024

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

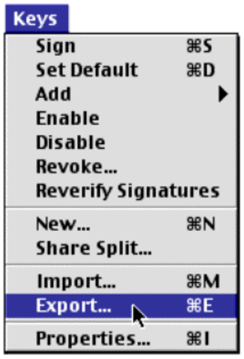
There are three ways to export your key pair.

1. To export your key pair using the **Keys** menu:
   a.) Open the PGP 6.5 folder from the location where you installed it.

   b.) Select **PGPkeys**.

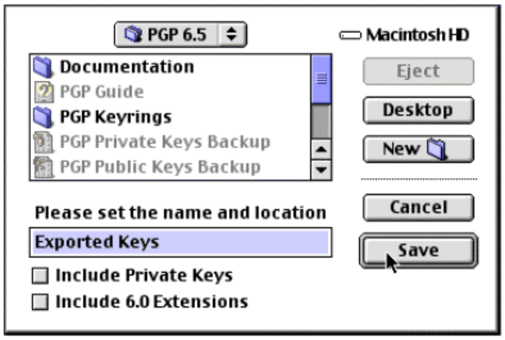
   c.) Select your key pair by highlighting the name that you entered in the **Key Generation Wizard**.

   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**.



Please set the name and location

Exported Keys

□ Include Private Keys

□ Include 6.0 Extensions

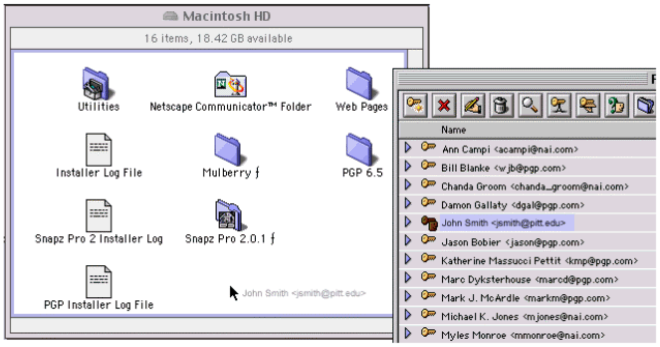
2. To export your key pair using **Drag and Drop**:

   a.) Open the PGP 6.5 folder from the location where you installed it.

   b.) Double-click **PGPkeys**.

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

   d.) Hold down the mouse button and drag your key pair to the desktop or desired folder. Release the mouse button.


Macintosh HD
16 items, 18.42 GB available
Utilities
Netscape Communicator™ Folder
Web Pages
Installer Log File
Mulberry ƒ
PGP 6.5
Snapz Pro 2 Installer Log
Snapz Pro 2.0.1 ƒ
PGP Installer Log File
John Smith <jsmith@pitt.edu>
Name

Ann Campi <acampi@nai.com>
Bill Blanke <wjb@pgp.com>
Chanda Groom <chanda_groom@nai.com>
Damon Gallaty <dgal@pgp.com>
John Smith <jsmith@pitt.edu>
Jason Bobier <jason@pgp.com>
Katherine Massucci Pettit <kmp@pgp.com>
Marc Dyksterhouse <marcd@pgp.com>
Mark J. McArdle <markm@pgp.com>
Michael K. Jones <mjones@nai.com>
Myles Monroe <mmonroe@nai.com>

3. To export your key pair using **Copy and Paste**:

   a.) Open the PGP 6.5 folder from the location where you installed it.

   b.) Double-click **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.

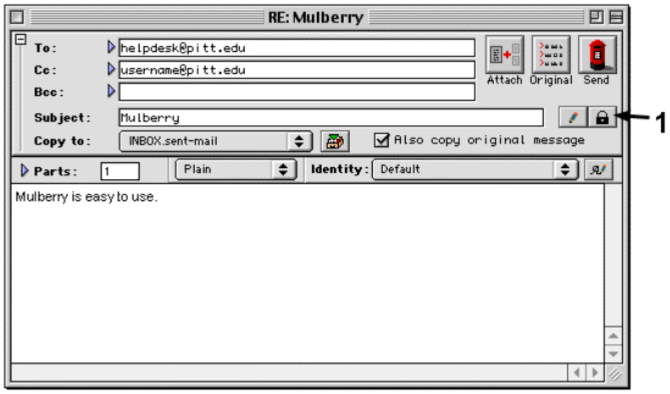
Encrypting Messages

Once you have installed PGP, 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.



To: helpdesk@pitt.edu
Cc: username@pitt.edu
Bcc:
Subject: Mulberry
Copy to: INBOX.sent-mail
☑ Also copy original message
Parts: 1
Plain
Identity: Default

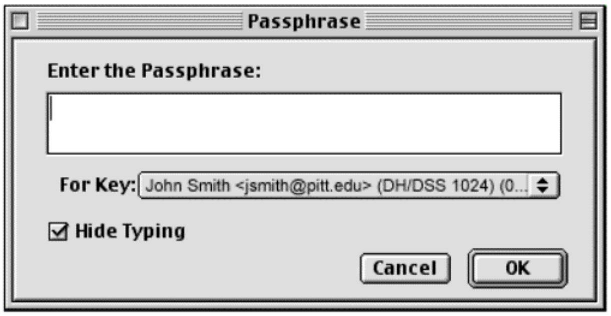
Mulberry is easy to use.

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.



Passphrase

Enter the Passphrase:

For Key: John Smith <jsmith@pitt.edu> (DH/DSS 1024) (0...

☑ Hide Typing

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**.