Introduction to PGP and Lock & Key

Press here **if you would like a guided tour of Lock & Key.**

The rapid growth of the Internet has fueled great interest in encryption for protecting the security of messages transmitted over the Internet.

Pretty Good Privacy (PGP) has become the de facto standard for high-security encryption. PGP uses what is known as dual-key cryptography. For each user, it creates a pair of keys, a public key and a private key. Either can be used to encrypt messages which can be read by the other. The private key is kept secure by the owner, and requires a secret pass phrase to use. The public key, however, can be widely distributed (and often will be available from a BBS or a public key repository). The public key can be freely distributed because it requires the private key, which only the owner can use, to lock or unlock messages. This is a significant advantage over conventional cryptography, which uses a single key, where the single key, if intercepted, can be used by an unauthorized person to decrypt messages.

Dual-key cryptography provides for two separate, but related, uses:

- **Encryption.** The sender uses the recipient's public key to encrypt a message or a file for the intended recipient. This message or file can then be sent through insecure channels such as the Internet. Only the recipient, who is in possession of the matching private key and who knows its pass phrase, can decrypt the message.

- **Electronic "signatures."** The sender uses his private key (as to which only he knows the password) to add a "signature" (a brief encrypted string of characters) to any message or file. The recipient can use the sender's public key to verify that the message was, in fact, sent by the sender, and not by an impostor.

Limitations of PGP

PGP has been described as "public key cryptography for the masses." Since PGP is freeware, is widely available, and has become a standard, this statement is largely true. However, PGP is a DOS-based program, with an obscure command line syntax, which intimidates new users and discourages the use of this potentially valuable program.

There have been many shells and front ends written for PGP to make use easier, especially under Windows. What makes **LOCK & KEY** different? LOCK & KEY, unlike other PGP shells, is completely integrated into the Windows 95 Explorer. What this means is:

- You can **right-click on any file** to bring up a menu choice for encrypting the file. Simply enter the name(s) of the intended recipient(s) whose public keys you wish to use to encrypt the message.

- You can **double-click on any encrypted file** to decrypt that file using your private key.

- You can **double-click on any public key file** to add it to your public key ring.

- If you have **Quick View or Quick View Plus** installed, you can view the decrypted file using Quick View or Quick View Plus. Optionally, you can save the result to a file.

- You can choose to **Open (execute)** or **Print** any decrypted file.

- You can encrypt text in the **Windows clipboard**; you can encrypt text or binary files to the Windows clipboard (to paste into an e-mail program, for example); you can decrypt encrypted text which has been copied to the Windows clipboard (e.g. from an e-mail program); and can decrypt a file to the clipboard.

LOCK & KEY works the way YOU want to work, making the most-used functions one-click simple.

- Include your public key (so the recipient can send an encrypted response) with an encrypted message as a single operation.

- Use any editor or other program to compose messages, using any template file (like an e-mail signature file).

- Encrypt or decrypt a batch of files in a single operation.

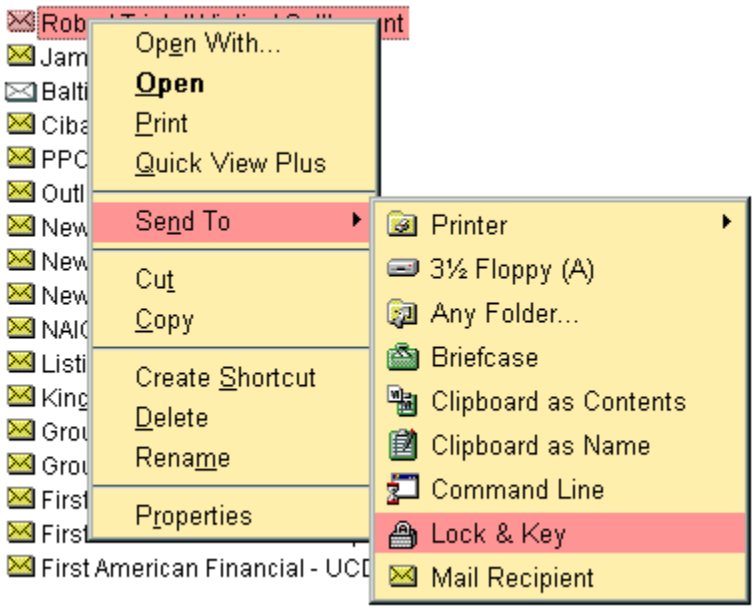
- Extract any public key to the clipboard, to paste into any e-mail program.

- View signatures within Windows 95.

LOCK & KEY **supports long file names** under Windows 95.

Lock32: Encrypting Files and Messages

LOCK & KEY automatically adds a shortcut to the Windows 95 SendTo folder. To encrypt any file, simply right click on the file in Explorer (or on the Windows 95 desktop), select the "Send To" menu item, and choose "Lock & Key."



This will bring up the main LOCK32 dialog box:

Simply enter the name (or part of the name) of the public key(s) of the intended recipient(s). If the recipient's name is found in your personal key ring, the file will be encrypted and renamed with a .PGP extension in the same directory where the input file is located. Unless you choose the "wipe" option, the unencrypted input file is not affected.

Following is a discussion of the various PGP options that can be selected using LOCK32.

Recipients
Input
Output
Encryption Method
Signature

Public key cryptography uses the public key of a specific recipient to encrypt the message, which can then only be decrypted by that person using his or her **secret key**. This is the normal method of operation of PGP and provides the greatest security, since the recipient's secret key is necessary to decrypt the message. The public key, however, can be freely distributed.

Use public key cryptography if you have the intended recipient's public key.

If you do not have the recipient's secret key, you will need to use **conventional cryptography**, which uses a single pass phrase to encrypt and decrypt. You will need a secure channel to send the pass phrase to the intended recipient; if the pass phrase is intercepted, anyone with the pass phrase can decrypt the message.

This displays the source file or data which will be encrypted.

If you've selected a file in Explorer, this will show the name of the file.

If you have not specified a file (for example, if you are running LOCK32 from the Start Menu, LOCK32 will encrypt the contents of the Windows Clipboard.

If you have used LOCK32's built-in editor (selected by pressing the “Compose” button), then this will indicate that Lock & Key's editor is the input source.

PGP permits the use of **electronic "signatures"** to authenticate messages. The sender uses his private key (as to which only he knows the password) to add a "signature" (a brief encrypted string of characters) to any message or file. The recipient can use the sender's public key to verify that the message was, in fact, sent by the sender, and not by an impostor. Use of an electronic signature requires that the recipient have your public key.

Note that you must enter your pass phrase in order to create a signature.

You need not encrypt a message in order to attach your signature.

If you have more than one secret key, you can select which one to use for making signatures by pushing the “Select” button. This will read your secret keyring and display a pop-up list of available signatures. Press OK to close the list. The chosen signature will be displayed.

If you check this box, PGP will encrypt each file or message so that it can be decrypted with your own secret key. This is a useful option for creating a “file” copy of messages or files you have encrypted. If you use this option, you can keep the encrypted copy (with greater security) on your own computer, and be able to access it later.

New Features in Version 4.0

- KEYCHAIN now includes a specially designed encrypted message editor**.** If you have Eudora or Pegasus Mail installed, you can use this editor to compose an encrypted message for delivery through the Internet using Eudora or Pegasus Mail. Unlike external programs and mail program plug-ins, this editor contains features especially designed for sending encrypted messages, including separate windows for **cleartext** and **encrypted** portions of messages; signing the message with your **electronic signature**; automatically appending your **public key** to messages; using the public keyring itself as an **address book**; and simultaneously encrypting and sending messages to **named groups** of recipients.

- LOCK & KEY now caches the list of keys in the public and secret keyrings, updating the keyring caches whenever the contents of the keyrings change. This allows the **keyrings to be loaded instantly**.

- LOCK & KEY now supports named groups of keys. You can create and edit groups of keys using KEYCHAIN. Using LOCK32, you can encrypt a file for all persons whose keys are included in the named key group. Using KEYCHAIN, you can compose and send an encrypted message to all persons in the key group.

- LOCK & KEY now supports detached signature certificates. You can create a detached signature certificate for a file using LOCK32; and can use KEY32 to verify that the signature certificate is valid; that is, that the sender signed the file and that the file contents have not been altered.

For a complete listing of changes, see the revision history.

Revision History

Version 4.0.0 – June xx, 1997

Version 3.1.0 – March 18, 1997

- LOCK32 permits configuring an external editor for composing messages. The internal editor has been removed.
- LOCK32 permits selecting a template file for composing messages.
- LOCK32 supports encrypting multiple files in a single operation.
- KEY32 supports decrypting multiple files in a single operation.
- Sending encrypted files to Lock & Key automatically activates KEY32.
- When LOCK & KEY is run, it will detect whether clipboard input is encrypted and will run LOCK32 or KEY32 as appropriate.
- LOCK32 can preserve the original long file name when encrypting a file to the Windows clipboard. KEY32 will read this information and offer to save the file using the original file name.
- LOCK32 and KEY32 will prompt the user for a filename to save encrypted or decrypted output, where a filename has not already been provided. Warnings will be provided before files are overwritten.
- KEY32 now validates clipboard input, to remove data which is not part of the PGP message or key; and removes extraneous data (including quoting characters at the beginning of each line) added by mail programs.
- KEY32 will now add a sender's public key to the keyring and decrypt a message in the clipboard as a single operation.
- KEY32 will verify a signature of a signed plaintext message.
- KEY32 will decrypt encrypted text files to the Windows clipboard.
- KEY32 now bypasses the "use default viewer" when viewing decrypted files using the version of Quick View which is included with Windows 95.
- The PGP pass phrase is passed to PGP without being written to disk, for greater security.
- KEY32 reads the name in an armored public key block and prompts the user whether to add this key to the public key ring.
- KEYCHAIN, a new module, provides key management functions, including generating key pairs, extracting keys, removing keys, setting the default signature key, and viewing the fingerprint of a key.
- The Lock & Key help file now includes an interactive tutorial, with "live" links to the Internet.
- An About box has been added. This box features "live" links to our web page and to e-mail. To access the About box in LOCK32 or KEY32, right-click on the Help button.
- The PGP console output window now scrolls, and displays output information for each file in a multiple file selection.
- Language glossaries have been added for Russian, Danish and Norwegian.

Version 3.0.0 – January 8, 1997

- LOCK & KEY now supports languages other than English. Language glossaries are provided for German, French, Spanish, Dutch, Italian and Finnish. Other glossaries can easily be added.
- LOCK & KEY now provides context-sensitive Windows 95 help.
- LOCK32 now contains an integrated text editor for composing PGP messages.
- LOCK32 includes an option to append your public key to any message encrypted to the Windows Clipboard, to make it easy for a recipient to encrypt a response, or to view your signature.

- KEY32 now features an option to open (execute) or to print a decrypted file, without permanently saving the file to disk.
- KEY32 will decrypt the file without prompting, using the option last specified (View/Save/Open/Print), and without verifying signature, if the PGPPASS environment variable has been set. This speeds decrypting numerous files.
- Clipboard support for RichText has been removed, to speed loading.
- LOCK & KEY now generates a debugging log when a runtime error occurs.
- LOCK32 now passes the PGP pass phrase to PGP using the PGPPASS environment variable rather than as a command line variable. This enables use of longer pass phrases without exceeding the maximum length of a DOS command line. Please note that this environment variable appears only in the virtual machine in which PGP is run, and disappears as soon as PGP finishes, so this does not compromise security.
- LOCK & KEY now wipes all temporary files which contain confidential data, to prevent recovery of the PGP pass phrase using Norton or other disk utilities.
- Several runtime errors present in version 2.1.0 have been corrected, including (1) runtime error 76 occurring where the public keyring name in CONFIG.TXT was enclosed in quotes; (2) runtime error 53 occurring with certain filenames; (3) failure of KEY32 to remove the .PGP or .ASC extension when decrypting files; (4) proper handling of encrypted .ZIP files; (5) runtime error 62 encountered with certain non-English versions of Windows 95; and others.

Version 2.1.0 – October 24, 1996

- LOCK32 and KEY32 modified to display input source (filename or clipboard).
- LOCK32 now supports PGP "wipe" option (-w).
- LOCK32 now permits Rich Text support to be disabled, making it possible to send clipboard text as plain text.
- LOCK32 now supports the PGP encrypt-to-self option, so the user can decrypt messages as well as the recipients.
- LOCK32 now supports selecting an alternate secret key for making signatures.
- KEY32 will now recognize a public key block that has been placed in the clipboard, and will offer to add the public key to your public key ring.
- KEY32 now uses PGP to read the public key ring, which avoids some errors when removing keys.
- Fixed bug in KEY32 which caused console output to be prematurely closed.
- LOCK32 and KEY32 now read the location of the public keyring from CONFIG.TXT (or PGP.INI).
- Certain settings (default user name and encrypt-to-self) are read from and stored in CONFIG.TXT (or PGP.INI). This should make longer PGP commands more reliable.

Version 2.0.2 – October 7, 1996

- Fixed bug which would cause some public key rings not to be read completely by LOCK32 and KEY32.
- Fixed bug introduced in version 2.0 which would prevent encrypting a message for multiple recipients.
- Fixed bug which caused sound not to play correctly in KEY32. Sound file is now installed in the program directory.

Version 2.0.0 – September 23, 1996

- LOCK32 now reads the default public key ring, and permits selection of a public key from a drop-down list.

- KEY32 can now be used to view the public key ring and to remove individual public keys.
- The default install option now places a shortcut to LOCK32 in the SendTo folder. The installation hs been improved and now creates an uninstall option in the Control Panel Add/Remove Programs applet.
- The registration password can now be entered without running a .REG file or REGEDIT.

Version 1.5.0 – August 28, 1996

- User preferences for encrypting, decrypting, signature and output are saved in the registry and restored when the program is next run.
- Registered users' registration password is stored in the registry.
- The PGPPASS environment variable, if present, is used instead of manual entry of the pass phrase.
- Signature of plaintext files is supported.
- The filename extension is stored when a file is encrypted, and restored when the file is decrypted and saved as a file.

Version 1.4.1 – August 13, 1996

- Added installation options for placing Lock & Key in the SendTo folder (to resolve compatibility issues with MS Office).
- Added an uninstall option.
- Added long file name support to LOCK32.EXE, when it is placed in the SendTo folder.
- Added support to KEY32 for adding public keys to the default public key ring.

Version 1.3.0 – August 8, 1996

- Added support for LOCK32 to encrypt text (including Rich Text) in the Windows clipboard.
- Added support for LOCK32 to save its output (in armored ASCII) to the Windows clipboard.
- Added support for KEY32 to decrypt encrypted data (armored ASCII) from the Windows clipboard.

Version 1.2.0 – August 6, 1996

- Added option to LOCK32 to encrypt files when armoring.
- Added option to LOCK32 to add signature when encrypting.
- Added option to view/save PGP console output when an error occurs.
- Modified KEY32 to display signature information.
- Modified KEY32 to view/save PGP console output when an error occurs.
- Corrected bug in LOCK32 that caused window to be truncated.
- Corrected bug in INSTALL program that resulted in “Runtime Error 53.”
- INSTALL now adds double click support for .ASC as well as .PGP files.

Version 1.1.0 – August 1, 1996

- Added option to LOCK32 to encrypt using conventional cryptography.
- Added option to LOCK32 to armor files (convert to 7-bit ASCII).
- Fixed bug in LOCK32 where user's TEMP file was other than C:\TEMP.
- Fixed bug in KEY32 where the user's pass phrase contained spaces.

Version 1.0.1 – July 29, 1996

- Corrected install routine to work properly on faster computers, avoiding run-time error.
- Improved install routine for creating registry entries, to properly work with long file names, and

to eliminate the REGEDIT message box.

- Fixed sound effects in KEY32.EXE

Version 1.0.0 – July 27, 1996

- Original Release.

Other Features

ENCRYPTING FILES AND MESSAGES

- LOCK & KEY includes an option to **encrypt all messages with the user's own public key**, so that the user (as well as the recipients) can decrypt the encrypted message.

- LOCK & KEY automatically **reads the public key ring** specified in the user's PGP configuration file. When encrypting a message or a file, you can now simply point and click to select the name of a user. You can still simply type in part of the name of one or more recipients to match names in the public key ring.

- LOCK & KEY supports the PGP option to wipe the input file after encryption.

- LOCK & KEY permits you to append your public key to messages encrypted to the Windows Clipboard, making it easy for the recipient to send an encrypted reply or to view your signature.

DECRYPTING FILES AND MESSAGES

- LOCK & KEY will allow you to **open (execute) or print a decrypted file**, in addition to the options of viewing the decrypted file using QuickView, or saving the file to disk.

ELECTRONIC SIGNATURES

- LOCK & KEY permits selection of any secret key (not just the default secret key) for signing messages.

- LOCK & KEY supports **signing plaintext files**. If the encryption option "None" is selected, an option to save output as plaintext is added. If these options are chosen, then the input file (which should be plain text) will not be encrypted, so it can be read without decryption, but the signature is added and can be verified using KEY32.

KEY MANAGEMENT

- LOCK & KEY will recognize a **public key that has been placed in the clipboard** and will offer to add it to your public key ring.

- KEYCHAIN provides complete key management functions, including **generating key pairs**, extracting keys, removing keys, setting the default signature key, and viewing the fingerprint of a key.

ADVANCED FEATURES

- LOCK & KEY now features support for languages. A language glossary is provided for English, German, Spanish, French, Italian, Dutch, Finnish, Russian, Danish and Norwegian. Support for other languages can easily be added by editing the language glossary. In addition, LOCK & KEY can work with file names containing accented characters.

- LOCK & KEY supports use of the PGPPASS environment variable. If the PGPPASS environment variable has been set, this value will be placed in the input fields for which the pass phrase is required (e.g. when signing files, or decrypting files encrypted with your public key). **PLEASE NOTE THAT THE PGPPASS ENVIRONMENT VARIABLE IS POTENTIALLY A SECURITY RISK AND ITS USE IS NOT RECOMMENDED.**

FOR ADDED CONVENIENCE

- LOCK & KEY features **context-sensitive Windows 95-style help**., including a tutorial to explain PGP and show how to use LOCK & KEY to make encryption and decryption with PGP simple.

- LOCK & KEY saves the last settings for encryption, decryption, output and signature options, so that the last settings used will be restored when the program is next run. NOTE THAT THE PASS PHRASE IS NOT SAVED IN THE REGISTRY. IT MUST BE ENTERED EACH TIME UNLESS THE PGPPASS ENVIRONMENT VARIABLE IS SET. Also, note that the "Wipe File" option is not saved between uses, to protect against accidental deletion of files.

- LOCK & KEY automatically detects whether the input data is an encrypted file (to be decrypted), a public key (to be added to the key ring), or a regular file or message (to be encrypted), whether the input data is a file or is contained in the Windows clipboard.

- LOCK & KEY will encrypt and decrypt multiple files or messages in a single operation. LOCK & KEY can even decrypt messages and add keys to the public keyring in a single operation.

- LOCK & KEY now **validates clipboard input**, to remove data which is not part of the PGP message or key; and removes extraneous data (such as quoting characters at the beginning of each line) added by mail programs. This makes it easier than ever to decrypt PGP-encrypted messages.

SUPERIOR WINDOWS 95 INTEGRATION

- LOCK & KEY **saves the original filename extension** when encrypting files, and automatically restores this extension when the file is decrypted and saved as a file.

- LOCK & KEY will preserve **long file names** when encrypting and decrypting files. LOCK & KEY can even **preserve the original long file name** when encrypting a file to the Windows clipboard. LOCK & KEY will read this information and offer to save the file using the original file name.

- LOCK & KEY will encrypt and decrypt messages in the **Windows clipboard**; and can place the encrypted or decrypted output in the Windows clipboard.

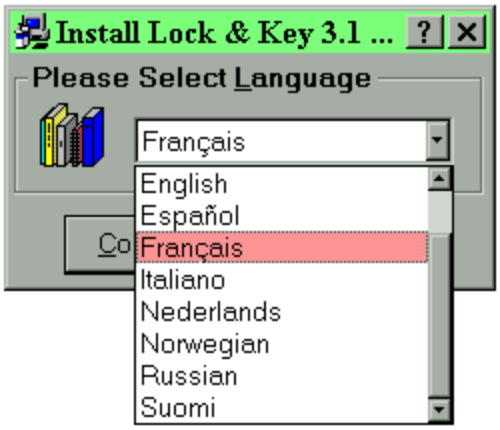
- LOCK & KEY will decrypt files to **QuickView** or **QuickView Plus** if present on your system. Also, LOCK & KEY will preserve the original filename extension when encrypting a file, and can use this information to automatically **Launch** or **Print** the decrypted file using the associated application. It is not necessary to save the file to disk first.

FOR ADDED SECURITY

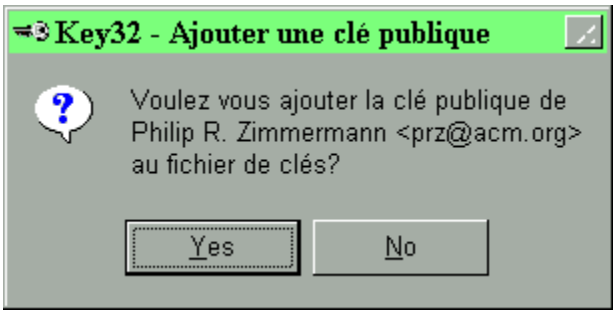
- For greater security, the PGP pass phrase is passed to PGP without being written to disk.

Language Support

LOCK & KEY version 3.1 now supports languages other than English. A language glossary is provided for English, German, Spanish, French, Italian, Dutch, Danish, Russian, Norwegian and Finnish. This language glossary is contained in the file GLOSSARY.INI, which is installed to the Lock & Key directory.



When installing LOCK & KEY, you are asked to choose a language. This language will be used for displaying labels in the LOCK & KEY dialog boxes, and for message boxes. This language preference is stored in the Registry and can be most easily changed simply by reinstalling LOCK & KEY. (Please note that LOCK & KEY will, for some operations, set PGP itself to run in English. This is necessary because LOCK & KEY must read the PGP output to determine what results have occurred. This should not be a major limitation, since PGP is run mostly behind the scenes. LOCK & KEY becomes the user's interface to PGP.)



GLOSSARY.INI is a text file that follows the structure of other Windows .INI files, and can easily be edited with Notepad. GLOSSARY.INI includes a section for each label or message which LOCK & KEY generate. Each section is followed by the appropriate language string for each language. For example, the following section shows wording for the “Recipients” label, in English, German, Spanish, French, Italian, Finnish, Dutch, Russian, Norwegian and Danish:

```
[Recipients]
en=&Recipients
de=&Empfänger
```

```
es=&Destinatarios
fr=&Destinataires
it=&Destinatari
fi=&Vastaanottajat
nl=O&ntvangers
ru=Ïîëó÷àòåëü
no=&Mottager
da=Modtage&r
```

Several things should be kept in mind if you decide to edit GLOSSARY.INI to add support for another language or to modify the phrasing that is provided.

First, use the vertical bar {|} to force a hard return in message boxes. While Windows does word wrap text in message boxes, it is sometimes preferable to cause lines to break differently. You will notice this is used in some of the longer messages in GLOSSARY.INI. Please note that all labels and messages must appear on a single line in GLOSSARY.INI.

Second, the ampersand {&} when used in a label controls where Windows places the accelerator key. The accelerator key is the key following the ampersand, and is underlined in the dialog box. For example, the above entry creates the following English label:

Recipients

Pressing ALT+R causes this option to be selected, when LOCK & KEY is run.

Third, some entries have a tilde {~}. This entry is used by LOCK & KEY to control where text generated by the program (such as the name of a signature) is to be merged. All messages which contain a tilde must have the tilde to tell LOCK & KEY where to merge the variable. Other messages should not contain a tilde.

Please note that the Lock & Key installation/uninstall programs display messages in English. Language support is provided only for LOCK32 and KEY32.

Thank you to the following users for their contributions to the existing language glossaries:

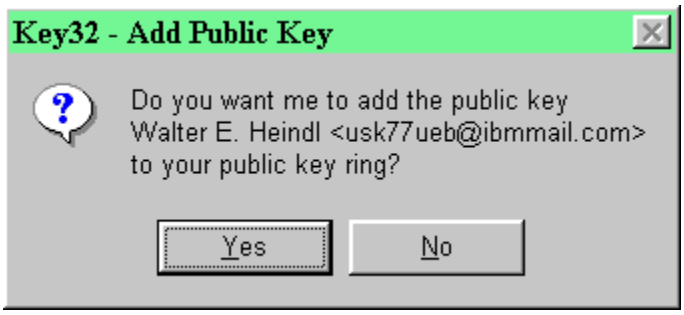
Spanish	Raúl Fernández García
French	Jean-Paul Kroepfli and Ganix Caldichoury
Dutch	Bert Hankes
Finnish	Juha Toronen
Italian	Francesco Lecca
German	Sylvester Boehle, Thorsten Puzich, Thomas Goutier
Danish	Thomas Hansen
Russian	Vadim Tregoubenko
Norwegian	Yann Aker

Please contact the author, Walter E. Heindl, wheindl@voicenet.com, if you would be interested in providing a glossary for additional languages. We will provide you with information on how to produce the glossary. Please do not provide a glossary without checking first, as we may

already have a particular language glossary "in the works."

Adding Keys To Your Public Key Ring

PGP saves public keys as files with the extension .PGP or .ASC. These are the same extensions used for encrypted and armored files, respectively. When you double-click on a file with the .PGP or .ASC extension, KEY32 reads the file to determine whether it contains a public key. If it does, you will be presented with a dialog box as follows:



Press Yes and KEY32 will attempt to add the key to your default public key ring.

Note: if the key file has an .ASC extension, Lock & Key will recognize that the file contains one or more keys, but will not be able to identify the names of the key owners.

KEY32 will respond with an error message if it is unable to add the key, and will give you an opportunity to review the actual PGP console output to identify why the error occurred. The most likely reasons are that the file is corrupted, or that the key was already present in your public key ring.

Occasionally, you may receive a user's public key in the form of text. Such a key block looks like the following (this is the author's actual public key):

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i

mQCNAzIQX1gAAAEEALScp5wuTGUmgqxKE0MAAl9gj4LAg01W/s1eOvDNxMlCzUgc
132JTX9XAnMX3SkTX57zTUY8wh5QxzQEEct4A4jpSTiv4qWUwRyF9GJM1G3JgJ2v
2co/a+Y1mjls87rxQSqt+ooLh9pwGP7NlUumC55ZVY8tzk80wlVrqiqKapYRAAUR
tCdXYWx0ZXIgRS4gSGVpbmRsIDx1c2s3N3VlYkBpYm1tYWlsLmNvbT6JAJUDBRAy
EF9ZVWuqKopqlhEBAd9FA/9HosknDNQES9lccQG8QprJ1Wgg+QW+AhMFM2tmESLl
pR065KYZH4v+ibtJpL0XTqp7v9USOSMEwvASiusEnCekrIgni8aMFYrT90Y3uedD
Zwu6/bBeAcOJRlEq6+yefByEK5d3iDiwreJIXA6p2eVExF0uOo7bwVv9s/5yynjD
9w==
=fmve
-----END PGP PUBLIC KEY BLOCK-----
```

To add such a key to your public keyring, first select the key and copy it to the Windows clipboard. Then, run KEY32. If KEY32 finds a public key block in the Windows Clipboard, it will offer to add the key to the default public key ring.

NOTE: Lock & Key will let you append your own public key to messages you encrypt to the Windows Clipboard.

Registration

LOCK & KEY is shareware. The shareware version is fully functional but includes a time delay. Registration will remove this delay. To register LOCK & KEY, send $24.95 to:

Walter E. Heindl
271 Misty Patch Road
Coatesville, PA 19320 USA

Please provide your e-mail address. You will be sent a personalized password file which will remove the time delay. The password file will work with future versions of LOCK & KEY, making upgrades free.

You may register online via CompuServe SWREG. From CompuServe, GO SWREG for details. Registration number is 12438.

You may also register online using your credit card and the First Virtual Internet payment system. Press here to register Lock & Key at our Internet site. If you are not yet a First Virtual member, press here for more information and to sign up.

Technical Support

For technical support, please visit our Web site:

http://www.voicenet.com/~wheindl/support.htm

If you are connected to the Internet, clicking the above link will take you there. We will endeavor to post information concerning common questions and problems. In addition, you will always find the latest version of LOCK & KEY there.

If you have any technical questions, bugs, etc. not addressed at our Web site, or if you have other suggestions or comments, send e-mail to:

Walter E. Heindl, wheindl@voicenet.com

If you are connected to the Internet, clicking the above link will open a mail message.

Lesson 2: Installation

LOCK & KEY requires the following:

1. A computer running **Windows 95** or **Windows NT 4.0**.

2. The **Visual Basic 4 (32-bit) runtime library** (VB40032.DLL, OLEPRO32.DLL and MSVCRT40.DLL). These files are widely available and are needed to run any application written in Visual Basic 4 (32-bit). If you do not already have these files in your \Windows\System directory, you may download the files from SIMTEL. If you have an Internet connection you can press the following link to retrieve the files:

   http://www.cdrom.com/pub/simtelnet/win95/dll/vb40032.zip

3. **Pretty Good Privacy (PGP)** version 2.6.2 or 2.6.3i. If you do not have PGP, you may obtain it from one of the following sources:

   Users in the United States: http://bs.mit.edu:8001/pgp-form.html
   Users outside the United States: http://www.ifi.uio.no/pgp

   Again, if you have an Internet connection, you can press the above links to obtain PGP. To install PGP, unzip the files into a directory, e.g. `c:\pgp`.

   You must have the PGPPATH= environment variable set in your AUTOEXEC.BAT file. For example, if your PGP files are stored in C:\PGP, then you must have the following line in your AUTOEXEC.BAT file:

   ```
   SET PGPPATH=C:\PGP
   ```

   You must also have a command in AUTOEXEC.BAT specifying a temporary file directory, e.g.:

   ```
   SET TEMP=C:\TEMP
   ```

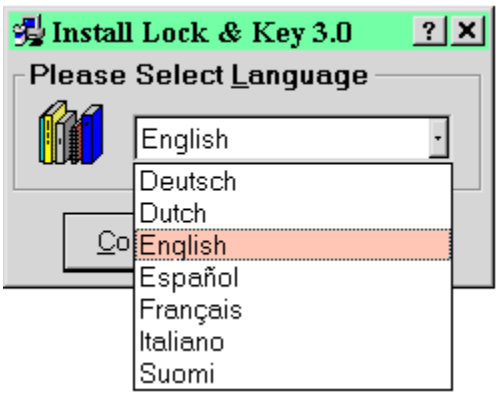
   It is strongly recommended that the temporary file directory NOT be the root directory of a drive. If you are using a RAMdrive as a temporary file directory, create a subdirectory of the root directory. This is because Windows applications create many temporary files and only a limited number of entries can be stored in a root directory.

   We strongly recommend that you read the documentation which comes with PGP. This provides a thorough explanation of public-private key cryptography and PGP features.

4. **To install LOCK & KEY**, simply unzip the files into any directory and run INSTALL.EXE.

   The install program will first ask you to **select a language**. Choices currently available

are English, German, Spanish, French, Italian, Dutch, Danish, Finnish, Norwegian and Russian. Select one of these languages and press Continue. You may change your selection later by editing GLOSSARY.INI (installed in the Lock & Key directory), or by reinstalling LOCK & KEY.



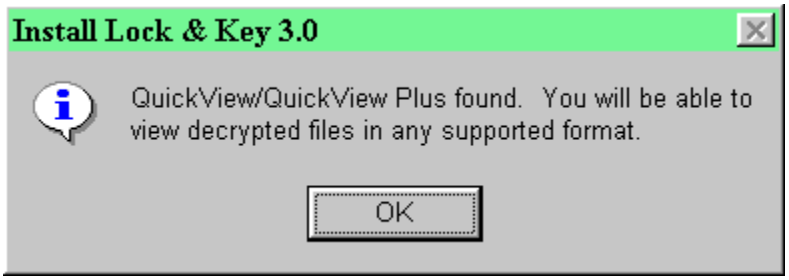
Lock & Key's program files and user guide will be copied to a subdirectory of your PGP directory.

The install program will create the following Start Menu options:

Key Management
Run Lock & Key
Lock & Key User Guide
Uninstall Lock & Key

The install program will modify the Windows Registry to associate .PGP and .ASC files (extensions for files created by PGP) with Lock & Key. It will also add a shortcut to the Windows "Send To" menu, so you can right-click to encrypt any file. The install program will also add Lock & Key to the list of programs which can be uninstalled by the Windows Control Panel "Add/Remove Programs" applet.

The install program will check for the presence of **QuickView or QuickView Plus**. KEY32 will, if one of these is present, enable you to automatically decrypt and view a file in any file format supported by QuickView or QuickView Plus. If QuickView/QuickView Plus is not present, and you choose to view a file immediately upon decryption, NOTEPAD will be used.



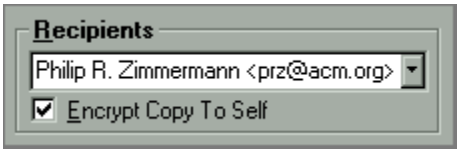
The install program also places RUNPGP.PIF and CONSOLE.PIF in the PGP directory. These files have been optimized for the PGP operations used by Lock & Key. Please note that RUNPGP.PIF file is set to run PGP.EXE minimized. You may, if you wish, change the properties of this .PIF file if you'd prefer to view PGP in action (e.g. to check for error messages). THIS .PIF FILE IS SET TO RUN IN THE BACKGROUND AND TO CLOSE ON EXIT. IT IS IMPORTANT THAT THESE SETTINGS NOT BE CHANGED, OR LOCK & KEY WILL NOT RUN PROPERLY.

5. If you have not used PGP before, you will first need to create your own **public-private key pair.** This will be covered in the next lesson.

6. Extract your newly-created public key and send it to those with whom you wish to send encrypted or signed messages. This can easily be done with KEYCHAIN, LOCK & KEY's key management module. Also, LOCK32 will, if you like, include your public key when sending an encrypted message to the Windows Clipboard, making it easier than ever to use PGP to exchange encrypted and electronically signed correspondence.

Lock32: Choosing Recipients

In order to use public-private key encryption, you must enter the name(s) (or portions of the name(s)) of the intended recipient(s). This will cause the message to be encrypted using the public key of each intended recipient. Note that this option will be greyed out unless public-private key encryption has been selected.



LOCK32 will automatically read your public key ring and place the contents into the drop-down combo box. You can scroll down (or type the first letter and scroll) to select a single recipient. Note: you cannot select multiple recipients this way. To select multiple recipients, type in a portion of the name of each intended recipient, e.g. Tom Dick Harry.

You can encrypt a file or message for a named group of recipients. Press here for more information on creating and managing groups of recipients.

If you check the "Encrypt Copy To Self" box, PGP will also use your own public key to encrypt the message. In this way, you will also be able to decrypt the message after it has been encrypted. Use this option to make a file copy for yourself! (Note: this setting is stored in the PGP configuration file and will affect any use of PGP independently of Lock & Key.)

Lock32: Output Options

LOCK32 gives you three choices for the encrypted output: a binary file, an “armored” file, or “armored” text placed in the clipboard.

A **binary file** uses the standard 8-bit character set, and should be used if you will be delivering the encrypted file using diskette, or if you are able to transmit binary files by electronic mail. Encrypted binary files are given the .PGP extension.

Armored files use low-7-bit encoding, which means that the file can be transmitted by methods that do not support binary files (such as some Internet mail programs). If you wish to transmit the encrypted output as a specific file but can't send a binary file, use this option. Armored files are given the .ASC extension. Note: it is possible to armor a file without encrypting it. This is similar to UUencoding and is a method for transmitting binary files over the Internet.

You will note that LOCK32 supports Windows 95 long filenames, unlike PGP itself. If the file you are encrypting has a long filename, the long filename will be preserved. LOCK32 saves the original extension when encrypting the file, so that SECRET.WK4 becomes SECRET.WK4.PGP (or SECRET.WK4.ASC) when it is encrypted. This enables the original extension to be restored when the file is decrypted and saved as a file. NOTE: The output file is saved in the same directory as the input file.

The third option also creates armored (7-bit) output, but places that output in the **Windows Clipboard**. This will be the preferred option if you wish to simply paste the encrypted output (message or a file) into an electronic mail message.

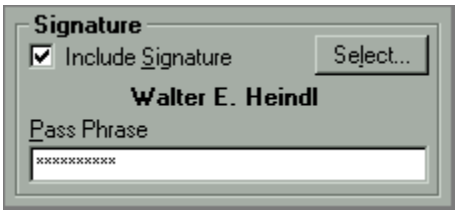
If you choose **“Include My Public Key,”** your default key (MYNAME= in CONFIG.TXT/PGP.INI) will be appended to the message in the Windows Clipboard. This is useful if the recipient doesn't have your public key, but needs it either to verify your own signature, or to send an encrypted response to you. This option requires that you have selected a user ID for making signatures. If no user ID is shown under “Signature,” then press the Select button and choose a user ID.

If you are encrypting files to the Clipboard, you also have the option to **Include the Original Filename**. This will append the name of the original file (including a Windows 95 long file name) to the message. If the recipient is also using Lock & Key, the file will automatically be saved on the recipient's system using the original long file name. If the recipient doesn't have Lock & Key, the recipient can use this information to name the file after it is decrypted.

LOCK32 remembers your preference between uses.

Lock32: Adding Your Electronic Signature

PGP will also let you use your own secret key to "sign" a message. This electronic "signature" can be verified by anyone with your public key. Note: you need to enter the pass phrase for your secret key to make a signature.



Some users may have more than one secret key. LOCK32 permits you to select any secret key in your secret key ring. Simply press the "Select" button, and LOCK32 will use PGP to read your secret key ring. A combo box will appear, with the name of each secret key in your secret key ring. The "Select" button will change to "OK." Simply pick a secret key for creating the signature and press the OK button. The name of the selected signature will appear in this box. Note: The selected signature is stored in the PGP CONFIG.TXT file, and will affect uses of PGP independently of Lock & Key.

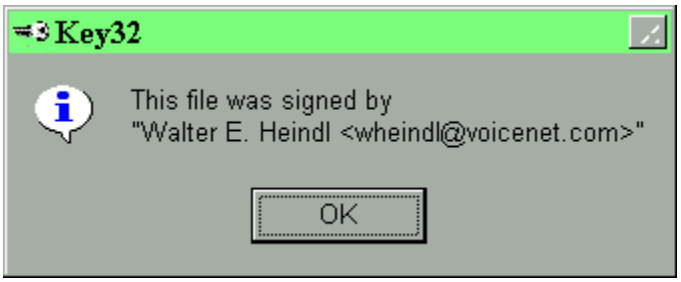
LOCK & KEY also makes it easy to view signatures added by other users.

LOCK32 remembers your preference between uses.

Key32: Verifying Signatures

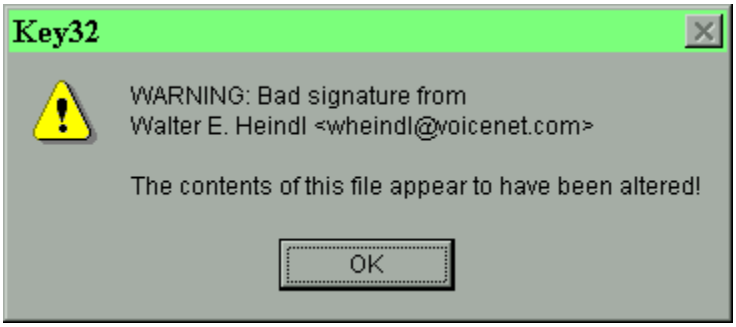
You can also use LOCK32 to electronically "sign" files, as a way of authenticating that you, the holder of the private key, and not an impostor, sent the file. You must enter your secret pass phrase, and PGP will affix an "electronic signature" which the recipient can verify using your public key. For more information, see how to affix your signature when encrypting files.

When using KEY32 to decrypt the file, it will automatically detect whether the encrypted file was signed, and, if it was signed, it will display information about the signer:



Note that PGP can only verify a signature is present if you have the public key of the signer in your public key ring. Often, senders will include their public key with a message so you can add the key to your public keyring and verify that the message was signed. For more information, see how to add a key to your public keyring.

A PGP signature verifies both that the file was signed by the keyholder; AND that the file contents have not been altered since it was signed. If the file is altered, LOCK & KEY will report it:



WARNING: It is common for a sender to include his public key with a message (in fact, Lock & Key can do this as a single operation). This is mainly for the purpose of enabling you to send an encrypted response. While you can use the public key to verify the signature on that message, if it was signed, you should keep in mind that the key is being sent to you by the same person who sent the message, and so you have no assurance that the key really belongs to the person who sent it to you. You should keep that in mind before you trust this first signature. You should be able to trust that the key is genuinely that of the sender before you rely on signatures. You can obtain this trust by various ways:

- Get the public key from a server location known to be accessible only to the sender.
- Get the public key from a public key server.
- Use a key that has been certified by persons known to you (sort of like a notary seal).
- Get the key physically delivered to you by the sender.

You can sign a file with or without encrypting the file. If you choose not to encrypt the file, you will be given the option of saving the output as a plaintext file with the signature attached. The file can be read without KEY32 or PGP; but, using KEY32, you can verify the attached signature.

Note that KEY32 will read the environment for the PGPPASS environment variable, and, if it is found, will place that value automatically in the pass phrase box. For more information and cautions, read about using PGPPASS.

KEY32 will only read a signature if you are decrypting a single file or message. Where multiple files or messages are decrypted in a single operation, KEY32 skips the signature verification process. This is done in order to facilitate automated operations on groups of files. You can still see whether a file is signed by decrypting it by itself.

Security Considerations: PGPPASS

PGP supports use of the PGPPASS environment variable as a way to avoid repetitive entry of your pass phrase. If it is found, the pass phrase will automatically be entered in the pass phrase box in KEY32 (when decrypting files encrypted with your public key) and LOCK32 (when signing files with your public key). From a DOS prompt, type SET PGPPASS=secretpassphrase, where secretpassphrase is your secret pass phrase. Note: for this to work within Windows, this command must be typed before Windows is launched. **THE PGPPASS ENVIRONMENT VARIABLE IS A POTENTIAL SECURITY HOLE, SINCE ANYONE WITH ACCESS TO YOUR MACHINE CAN INSPECT THE ENVIRONMENT VARIABLES OR ANY BATCH FILES THAT SET ENVIRONMENT VARIABLES, E.G. AUTOEXEC.BAT.** While support for this PGP feature has been added at the request of users, its use is not recommended where this security risk is present.

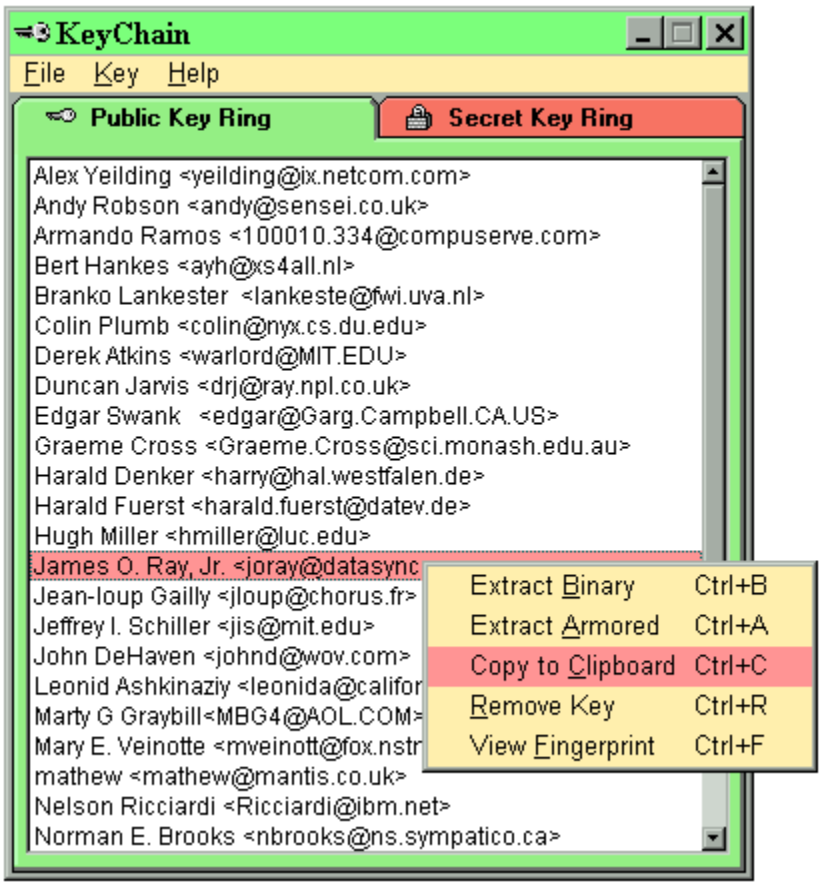
If KEY32 finds that the PGPPASS environment variable has been set, it will decrypt the file using the most recently saved decryption option (View, Save, Open or Print), and without displaying any signature. This speeds the process of decrypting numerous files.

KeyChain: Viewing Key Rings

PGP maintains keys in files called keyrings. Each user will have, by default, one public keyring and one secret keyring. By default, these will be named PUBRING.PGP and SECRING.PGP and will be located in the PGP directory.

Think of the public key ring as an "address book" of other users' PGP keys. The secret keyring is a list of your own identities (you might have more than one secret key for different purposes).

LOCK & KEY includes KEYCHAIN, which will allow you to view all keys in your public and secret keyrings, and to perform common key management functions such as extracting keys, deleting keys, or creating new key pairs. To access KEYCHAIN, press the Start Menu button and launch the "Key Management" shortcut in the Lock & Key program group. This will bring up the main KEYCHAIN window, which includes tabs for the public keyring and the secret keyring:



Using KEYCHAIN, you can:

- Generate a new public-private key pair.
- Extract any public key to a file, or to the Windows clipboard.
- Inspect the "fingerprint" of any key, to verify its authenticity.
- Select the default secret key for making electronic signatures.

- Remove any key.

Security Considerations

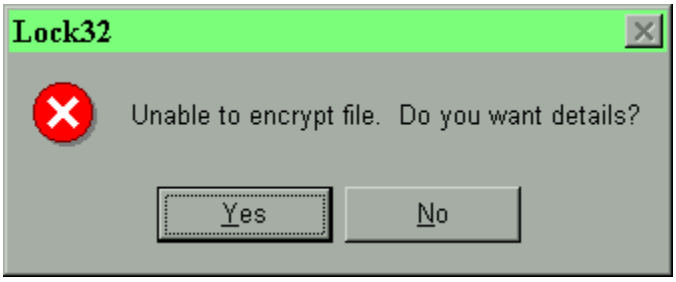
While public key cryptography provides reliable security for messages transmitted through external channels, the user must still take certain precautions to assure that confidential data in its unencrypted form, as well as the secret key and especially its pass phrase, is safeguarded from persons who may gain access to the user's computer.

LOCK & KEY itself observes certain precautions to assure that no vulnerabilities are introduced into the system. In particular, **LOCK & KEY passes the PGP pass phrase to PGP without writing the pass phrase to disk.** Note that the pass phrase is copied to the environment (in memory) in which PGP runs; this environment is destroyed when PGP exits.

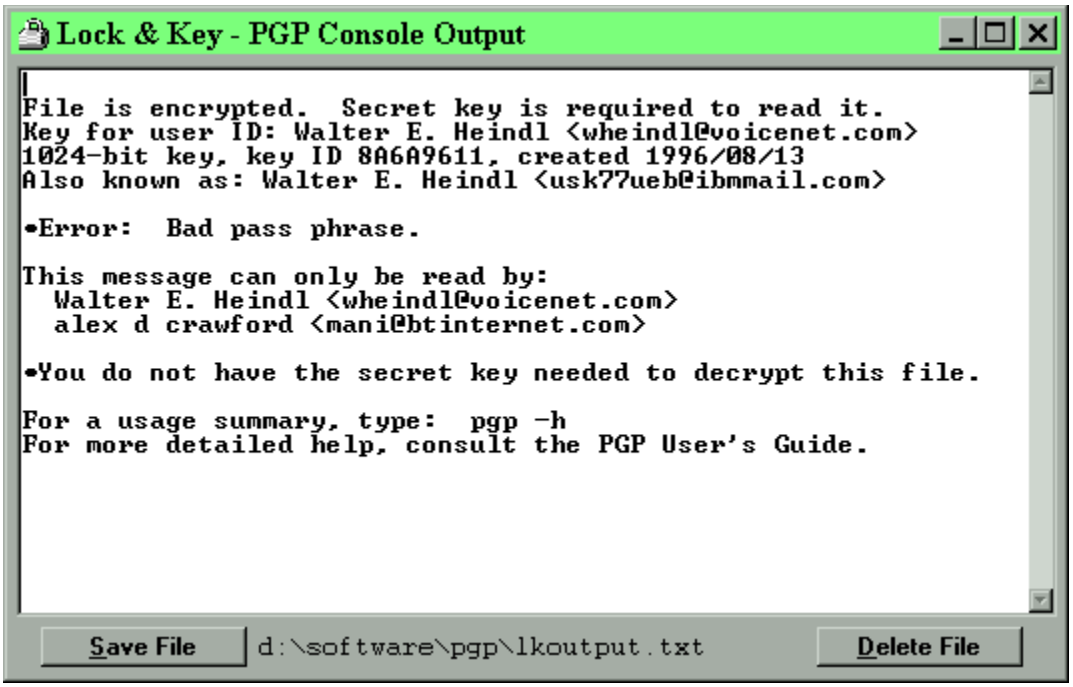
It has been observed that Windows 95 swaps portions of memory to hard disk. While this memory is deallocated by Windows when PGP exits, the data may remain in the Windows 95 swap file even after PGP closes. In theory, this file can be read by an intruder. As a practical matter, this risk should be slight, as (1) Windows 95 does not let other programs (such as a disk editor) access this file while Windows 95 is running; (2) if you have configured Windows 95 to dynamically adjust the size of the swap file, this file is deleted if Windows 95 exits normally; (3) the contents of this file is dynamic; and (4) this file is many megabytes in size and finding a few bytes of data would be difficult. To reduce this risk, it is recommended that you configure Windows 95 to dynamically adjust the size of the swapfile (using the Control Panel System applet) and exit Windows 95 (thus deleting the swap file) before powering down the computer. Note that this security issue is present whenever PGP is run within Windows 95, whether it is run directly from a DOS box or by a Windows-based front end.

Viewing PGP Console Output

LOCK & KEY captures PGP console output. If LOCK32 is unable to create an encrypted file for any reason, or if KEY32 is unable to decrypt a file or perform some other operation, it will report the error:



If you press Yes, you will view the PGP console output in Windows:



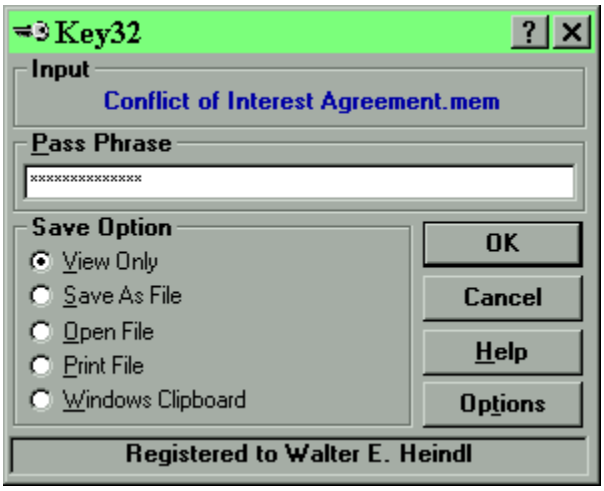
This will let you pinpoint the error. Likely causes include the following:

- The recipient's name does not appear in your public key ring.
- You attempted to sign the file but did not enter the correct pass phrase for your private key.
- You did not properly enter your pass phrase when decrypting the file.
- The file was not encrypted with your public key.

- PGP is not installed correctly.

Key32: Decrypting Files and Messages

Encrypted files have a .PGP or .ASC extension and, after LOCK & KEY is installed, will appear in Explorer with a lock for an icon. To decrypt an encrypted file, simply double-click on that file in Explorer or on the Windows 95 desktop, and KEY32 will be launched.



You may also receive a message encrypted with PGP as plain text. Such a message looks like this:

```
-----BEGIN PGP MESSAGE-----
Version: 2.6.3i

hIwDcCTG46t3n3EBA/4sJq9YiqVlTO1HjFV6guUczxS2IzHWhAoWcmyBQyKuVjWG
ovdWgSQfQttuFlLFEpePbx72zWrWDcPzlzHxmPOEtFuPOA9iu5nVMYi52bcspxw3
GY2ZjDuTKEUkbUb0TOOcnm3tx3+J+kgQQ/+sFWn8/OHNoHpaFt75mKBJFFgw8YSM
A1VrqiqKapYRAQQAgj6Llb+RxiSF1kX2UHm3A6kcR8fIAoqHMfimXj5TMX0rbSmJ
UwFBwuDq1mGc6HbNHnaWIfLvMOj9lS8Dvx+MUBklE4gNsYsup4qvz0U+2yAzQ0DC
wonVggUbzyPbRhjahUHyOU+IdXm43OsUVkqSvRoncfM4ynStK45eMtbMpPemAAAA
cy6KEbmdxCxs8RMg+AxHkPGVqq58xFiqxwizFOOnfpZtIIOtKRjgrghF/PwtDzkP
BJxHmODktRY/d4dyV9Z8afh740OTDPzZWq339Pdb9Oz+Xp4jBFopUwpnRZhXN8ET
TF7hyR8Hgy8ep2Gb5Aem/Pg0J/E=
=/ifs
-----END PGP MESSAGE-----
```

To decrypt such a message, select the message (including the first and last lines), copy it to the Windows Clipboard, and run KEY32.EXE ("Decrypt Clipboard Contents" on the Windows 95 Start Menu).

KEY32 will prompt you for the pass phrase. Enter one of the following:

- If the file was encrypted using your public key, you should enter the pass phrase which unlocks your secret key.

- If the file was encrypted using conventional encryption, you should enter the pass phrase

which was used to encrypt the message.

- If the file is not encrypted (either armored without being encrypted, or plaintext with a signature attached), you do not need to enter anything..

KEY32 will also give you the following choices on what to do with the decrypted output:

- **View the file** using QuickView or QuickView Plus (if installed), or Notepad.

- **Save the file to disk.** If the input source is a file, the file will be saved using the original filename, minus the .PGP or .ASC extension. If the input source was the clipboard and the sender used Lock & Key to preserve the original filename (including a long file name), the file will be saved using that name. You will get a "Save As" dialog box which you can use to specify the folder in which the file will be saved, or to rename the file. If the input source is the clipboard and the sender did not use Lock & Key, you'll be given a "Save As" dialog box to name the file to be saved. If there is an existing file with the same name, Lock & Key will ask you whether you want to overwrite the file (press Yes), rename the file (press No), or skip the file (press Cancel).

- **Open (launch) the file** with the associated application. Note that this option will not be available if the input source was the clipboard. This option is intended for use where LOCK & KEY was used to encrypt the file, and the file was transported with the long file name intact. In this way, the original file's extension is preserved, and Windows 95 uses this information to open the file.

- **Print the file** with the associated application. Note that this option will not be available if the input source was the clipboard. This option is intended for use where LOCK & KEY was used to encrypt the file, and the file was transported with the long file name intact. In this way, the original file's extension is preserved, and Windows 95 uses this information to print the file.

- **Copy the decrypted file to the clipboard** so it can be pasted into an editor or e-mail application. Please note, this option only works with text files. Lock & Key will analyze the output and will place only text files in the clipboard. If you've chosen this option and Lock & Key encounters a binary file, Lock & Key will send the file to QuickView instead.

Error Messages

LOCK & KEY can be configured to write a detailed execution log which can be used to trace errors. To enable this feature, add the following setting to LOCK&KEY.INI:

```
[Common]
Verbose Log=Yes
```

By default, this log will be saved as LOCK&KEY.LOG in the Lock & Key program folder.

If a runtime error occurs, LOCK & KEY will enable this setting automatically and will ask you to retry the operation. If the error recurs, please send this log file to the author at:

Walter E. Heindl, wheindl@voicenet.com

You must choose the name of a **recipient** from the drop-down list of keys in your public key ring.

If you wish to encrypt the message for more than one recipient, do not choose a recipient from the list. Instead, type a portion of the user ID (which must be unique) of each intended recipient, e.g. “Tom Dick Harry”

If “Encrypt To Self” is checked, then all messages will also be encrypted using your own public key, so you can decrypt the encrypted file too.

If this option is checked, then PGP will wipe the unencrypted input file after successful encryption. The file, once wiped, cannot be recovered using conventional file recovery tools. This option should be used with caution, and should not be used if the original file is “read only.”

The **“Binary”** option will cause the encrypted output to be saved as a file in the same directory as the input (source) file. The filename will be the same as the input file, but with the .PGP extension added. Use this option if you plan to transmit the encrypted file via a diskette, or through an e-mail channel capable of handling binary files. Note: If the input source is the Windows Clipboard or the Lock & Key editor, the file will be saved as `C:\OUTPUT.PGP`.

The “Armored” option will cause the encrypted output to be saved as a file in the same directory as the input (source) file. The file will first be converted to a 7-bit format, which can be transmitted through most Internet mail channels. The filename will be the same as the input file, but with the .ASC extension added. Use this option if you plan to transmit the encrypted file via an e-mail channel that is not capable of handling binary files. Note: If the input source is the Windows Clipboard or the Lock & Key editor, the file will be saved as `C:\OUTPUT.ASC`.

The **“Clipboard”** option will cause the encrypted output to be placed in the Windows Clipboard, from which it can be pasted into an e-mail editor. This is the most convenient way to send an encrypted message using Internet mail.

You must select the form in which Lock & Key will save the encrypted output.

The **Binary** option will cause the encrypted output to be saved as a file in the same directory as the input (source) file. The filename will be the same as the input file, but with the .PGP extension added. Use this option if you plan to transmit the encrypted file via a diskette, or through an e-mail channel capable of handling binary files. Note: If the input source is the Windows Clipboard or the Lock & Key editor, the file will be saved as `C:\OUTPUT.PGP`.

The **Armored** option will cause the encrypted output to be saved as a file in the same directory as the input (source) file. The file will first be converted to a 7-bit format, which can be transmitted through most Internet mail channels. The filename will be the same as the input file, but with the .ASC extension added. Use this option if you plan to transmit the encrypted file via an e-mail channel that is not capable of handling binary files. Note: If the input source is the Windows Clipboard or the Lock & Key editor, the file will be saved as `C:\OUTPUT.ASC`.

The **Clipboard** option will cause the encrypted output to be placed in the Windows Clipboard, from which it can be pasted into an e-mail editor. This is the most convenient way to send an encrypted message using Internet mail. If the **Include My Public Key** option is checked, your public key will be appended to the message, so the recipient can verify your signature or send an encrypted response.

Use **conventional encryption** to encrypt the file or message using conventional (single key) encryption. You must enter a **pass phrase** here which will be used to encrypt and to decrypt the file or message. Use this option if the recipient has PGP but you do not have the recipient's public key, and if you can transmit the pass phrase to the recipient by secure means.

Use this option if you do not wish to encrypt the file. This option is valid only in the following cases:

- You are choosing to use ASCII armoring (Output options Armored or Clipboard) to encode the file for transmission over mail channels that do not support sending binary files.
- You wish to add your signature without encrypting the file.

This causes the **Lock & Key integrated editor** to appear. Use this editor to compose a text message for encryption using PGP. The editor supports Windows keyboard shortcuts for cutting, copying and pasting text.

Displays the file or data which will be decrypted. If a file was specified, this will be the file name, minus the .PGP or .ASC extension. If no file is specified, KEY32 assumes that there is encrypted data in the Windows Clipboard.

If the file or message was encrypted with your public key, you must enter the **pass phrase** which unlocks your secret key. If the file or message was encrypted with conventional encryption, you must enter the pass phrase which was used to encrypt the message.

If QuickView/QuickView+ is installed, the decrypted file will be opened in QuickView. You can use QuickView to view or print the file or to copy file data to the Windows Clipboard. If QuickView is not installed, the decrypted file will be opened in Notepad.

This option will cause the decrypted output to be saved as a file, in the current directory, with the filename shown in blue. If KEY32 is decrypting data in the Windows Clipboard, the file will be saved as `c:\output`.

This option will cause the decrypted file to be printed by the associated application. This option will only work properly if the correct extension is included with the filename above. (If LOCK32 was used to encrypt the file, the original filename and extension is preserved.) This option will be unavailable if data in the Windows Clipboard is being decrypted. However, you can still use QuickView to print the file (if you have QuickView installed) by selecting the View option.

KEY32 gives you the following choices on what to do with the decrypted output:

- **View** the file using QuickView or QuickView Plus (if installed), or Notepad.
- **Save** the file to disk. If the input source is a file, the file will be saved using the original filename, minus the .PGP or .ASC extension. If the input source was the clipboard, the file is saved as `C:\OUTPUT`.
- **Open** (launch) the file with the associated application.
- **Print** the file with the associated application.

The Open and Print options will only work if the filename (shown) contains an extension associated with an application in Windows 95. These options will not be available if the input source was the clipboard.

When installing LOCK & KEY, you are asked to choose a language. This language will be used for displaying labels in the LOCK & KEY dialog boxes, and for message boxes. This language preference is stored in the Registry and can be most easily changed simply by reinstalling LOCK & KEY. The language text is stored in GLOSSARY.INI in the PGP directory and can easily be modified to support additional languages. See the Lock & Key User Guide for details.

Lock & Key lets you view decrypted files with **QuickView** or **QuickView Plus**, if these are installed. These are file viewers that let you view various wordprocessing, spreadsheet, graphic and other files without using the application which created them. This is an especially convenient means of decrypting and viewing files in a single step. If Lock & Key can't find QuickView or QuickView Plus, it will offer to let you view decrypted files in Notepad.

If you answer **Yes**, the author's public key will be added to your public keyring, which means you will be able to send encrypted messages to the author. You do not need to answer Yes if you have installed Lock & Key previously and have already done this step.

Answer **Yes** if you wish to view the Lock & Key user guide (a Windows Help file) now. If you answer **No**, you can view the User Guide by pressing the **Help** button in Lock & Key, or by selecting the Start Menu shortcut.

If this option is checked, your public key will be appended to the encrypted message which is placed in the Windows Clipboard. This will enable the recipient to verify your signature (if you've added your "electronic signature"), or to encrypt a reply using your public key. This option is available only if you have chosen the Windows Clipboard output option. The user name will be your name shown in the Signature box. If no user name is shown, press the Select button and choose a user name.

LOCK & KEY is shareware. The shareware version is fully functional but includes a time delay. Registration will remove this delay. To register LOCK & KEY, send $19.95 to:

Walter E. Heindl
271 Misty Patch Road
Coatesville, PA 19320 USA

Please provide your e-mail address. You will be sent a personalized password file which will remove the time delay. The password file will work with future versions of LOCK & KEY, making upgrades free.

You may now register online via CompuServe SWREG. From CompuServe, GO SWREG for details. Registration number is 12438.

Public key cryptography uses the public key of a specific recipient to encrypt the message, which can then only be decrypted by that person using his or her secret key. This is the normal method of operation of PGP and provides the greatest security, since the recipient's secret key is necessary to decrypt the message. The public key, however, can be freely distributed.

Use conventional encryption to encrypt the file or message using conventional (single key) encryption. You must enter a pass phrase here which will be used to encrypt and to decrypt the file or message. Use this option if the recipient has PGP but you do not have the recipient's public key, and if you can transmit the pass phrase to the recipient by secure means.

You may also choose not to encrypt the file by selecting none. This option is valid only in the following cases:

- You are choosing to use ASCII armoring (Output options Armored or Clipboard) to encode the file for transmission over mail channels that do not support sending binary files.
- You wish to add your signature without encrypting the file.

Lock & Key

Windows 95 Explorer PGP Interface

Version 4.0.0 – June __, 1997

Mail: **wheindl@voicenet.com**

http://www.voicenet.com/~wheindl/lock&key.htm

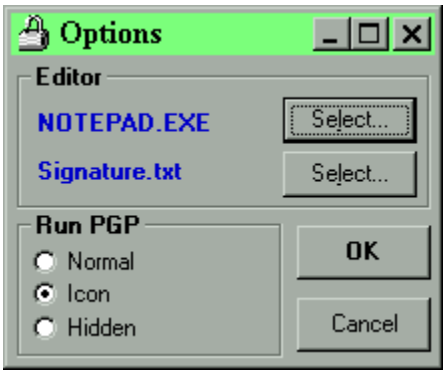
Lock32: Composing Messages

You can compose a message to be encrypted by PGP, without leaving Lock & Key. By default, Windows Notepad is used for composing messages. However, you can configure Lock & Key to use any external program as an editor (e.g. WordPad, MS Write, your word processor or favorite text editor). You can even use another type of program (such as a spreadsheet or a graphics program) if that's what you need.

NOTE: Version 4.0 of LOCK & KEY lets you compose and send encrypted messages directly using KeyChain. This is the fastest and easiest way to compose and send an encrypted message using any public key in your keyring, in a single operation. KeyChain features a message editor specially designed for encrypting messages, including both encrypted and unencrypted sections, appending your public key, signing the message using your secret key, and using your public key ring as an address book. This feature requires a compatible Internet mail program, e.g. Eudora (Lite or Pro, version 3.0) or Pegasus Mail. For more information on this feature, press here.

A very powerful feature is the ability to specify a template file. This feature is much like an e-mail signature file: you can include letterhead or reply information, a saying, or any other data at all that you'd like to include within encrypted messages.

To choose an editor or a template file, press the "Options" button. This will bring up the following dialog box:



Press either "Select" button to choose an editor or a template. Please note, the program will look first to your Windows directory for the editor, and to the \Windows\ShellNew directory (where template files for the Explorer "New" menu are stored) for the template file. You may, however, browse to any directory for either the editor program or the template file.

Please note that the template file should be usable with the editor program. If your editor is a simple text editor, the template file should be a text document (blank or with a signature included). If your editor is a wordprocessor such as WordPad, the template should be a file that was created with that program. The same is true if you choose to use a spreadsheet or a graphic program as an editor; e.g. to use a spreadsheet as an editor, save a worksheet (blank or with

standard data) in the \ShellNew folder, and select that as a template.

To compose a message, simply press the "Compose" button. Your template file will be copied and the selected editor will be launched. When you're done working on the file and are ready to encrypt it, simply exit the program (be sure to save the file!), choose your recipients and encryption options, and press OK. Lock & Key will then encrypt the file which you've just created.

Lesson 3: Creating Your Own Key Pair

The first step in using PGP is to create your own public-private key pair. If you're already familiar with generating keys, you can skip this lesson.

First, click here to launch KEYCHAIN, LOCK & KEY's key management module. Or you can press the Windows 95 "Start" button, select Programs | Lock & Key | Key Management. This will launch KEYCHAIN. Note that the program has two tabs, one for your public "key ring" (all of the public keys you've collected), and one for your secret "key ring" (one or more secret keys).

If you chose to add the author's key when you installed LOCK & KEY, you'll see the author's key (Walter E. Heindl) in your key ring. There may be others as well.

Click on the "Secret Keyring" tab. This window will show any existing secret keys. If you've never generated a key pair, this window will be empty.

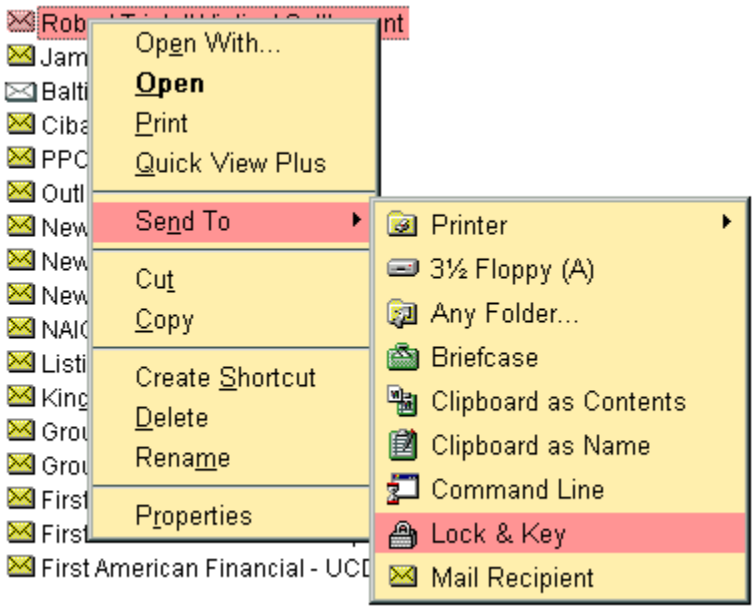
Now, with the secret keyring visible, select Key | Generate Key Pair from the menu (or press Ctrl-G). This will launch PGP in a DOS window, since key generation must be done interactively. Follow the directions in the DOS window. You will first be asked to specify a level of security. Most users will choose the highest level. You will then be asked to specify a user name (how your name will appear to those using your public key). It is customary to specify your name followed by an Internet mail address, e.g. Joe Doakes <jdoakes@anydomain.com>. You will then be asked to enter a pass phrase. This should be from 1 to 30 characters long. You'll need to remember this pass phrase in order to use your secret key to add signatures or decrypt messages. You'll then be asked to re-enter the same pass phrase (to protect against typing errors). Finally, PGP will ask you to type some random keystrokes.

When PGP finishes, it will exit, and your new key pair should be visible in both the Public Keyring and Secret Keyring.

Press here to continue with the next lesson.

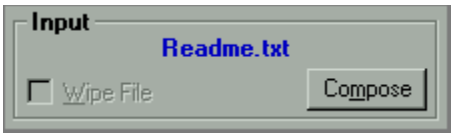
Lesson 4: Encrypting A File

To begin this lesson, press here to open a folder in Explorer. Now, click on any file. It doesn't have to be a text file – it can be a wordprocessing document, a spreadsheet, or a graphic file. When you have highlighted the file, right-click (press the right mouse button), choose "Send To," and choose "Lock & Key."



This should cause the main Lock & Key window to appear.

Notice that the name of the file you selected is shown under "Input." (Please make sure the "Wipe File" box is NOT checked. If that box is checked, the original file will be deleted after it is encrypted. That's an advanced feature we're not ready to try yet.)



You can choose several options in this window. First, you will need to make sure that "Public-Private Key" encryption is selected under Encryption Method.

Second, click the arrow next to the Recipients box. This will reveal a drop-down list of the public keys in your public key ring. At a minimum, this will include your own public key. It will also include the author's, if you chose to add the author's public key when you installed LOCK & KEY. Choose any name from this list. That person's public key will be used to encrypt the file – meaning that only this person (using his secret key) will be able to decrypt it. (Be sure to check the box that says "Encrypt Copy to Self." This will let you decrypt any message you've encrypted, using your own secret key.)

You will also need to choose the output form of the encrypted file. You can choose binary, which will save the encrypted file to disk. You can choose armored, which will save the encrypted file to disk in a format that doesn't include extended characters – the file will be slightly larger, but can be more easily sent by Internet mail. Or you can choose to save a step and have the encrypted file placed in the Clipboard, allowing you to paste it into an e-mail message. For this lesson, choose Binary.

Finally, make sure the box under Signature is NOT checked. We'll use that in a later lesson.

When you're done, press OK. LOCK & KEY will now run PGP in the background, processing the file. You'll know it is done when the lock snaps shut. If there is any error, you'll get an

error message.

Now, look at the Explorer window where you first selected the file. You should see a new file in this folder – it will have the same name as the original file, but with the .PGP extension added. You'll know it is an encrypted file because of the icon (a lock). This is the encrypted file. (If you'd like to see what an encrypted file looks like "on the inside," and if you have QuickView installed, right-click on that file and choose QuickView.)

Please leave this Explorer window open and click here for the next lesson.

Lesson 5: Decrypting A File

Now we will use LOCK & KEY to decrypt the file which we just encrypted.

If you did not leave the Explorer window open after the last lesson, click here to reopen it. Make sure the Explorer folder containing the encrypted file is visible, and double-click on the encrypted file (it will have a lock for an icon). This will launch KEY32, the module which uses PGP to decrypt files. KEY32 inspects the file to determine whether it is an encrypted file or a public key. If it is a public key, you will receive a message prompt identifying the key and asking if you'd like to add it to your public key ring. Since this was an encrypted file, however, you will instead see the main KEY32 window:

The KEY32 window is very simple. Notice that the name of the encrypted file is shown. There is also a box for entering your secret key's pass phrase. Type in your pass phrase. This is needed so your secret key can be used to decrypt the file.

You are also given five choices as to what to do with the file after it is decrypted. You can save it as a file; you can open it in the associated application (for example, to open a spreadsheet in the spreadsheet program); you can print it; you can copy it to the Windows Clipboard (if it is text); or you can view it with QuickView (if it is installed on your system).

If you have QuickView installed, select View. Otherwise, select Open. Then press the OK button. LOCK & KEY will then run PGP in the background. You'll know it is finished when the lock snaps open. Then, you should see QuickView (or the application that created the file) display the file.

When you're done with QuickView, close it by clicking on the "X." KEY32 is waiting silently in the background and will safely delete the decrypted file.

Click here to go to the next lesson, where we'll learn how to compose a message and add an electronic signature.

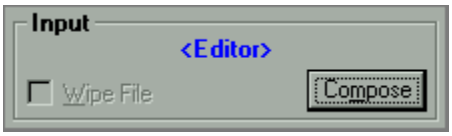
Lesson 6: Composing And Signing A Message

Now we will use LOCK & KEY to compose a new message, encrypt that message, "sign" that message, and prepare it to be sent to another user.

First, run LOCK32 by clicking on the Windows 95 "Start" button; choose Programs, Lock & Key, Run Lock & Key. Or you can press here.

Next, press the "Compose" button. This should launch Notepad with a blank document. (You can press the Options button and choose a different editor, as well as a template file, but for now let's work with Notepad.) Type a brief message in Notepad. When you're finished, close Notepad by clicking on the "X." Be sure to answer Yes when you're asked to save the file.

Note that the LOCK32 window now shows that the editor was used to compose a message.



Click on the Recipients arrow and choose a recipient from the drop-down list. Again, make sure that Encrypt Copy to Self is checked; otherwise, you won't be able to decrypt the message yourself.

This time, under Output, choose Windows Clipboard. Check the box that says Include My Public Key. This will add your public key to the message, so that the recipient can send you an encrypted response.

Now, check the box that says Include Signature.

The program will read the name of your "default" user name for making signatures, if one exists. If this is blank, press the "Select" button. This will give you a drop-down list of secret keys (you may have more than one). Pick one to use for making signatures and press OK.

You will need to type in your pass phrase in order to make an electronic signature. After you've

done this, press OK. LOCK & KEY will encrypt the file, copy the data to the Windows Clipboard, and add your public key.

You can then switch to your mail program and paste this into an electronic mail message. For now, press here to run Notepad and we'll pretend this is your mail program. Type Ctrl-V (or select Edit, Paste) to paste the data. You'll see what an encrypted message looks like. Scroll down and you will see your public key.

Be sure to keep Notepad open! Click here to go to the next lesson, where we'll decrypt this message.

Lesson 1: PGP – What's It All About?

PGP stands for "Pretty Good Privacy." PGP is a widely available, freeware, DOS-based cryptography program which has become an international standard for high security cryptography. Because it is widely available, it is a logical choice for secure messaging not only within an organization, but with others as well.

PGP uses a technique called public-private key cryptography. To understand what this means, and why this provides greater security, it helps to understand a little bit about conventional cryptography. Conventional cryptography uses a single "key" (which is usually a secret phrase) to encrypt the data. The cryptography program uses a formula, or algorithm, to process the data using this key. The result can only be deciphered by someone with the same cryptography program and the same key.

The security risk with conventional cryptography is that the key itself must be transmitted by a secure means, and kept confidential. Anyone who can gain possession of this key can decipher any message encrypted using that key.

Public-private key cryptography solves this problem by creating a matched pair of keys. A message encrypted with one can only be decrypted with the other, and vice versa. Because two keys are required, one of the keys (called a public key) doesn't need to be kept secure. In fact, it can be publicly posted on a BBS. The other key (called a secret key) does not need to leave the user's system, so it can be kept secure. The secret key itself requires a pass phrase known only to the user.

Public-private key encryption provides for two related uses. First, the sender can use the public key of another person to encrypt a message to that person. Since this message can only be decrypted with the matching secret key, only the intended recipient can read the message.

Second, the sender can use his own secret key to encrypt a message. Anyone who can obtain the sender's public key can read the message. While this doesn't provide for security, what it DOES provide is proof to the recipient that the message actually came from the sender. This is the basis of so-called "digital signatures."

The two methods can be combined. A sender can encrypt a message using the recipient's public key, and "sign" it using his own secret key. The recipient then uses his own secret key to decrypt the message, and the sender's public key to verify that it was "signed" by the sender. This technique forms the basis of secure commerce over the Internet.

The main weakness of PGP is that it is a DOS-based program, with an obscure command-line syntax, which is difficult to learn and use. LOCK & KEY overcomes these limitations by letting you access PGP's functions without leaving Windows. This tutorial will show you how to use LOCK & KEY, and PGP, to create your own public-private key pair, to encrypt messages, to decrypt messages, to sign files, and to view signatures. This tutorial assumes that you have installed PGP and LOCK & KEY, but does not assume you've ever worked with PGP before.

If you do not have PGP, or have not installed it, please read the next lesson concerning installation of PGP and Lock & Key. If you have installed PGP, you can skip ahead to lesson 3.

Lesson 7: Decrypting An E-Mail Message

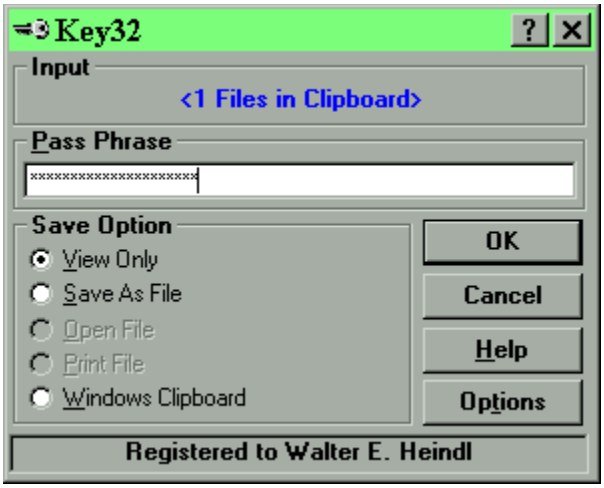
This lesson will show you how to decrypt an encrypted e-mail message, and to verify that it was signed. You should have Notepad open from the previous lesson. The Notepad window should contain the message which you encrypted in the last lesson, and also the public key of the user who sent it.

First, select all the text in the Notepad window. You can do this easily by selecting **Edit | Select All** from the menu. Then, copy this text to the Windows clipboard by pressing Ctrl-C or by selecting **Edit | Copy** from the menu.

Second, press here to run Lock & Key. Lock & Key will recognize that the Windows clipboard contains an encrypted message, and will launch KEY32, the Lock & Key decryption module. KEY32 will "read" the clipboard data, finding any encrypted messages, signatures and public keys present. Since the message we've just encrypted included your public key, you will first be prompted whether you want to add this public key to your key ring.

If you did not already have this key in your public key ring, you could press Yes to add the key.

The KEY32 main window will now appear, which this time will show that there is encrypted data in the clipboard:



Again, you will need to enter your PGP pass phrase, and select the desired option for what to do with the decrypted data. (Note that the Open and Print options are greyed out. This is because Lock & Key requires an input file name in order to tell which application to use to open or print the file.) Select View and press OK. KEY32 will run PGP in the background. KEY32 monitors the PGP output, checking for signatures. Since the message we're using was signed, you should receive a message indicating this:

Click OK and in a moment the decrypted message will appear in QuickView.

This covers the basics of how to use Lock & Key with PGP to encrypt and decrypt files and messages, how to generate key pairs, how to add keys to your keyring, how to sign messages and how to read signatures. Advanced topics are covered in the reference section of this user guide. You can click here to learn more about any of these topics.

How to extract keys from the public key ring
How to remove keys from the public or secret key ring
How to view the fingerprint of a key
How to choose which secret key to use for making signatures
How to select which editor and template file will be used for composing messages

Use this option to extract the highlighted public key to a binary file. This is usually preferred only for transmitting keys on disk.

Use this option to extract the highlighted public key to an armored ASCII file. This is usually preferred for transmitting key files through electronic mail.

Use this option to extract the highlighted public key and to copy it to the Windows Clipboard. This is a convenient way to paste a public key into an e-mail message. (PLEASE NOTE: LOCK32 lets you automatically append your own public key to any message in a single operation.)

Use this option to remove the selected key from the public or secret keyring. Please note that this operation cannot be undone, so you may want to extract the key to a file first.

Use this option to generate a new matched public-secret key pair. This choice will run PGP interactively. Follow the PGP screen prompts to choose a level of security, a user name, and a pass phrase.

This option causes the selected secret key to become the default secret key for making signatures. This is useful if you have more than one secret key. This setting can also be changed in LOCK32.

This option displays the 16-byte "fingerprint" for the selected key. You can and should use this to verify the authenticity of a public key sent to you from an insecure channel. You can, for example, speak on the telephone to the sender and ask the sender to read his key's "fingerprint." You can display the "fingerprint" of your own secret key so you can confirm your key's authenticity to someone who has received your public key.

This tab shows a list of all public keys which have been added to your public keyring. You can choose any key in this list, and right-click to pop up a list of available commands (such as extracting or removing the key from the keyring).

This tab shows a list of all secret keys which are present in your secret keyring. You can choose any key in this list, and right-click to pop up a list of available commands.

Checking this option will cause the original filename to be appended to the clipboard output. If the recipient is using Lock & Key, the file will be automatically saved with the original filename. If the recipient is not using Lock & Key, the recipient can use this information to identify the file. This option supports Windows 95 long file names.

Use this to set Lock & Key options for the **editor** and the **template file** which will be used for composing messages using LOCK32; and for setting whether to run PGP in a **normal** window, **minimized** or **hidden**.

This dialog shows the editor program and the template file which will be used for composing messages. You can use any text editor, word processor, or even a spreadsheet or graphics program. The template file can be a blank file of the type associated with the editor (e.g. a blank WordPad document) or can include standard information, such as a letterhead, a form, or a signature. Template files are located by default in the \Windows\ShellNew folder.

This dialog shows whether PGP will run in a normal window, minimized or hidden. It is suggested that you run PGP minimized, so that the window can be inspected if an error occurs. Please note: Windows 95 users may need to edit the properties of RUNPGP.PIF (in the PGP folder) if they wish to run PGP in a normal window.

This option causes the decrypted output to be placed in the Windows clipboard. Please note, this option only works with plain text files. If any binary files are included in the output, you will be prompted either to skip those files or view them with QuickView. If you decrypt more than one file, all will be appended to the clipboard.

KeyChain: Generating Key Pairs

KEYCHAIN makes it easy to create new public-private key pairs using PGP. Please note, generating keys using PGP requires interacting with PGP. However, KEYCHAIN invokes PGP with the necessary parameters, and provides confirmation when complete that the key has been generated.

To generate a key pair, first make sure that the secret keyring is visible by clicking the secret keyring tab. Then, select Key | Generate Key Pair to launch PGP. PGP will first ask you to select the degree of security which the key will provide, ranging from 1 (commercial grade) to 3 (military grade).

You will then be asked to specify a user name (how your name will appear to those using your public key). It is customary to specify your name followed by an Internet mail address, e.g. Joe Doakes <jdoakes@anydomain.com>.

You will then be asked to enter a pass phrase. This should be from 1 to 30 characters long. You'll need to remember this pass phrase in order to use your secret key to add signatures or decrypt messages. You'll then be asked to re-enter the same pass phrase (to protect against typing errors). Finally, PGP will ask you to type some random keystrokes.

When PGP finishes, it will exit, and your new key pair should be visible in both the Public Keyring and Secret Keyring.

You may have more than one secret key. If you do, however, you will need to specify which secret key should be used for making signatures. This can be done by selecting any secret key in the secret keyring list, and choosing Key | Make Default (or press Ctrl-D) to select this key for making signatures. (NOTE: You can also change the secret key for making signatures in LOCK32.)

KeyChain: Extracting Keys

Once you've created a key pair, you'll need to send the public key to others so that they can send encrypted messages or files to you, and so they can verify any signatures which you've made using your secret key. You may also occasionally find it necessary to extract another user's key. NOTE: While it is theoretically possible to extract secret keys, only public keys should be distributed; so this feature works only while the public keyring is visible.

To extract a key, make sure the public keyring is visible by clicking the public keyring tab. Select the key you want to extract, and then activate the Key menu on the menu bar or by right-clicking on the desired key.

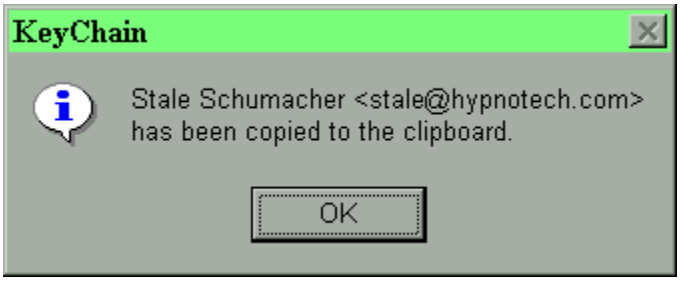
KEYCHAIN provides for three different ways to extract a key: as a **binary file**, an **armored file**, or by copying the key to the Windows clipboard.

- A binary file is a disk file which uses 8-bit encoding (special characters). Since many Internet mail transports can't handle binary files, these are usually preferred if the extracted key will be delivered on a disk. Binary key files have the extension .PGP.

- An armored file is a disk file which uses 7-bit encoding (text characters). Generally, armored files are slightly larger than binary files, but they can more easily be transported by Internet mail. Armored key files have the extension .ASC.

In either case, KEYCHAIN will prompt you for a filename to save the extracted key using a standard Windows 95 dialog box.

KEYCHAIN can save a step by extracting a key (in armored format) to the Windows clipboard. This allows you to paste the key directly into an e-mail message.



Please note that LOCK32 can automatically add your public key to a message encrypted to the clipboard, in a single operation.

KeyChain: Default Signature

It is possible to have more than one secret key. You might, for example, use one secret key for business use and one for personal use, each with a different user name or e-mail address. If you have more than one secret key, however, PGP needs to know which one should be used for making signatures. By default, this is the last key created, but this can easily be overridden.

To choose a secret key for making signatures, first make sure the secret keyring is visible by clicking the secret keyring tab. Then, choose Key | Make Default (or press Ctrl-D) to select this key for making signatures.

The default secret key is stored in the PGP configuration file, PGP.INI or CONFIG.TXT, under the keyword `MyName=`. This choice will affect the operation of PGP run independently of LOCK & KEY.

NOTE: You can also change the secret key for making signatures in LOCK32.

KeyChain: Removing Keys

KEYCHAIN provides a convenient way to remove keys from either the public or secret keyrings. You may, for example, if your keyring gets too large, want to remove public keys of users that you don't correspond with. You may also want to remove a secret key that you no longer use and have revoked.

To remove a key, select the key in either the public or the secret keyring; then choose Key | Remove (or press Ctrl-R). The keyring lists will be updated to show the change.

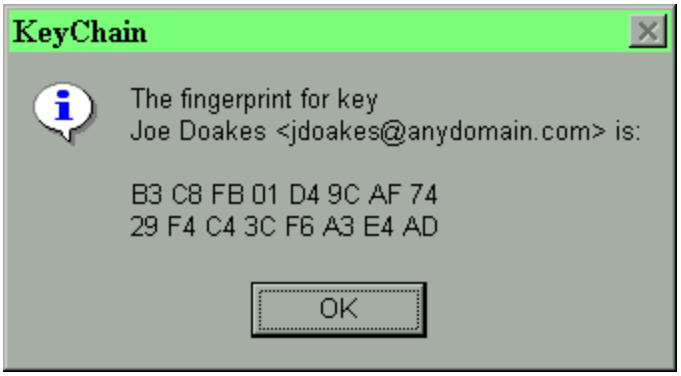
NOTE: Some PGP keys may be given more than one user name by their owner. Such a key cannot be removed automatically. If you try to delete such a key, KEYCHAIN will recognize this and offer to run the command interactively. You will be prompted by PGP whether to remove only selected usernames, or the entire key.

KeyChain: Viewing Fingerprints

Suppose you receive a public key by e-mail. You want to use that public key to encrypt a message that can only be read by the username shown on the key. Or you want to use that public key to verify that the signature on a message is authentic. How do you know that the public key in fact came from that user? If the key is forged, you might send a private message encrypted with that key, and the forger will be able to read it.

PGP provides a means of authenticating keys. Every key has a "fingerprint," a series of 16 bytes that identifies the key and protects against forged keys. If you want to check the authenticity of the key, contact the person who sent it to you, and ask that person to read the key's fingerprint. Assuming you know for sure you are speaking to the right person, this provides a trustworthy means of making sure the key is authentic.

LOCK & KEY can display the fingerprint of any key in the public or secret keyring. Simply select Key | View Fingerprint (or press Ctrl-F). LOCK & KEY will display the fingerprint of the key:



Note that you can use this feature in both the public keyring (to have a public key verified) and the secret keyring (to verify your key for someone else). Note that both the public key and the secret key of a keypair have the same fingerprint.

Lock32: Input Source

LOCK32 will display the name of the input file (or as much as will fit) in this box. If you are running LOCK32 without a filename, LOCK32 will encrypt the contents of the clipboard, in which case this box will read "<Clipboard>."

If you check the "wipe file" box, LOCK32 will cause PGP to erase the original un-encrypted file. This option will be greyed if the input source is the clipboard. NOTE: To avoid inadvertently deleting files, this option is not saved between uses but must be selected each time LOCK32 is run.

Pushing the "Compose" button opens a customized signature template in a user-selected editor. If no choices have been made (by pushing the Options button), Notepad is opened with a blank file. For more information on this feature, see Lock32: Composing Messages.

Lock32: Encryption Methods

LOCK32 supports both encryption methods used by PGP: public-private key cryptography and conventional (single key) cryptography.

Public key cryptography uses the public key of a specific recipient to encrypt the message, which can then only be decrypted by that person using his or her secret key.

Conventional cryptography involves using a single pass phrase to encrypt the message. This pass phrase must be known to both the sender and the recipient. This method is less secure than public-private key cryptography, as the pass phrase could become known to others unless it is securely transmitted. Nevertheless, this method makes it possible to send encrypted messages to persons who do not have public keys available.

You may also choose "none." This will only be a valid choice in the following situations:

- You wish to "armor" the file (convert a binary file to 7-bit encoding, so that it may be transmitted through mail channels which do not support binary files).
- You wish to sign the file, but want to keep the file as plaintext so it can be read without PGP.

Simply select which of the three options you wish to use. Note that if you choose the option of conventional encryption, the "Recipients" section is changed to a box for entering the secret pass phrase. If no encryption is selected, both the recipients box and the pass phrase are greyed.

LOCK32 remembers your preferences between uses.

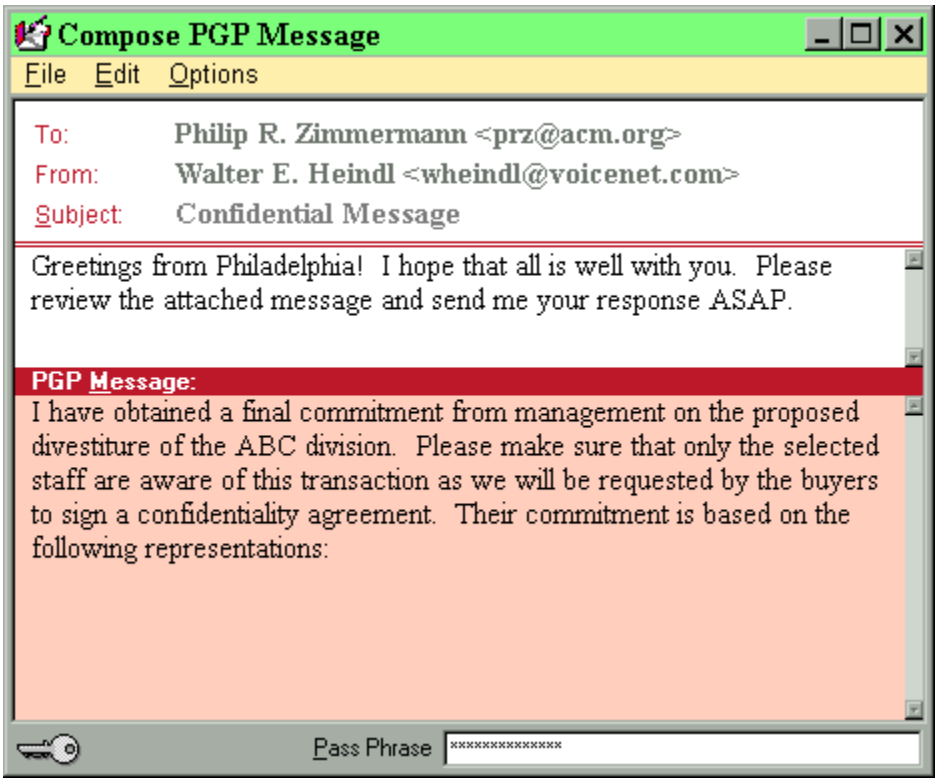
Troubleshooting

When I run PGP in DOS, it reports "CONFIG.TXT: unknown keyword: [Lock." What is the cause of this message, and should I be concerned?

When LOCK & KEY is first installed, it adds the line "[Lock & Key]" to the beginning of the CONFIG.TXT or PGP.INI file. This is necessary in order for LOCK & KEY to safely read/write settings from this file using Windows .INI file functions. While a side effect of this is that PGP reports the above message, the message is harmless and PGP runs normally.

KeyChain: Composing Messages

If you have a compatible Windows Internet Mail program installed, you can compose an encrypted message directly in KeyChain. To activate this feature, right-click on any public key and choose Compose Message from the menu, or press Ctrl-M. This will cause the KeyChain message editor to appear.



The KeyChain message editor includes a number of features especially tailored for creating encrypted messages:

- You can use your public key ring directly as an address book. (Note that each address must specify a valid Internet mail address; this is standard form for PGP public key names.)

- The editor includes a window for composing an un-encrypted section, which can be used for personal greetings or instructions concerning the message.

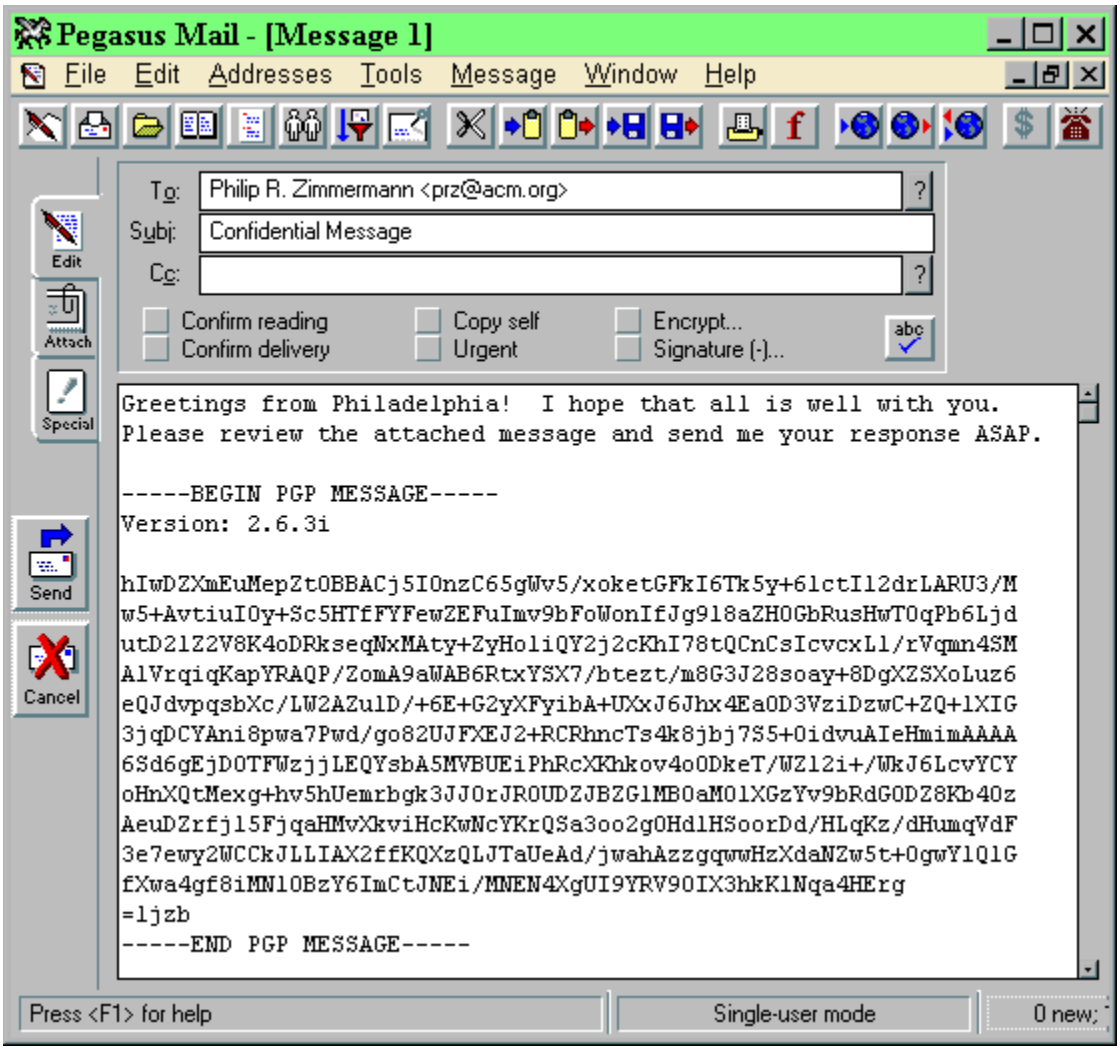
- The bottom portion of the editor (shaded) is the encrypted section. Anything typed in this section will automatically be encrypted using the recipient's public key.

- You can automatically append your public key to the message, to allow the recipient to send an encrypted response or to read your electronic signature. This setting can be activated from the Options menu, or by pressing Ctrl-K. Note that a key is visible in the bottom line of the editor when this option is enabled. This setting is remembered

between uses.

- You can sign the message using your secret key. This setting can be activated from the Options menu, or by pressing Ctrl-S. If this option is not enabled, the pass phrase box in the bottom line will be grayed. Note that the signature used will be based on the secret key of the sender. If you have more than one secret key, the default secret key will be used. You can change the default secret key using KeyChain; press here for more information.

When you are finished composing your message, press Ctrl-E (Encrypt), or press Alt-F4 and answer Yes when asked if you would like to encrypt the message. The message will be encrypted and your Internet mail program will be activated to queue the message for delivery.



Please note the following considerations when using this feature:

- This feature requires an Internet mail program that can process formatted text messages from the command line. Eudora (Lite and Pro) 3.0 and Pegasus Mail are known to

support this feature. The feature is not supported by CyberCreek Mail Express.

- The installation program looks for a compatible Internet mail program by searching the Registry to see which mail program has "hooked" the Mailto url. (This would be the e-mail program that is called by default when you click an e-mail link in your browser.) The program will report whether it has found a compatible program and will record the settings in LOCK&KEY.INI (in the Lock & Key folder).

  You can override the settings by editing LOCK&KEY.INI directly. Here are the settings to make or modify:

```
[KeyChain]
MailProg=Pegasus Mail
MailPath=d:\Internet\Pegasus\winpm-32.exe -j
```

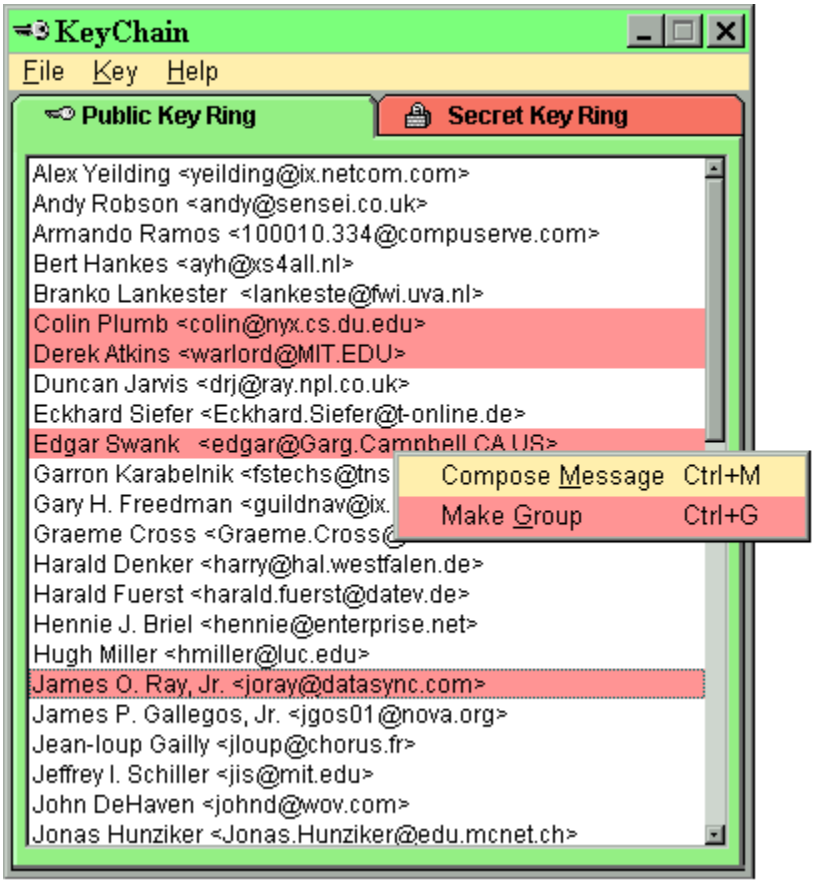
  The MailProg entry is simply the name of the mail program that will be reported in message boxes and can be set to anything. The MailPath entry must contain the full path of the compatible Internet mail program. **Important:** if Pegasus Mail is your Internet mail program, you must include -j at the end of this entry. You should not include this switch if your Internet mail program is Eudora.

Managing Groups of Keys

KEYCHAIN features the ability to create and manage named groups of keys. You can, using KEYCHAIN's message editor, compose a message for a named group, and each member of the group will be able to decrypt the message. Moreover, key groups will also appear in LOCK32's drop-down recipient list box, so you can use LOCK32 to encrypt files for an entire group.

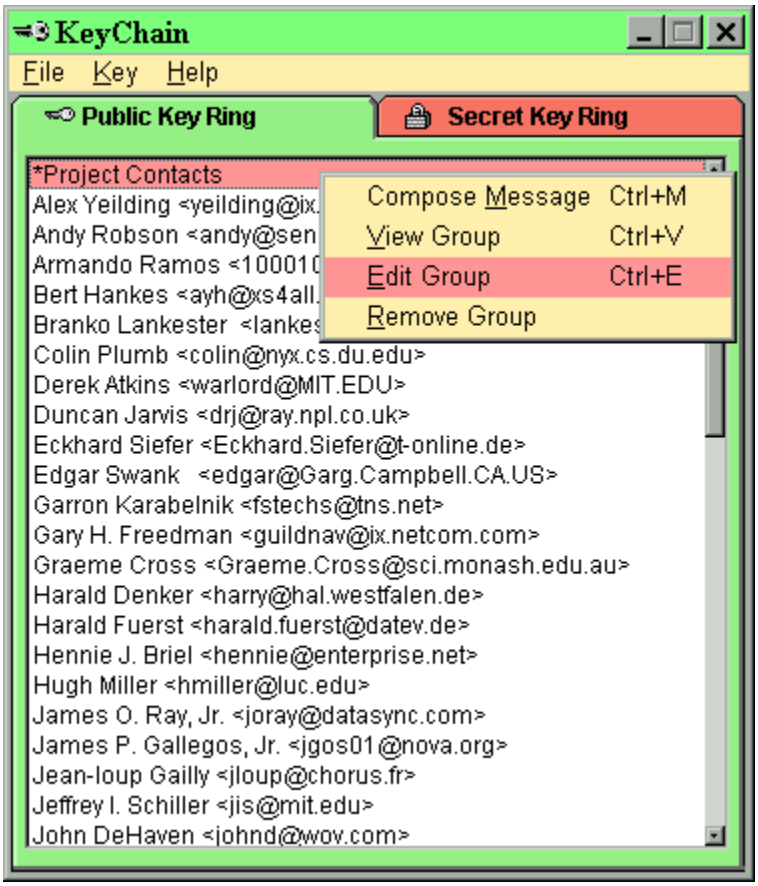
Please note that Lock & Key uses the unique key ID of each key to send key information to PGP. Each key therefore requires 11 characters. The DOS command line is limited to 127 characters, some of which is required for the rest of the PGP commands. As a result, this group feature works best with smaller groups of up to about six persons.

To create a group, open the KEYCHAIN window, and select the keys you want to include. As in any Windows application, press and hold Shift and use the arrow keys to select consecutive keys; press and hold Ctrl while clicking individual keys to select nonconsecutive keys.

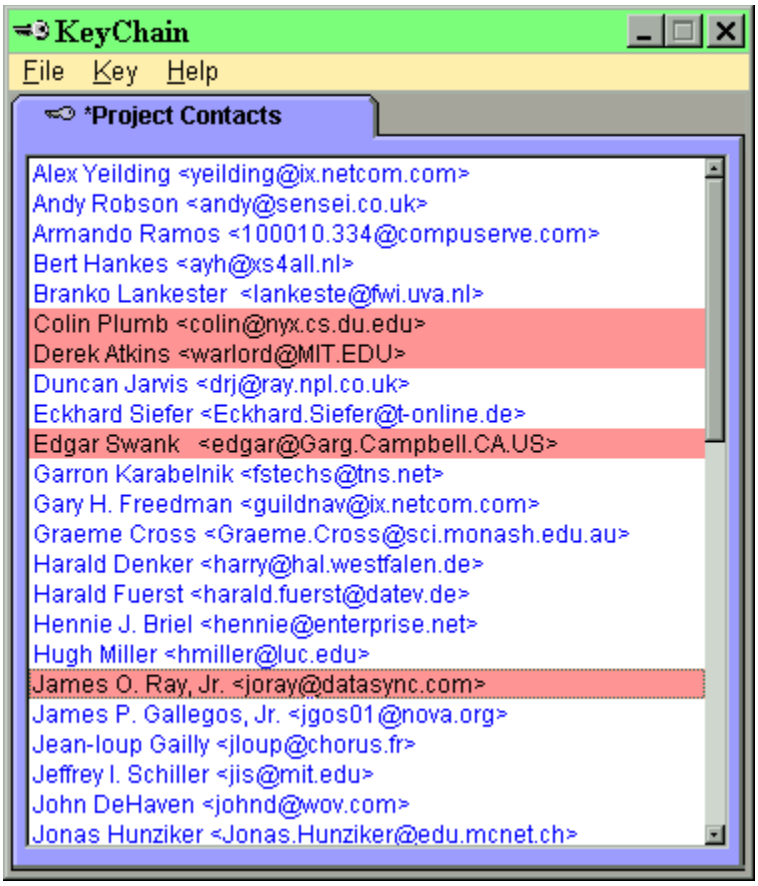


Then simply right-click and choose Make Group from the menu, or press Ctrl-G. You will be asked to choose a name for the group. Please note, KEYCHAIN will automatically add an asterisk (*) at the beginning of the group name, which will cause all groups to appear at the beginning of the key list.

Once you have made a group, you can right-click on the name of that group to compose a message for all members of the group, to edit the list of members in the group, or to display a dialog that lists all the members in the group. Please note, if you use KEYCHAIN to compose a message for members of a group, the message will be queued for delivery to each member of the group in Eudora or Pegasus Mail; for more information, see KeyChain: Composing Messages.



To edit the contents of a group, right-click on the name of the group and select Edit Group from the menu, or press Ctrl-E. This will cause a blue-tabbed page to appear, listing all public keys, and highlighting those keys that are part of the group. The Edit Group window features a special selection mode: click on any key (or press the spacebar) to select a key, or to deselect a key that is already selected. When finished, select Update Group (to save your changes) or Cancel (to discard changes).


KeyChain
File
Key
Help
*Project Contacts
Alex Yeilding <yeilding@ix.netcom.com>
Andy Robson <andy@sensei.co.uk>
Armando Ramos <100010.334@compuserve.com>
Bert Hankes <ayh@xs4all.nl>
Branko Lankester <lankeste@fwi.uva.nl>
Colin Plumb <colin@nyx.cs.du.edu>
Derek Atkins <warlord@MIT.EDU>
Duncan Jarvis <drj@ray.npl.co.uk>
Eckhard Siefer <Eckhard.Siefer@t-online.de>
Edgar Swank <edgar@Garg.Campbell.CA.US>
Garron Karabelnik <fstechs@tns.net>
Gary H. Freedman <guildnav@ix.netcom.com>
Graeme Cross <Graeme.Cross@sci.monash.edu.au>
Harald Denker <harry@hal.westfalen.de>
Harald Fuerst <harald.fuerst@datev.de>
Hennie J. Briel <hennie@enterprise.net>
Hugh Miller <hmiller@luc.edu>
James O. Ray, Jr. <joray@datasync.com>
James P. Gallegos, Jr. <jgos01@nova.org>
Jean-loup Gailly <jloup@chorus.fr>
Jeffrey I. Schiller <jis@mit.edu>
John DeHaven <johnd@wov.com>
Jonas Hunziker <Jonas.Hunziker@edu.mcnet.ch>

Detached Signatures

Suppose you have a file (which could be a binary file, such as a wordprocessing document or a spreadsheet) and you want to have one or more individuals "sign" the file using their secret keys, so that anyone having the public key could verify that these individuals "signed" the file, and that the file has not been altered?

This can be conveniently done by using "signature certificates," which are signature files separate from, but associated with, the file being signed.

A "signature certificate" has the extension .SIG. If LOCK32 is used to create the "signature certificate," the filename will be the same as the original file (including long filenames) plus the original extension. For example, if you sign the file

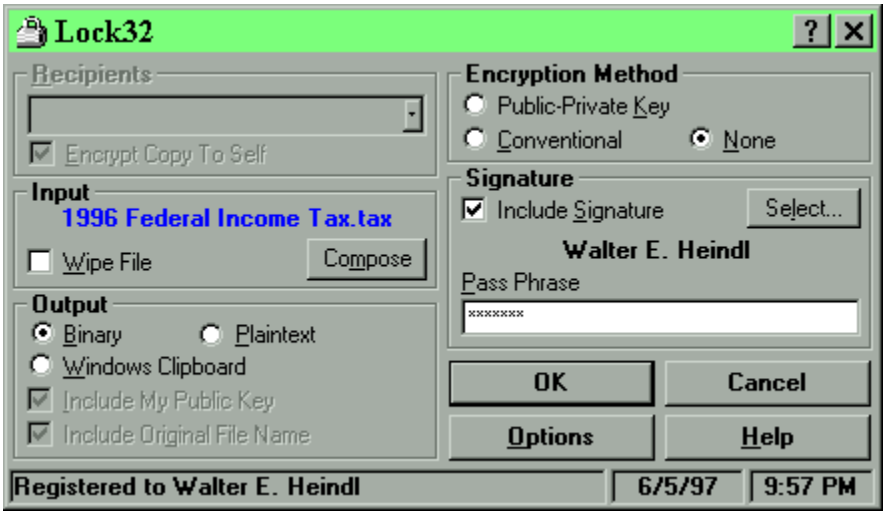
```
C:\Documents\Financial\1988 Budget.XLS
```

the detached signature certificate will be

```
C:\Documents\Financial\1988 Budget.XLS.SIG
```

The signature certificate will show a small key for an icon.

To create a detached signature certificate, follow these steps:



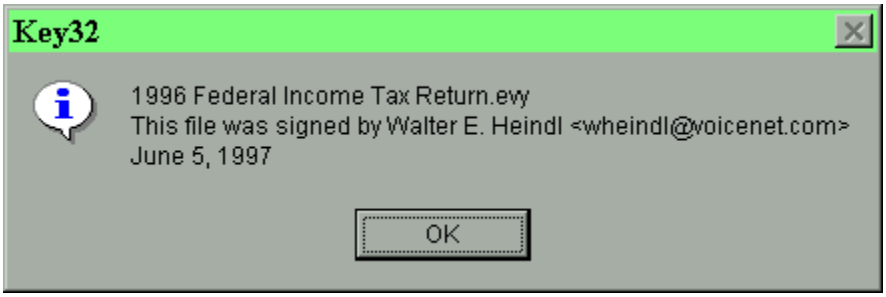
1. For output, choose BINARY.
2. For encryption, choose NONE.
3. For signature, choose INCLUDE SIGNATURE. Enter your pass phrase.

There are several ways to verify the signature certificate.

First, if the signature certificate was created with LOCK & KEY and has not been renamed, then

you can simply double-click on the signature file. LOCK & KEY will find the file being verified. Note that the file being verified must be in the same folder!

Second, you can select both the signature certificate and the file being verified, right-click and send to LOCK & KEY. This is necessary if either file has been renamed, or if the signature certificate wasn't created using LOCK & KEY.



Note that the person verifying the signature must have the signer's public key in the public key ring.

Configuration File Settings

Configuration settings are stored in LOCK&KEY.INI which is found in the Lock & Key program folder. The following is a description of the settings which can be made in this program. Many settings (such as screen position) are simply user preferences saved from session to session. However, there are a number of settings useful for troubleshooting or advanced configuration purposes.

[Common]

UserName=

This shows the name of the registered user.

UserID=

This shows the registration password for the registered user and is necessary to avoid the shareware delay.

RunPGP=0 | 1 | 2

This setting controls how the PGP DOS window is displayed: **0** (hidden), **1** (minimized), or **2** (normal). Windows 95 users: please note that this setting is overridden by the PIF file settings.

Verbose Log=Yes | No

This setting controls whether LOCK32 and KEY32 generate a detailed execution log. This log can be very useful for troubleshooting purposes.

RunPGPPath=

This is the path where Lock & Key places temporary batch files used for running PGP. RUNPGP.PIF and CONSOLE.PIF must be saved in this folder. By default, this is the PGP folder set by the PGPPATH= environment variable. However, if for any reason you have PGP stored in a folder that doesn't permit files to be saved (e.g. a network server), then you must modify this setting to point to another location. Please note that you must move RUNPGP.PIF and CONSOLE.PIF to this location. (Note: if you install a new version of Lock & Key after changing this setting, the installation program will place these files here.)

PGPEXEPath=

This is the path where PGP.EXE is found. By default, Lock & Key will look for PGP in the folder specified by the PGPPATH= environment variable. However, if PGP.EXE is found in a different location (e.g. a network server), this value should be modified.

ErrorLog=Lock&Key.log

This is the name of the log file created by Lock & Key. If Verbose Log is set to No, this filename will be used to generate reports of runtime errors only. If Verbose Log is set to Yes, this filename will contain a detailed log of the most recent program execution. By default, this value is set to **Lock&Key.log** in the Lock & Key program folder. Please note, if this file is to be placed in any other location, the full path must be specified.

PGPLog=LKOutput.txt

This is the filename used to capture PGP console output. By default, this is **LKOutput.txt** in the folder specified by the PGPPATH= environment variable. If PGPPATH= points to a read-only path (such as a network drive), this should be changed. If the path is anything other than PGPPATH, then the full path needs to be specified. **Important note:** this value is passed to PGP as part of each command. Since the length of a PGP command is limited, there are advantages in keeping this entry short. Therefore, it is recommended that this file remain in the PGPPATH folder if at all possible, so the full path can be omitted.

StatusTop=, StatusLeft=

These settings specify the coordinates of the top left corner of the PGP console output window, which is displayed whenever LOCK32 or KEY32 is unable to encrypt or decrypt the selected file, or if PGP generates an error message (such as a bad pass phrase). These settings can be changed by dragging the PGP console output and you will not ordinarily have to edit these settings directly.

Signature=

This setting controls the text that will be appended by LOCK32 and KEYCHAIN to encrypted messages. By default, this will display information about Lock & Key. You may substitute any other message; include this key with no value and no text will be appended. Include a vertical bar (|) within this setting to force a line break.

[Lock32]

Top=, Left=

These settings store the screen coordinates of the LOCK32 window and are saved each time LOCK32 is run. Please note that these screen coordinates typically are based on a screen width of 12000 and height of 9000. You will probably have no need to edit these settings.

Copy To Self=Yes | No

This setting controls whether files and messages are also encrypted using the sender's default public key. By default, this is set to Yes, which will permit you to decrypt any file or message which you encrypt, using your default secret key. Please note that this setting is stored in CONFIG.TXT/PGP.INI and affects PGP operations independently of Lock & Key. This setting

can be changed by checking or unchecking the appropriate box in the LOCK32 dialog box.

Append Key=Yes | No

This setting controls whether the user's default public key is added to output sent to the Clipboard. This is a convenient way to include your own public key with e-mail messages. This setting can be changed by checking or unchecking the appropriate box in the LOCK32 dialog box.

Include File Name=Yes | No

This setting controls whether the name of the original file is included with encrypted data sent to the Clipboard. If the recipient is using KEY32 to decrypt the file, KEY32 can use this information to automatically reconstruct the original file name. If the recipient is not using KEY32, the information may still be useful to the recipient. This setting can be changed by checking or unchecking the appropriate box in the LOCK32 dialog box.

Encryption=RSA | Conventional | None

This setting controls whether LOCK32 defaults to using RSA public-private key encryption, conventional encryption, or no encryption (for unencrypted armoring, or signing plaintext). This setting can be changed by selecting the appropriate button in the LOCK32 dialog box.

Output=Binary | Armored | Clipboard

This setting controls whether LOCK32 asks PGP to produce a binary encrypted file; an armored (7-bit) file suitable for Internet mailing; or sends the encrypted output (armored) to the Clipboard, for pasting into an e-mail message. This setting can be changed by selecting the appropriate button in the LOCK32 dialog box.

Signature=Yes | No

This setting controls whether LOCK32 adds the user's electronic signature when encrypting. This setting can be changed by checking or unchecking the appropriate box in the LOCK32 dialog box. Please note that the user's default signature is used. This is the value following MyName= in CONFIG.TXT/PGP.INI.

Remove Accents=Yes | No

This setting controls whether LOCK32 attempts to rename files having accented or other special characters in their filenames before encrypting them. If you ever encrypt files that have accented or special characters in their filenames, this setting must be set to Yes in order for PGP to recognize and handle the filename. Please note that LOCK32 renames the file with the original long filename when PGP has finished. If you never use files having accented or special characters in their filenames, and encounter any file naming errors, you can disable this by changing this setting to No.

SavePath=*path*

This is the path which will be used to save Clipboard data which is being saved as a binary or armored file. Note that if the input source is a file, the encrypted file will be saved to the original path without prompting. This setting can be changed by changing the path in the "Save As" dialog box.

LineLength=0 | *number*

This setting, if present, causes LOCK32 to automatically add hard returns at the end of each line, when LOCK32 is being asked to add your signature to a plaintext message (Encryption=None) and sending the output to the Clipboard. This is necessary because PGP otherwise will not detect that the input is plaintext and will armor the text before signing it, making the signed plaintext message unreadable without decryption. This setting is the maximum number of characters allowed per line; this is set at 72 by default. Changing this setting to 0 disables the function. If you use an editor that already adds a hard return at the end of each line, or if you do not wish signed messages to be saved as plaintext, change this setting to 0.

Editor=notepad.exe

This setting identifies the default editor for composing messages in LOCK32. By default this is NOTEPAD.EXE. Change this setting using the Options dialog in LOCK32.

Template=

This setting identifies the template file which will be used when composing messages in LOCK32. By default this setting is blank (i.e. a blank file is used). Change this setting using the Options dialog in LOCK32. Be sure that this file can be read by the default editor.

[Key32]

Binary Viewer=

This setting identifies the viewer that will be used to view decrypted files which contain binary data. By default this will point to QUIKVIEW.EXE, which is used to launch QuickView or QuickView+. You may replace this with the full path name of another binary viewer (e.g. KeyView).

ASCII Viewer=

This setting identifies the viewer that will be used to view decrypted files which contain pure text. By default this will point to NOTEPAD.EXE. You may substitute your favorite text editor. Be sure to include the full path if the program is not in a folder in your search path. This setting is provided to allow faster viewing of decrypted files containing nothing but text. You may, however, have all decrypted files sent to QuickView by changing this setting to point to QUIKVIEW.EXE. If you do change this setting, be sure that the program you choose will

handle the largest text files you expect to decrypt; many text editors have limits on the file sizes they will handle.

Decrypt Option=View | Save | Open | Print | Clipboard

This setting specifies what will be done with decrypted files and messages. This setting can be changed by selecting the appropriate button in the KEY32 dialog box. Inappropriate or unsupported choices will be grayed (e.g. opening or printing a decrypted file that has no filename). Also, if Clipboard is checked, and if KEY32 identifies the decrypted data as other than pure text, KEY32 will run QuickView instead.

Top=, Left=

These settings specify the coordinates of the top left corner of the KEY32 dialog box. Change these settings by dragging the KEY32 window to the desired position. Please note that these screen coordinates typically are based on a screen width of 12000 and height of 9000. You will probably have no need to edit these settings.

[KeyChain]

MailProg=Eudora | Pegasus Mail

This setting identifies the name of the mail program used to transport messages composed using the KeyChain message editor. The program is identified when LOCK & KEY is first installed. Note that this setting controls status messages only; it does not affect the operation of the program.

MailPath=

This setting contains the full path of the mail program used to transport messages composed using the KeyChain message editor. The program is identified when LOCK & KEY is first installed. Valid entries are the full path of the Eudora (Lite or Pro, version 3.x) or Pegasus Mail programs. Note that if Pegasus Mail is chosen, -j must be included after the name of the program file.

ComposeTop=, ComposeLeft=, ComposeWidth=, ComposeHeight=, ComposeWindow=

These settings control the display of the KeyChain message editor. These settings can be changed by resizing or moving the KeyChain message editor's window and will not ordinarily need to be changed directly. ComposeWindow will be set either to 0 (normal window) or 2 (maximimzed window).

Slider=

This setting controls the location of the bar that separates the unencrypted (top) and encrypted

(bottom) portions of the KeyChain message editor. The value stored here will be between 0 and 1000. Change this setting by dragging the slider bar in the KeyChain message editor window. It should not be necessary to change this setting directly.

Color=

This setting controls the color scheme used for the KeyChain message editor. Available choices are 0=Gray, 1=Red, 2=Violet, 3=Blue, 4=Teal, 5=Green, 6=Yellow and 7=Buff. Change this setting using the Color dialog on the Options menu for the KeyChain message editor. It should not be necessary to change this setting directly.

Font=, FontSize=

These settings control the font used in the KeyChain message editor. You may change this setting using the Font dialog on the Options menu for the KeyChain message editor. That dialog allows you to choose among Arial, Courier New and Times New Roman, within a range of sizes. You can, if you wish, edit these settings manually to specify other settings.

Top=, Left=

These settings specify the coordinates of the top left corner of the main KeyChain window. Change these settings by dragging the KeyChain window. You should not need to edit these settings directly.

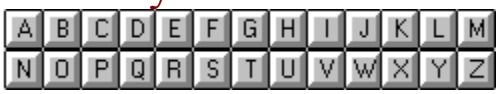
Signature=Yes | No

This setting specifies whether the KeyChain message editor will sign encrypted messages using your default signature. Change this setting on the Options menu of the KeyChain message editor. Note that if this setting is Yes, the pass phrase box will be visible. If this setting is No, the pass phrase box will be grayed out.

Append Key=Yes | No

This setting specifies whether the KeyChain message editor will append your default public key to messages. Change this setting on the Options menu of the KeyChain message editor. Note that if this setting is Yes, a key will be visible at the bottom of the KeyChain message editor.

Glossary



A
armored

C
CompuServe SWREG
console output
conventional cryptography
cryptography

D
dual-key cryptography

E
electronic signature
encryption
environment variable

F
fingerprint

K
keys

P
pass phrase
PGPPASS
plaintext
Pretty Good Privacy (PGP)
private key
public key
public key repository
public keyring
public-private key cryptography

Q
Quick View
Quick View Plus

R
RAMdrive
REGEDIT

Registry

armored
A process of translating a binary file (8 bits per character) into a text file (6 bits per character) to enable the file to be transmitted over Internet mail transports which cannot handle binary files.

CompuServe SWREG

A service offered to CompuServe subscribers for registering shareware. The charge for the shareware is collected from the subscriber by CompuServe as part of the CompuServe charges.

console output
The messages displayed by PGP when it is run from DOS, including status reports and error messages. This information is captured by Lock & Key and can be viewed within Windows if an error occurs.

conventional cryptography
A system of cryptography which uses a single key to encrypt a message. The same key is used to decrypt the message. Anyone who can obtain the key can use it to decrypt a message encrypted with that key.

cryptography
The science of encoding text with a formula to make it unreadable to any person not knowing the formula which was used to encode the text.

dual-key cryptography

A system of cryptography which uses matched pairs of keys: a public key (which is freely distributed) and a private (secret) key known only to the owner. A message encrypted with one key can only be decrypted with the other key.

electronic signature
Additional data added to a file which was created using the sender's private (secret) key, and which the recipient, by using the sender's public keys, can verify that the message originated with the sender.

encryption
A process of altering the characters in a message, using a formula or algorithm, so that the message is not readable to anyone not having the formula or algorithm needed to decrypt the message.

environment variable
A place where the operating system stores information needed by programs (such as the location where temporary files are kept). PGP (and Lock & Key) uses the PGPPATH environment variable to locate the PGP program files.

fingerprint

A set of characters that uniquely identifies a key pair. PGP key pairs are identified by 16-byte fingerprint that can be used to authenticate the key.

keys
Strings of characters which are used to encrypt a message. The characters in the key are processed with the characters in the message using an encryption algorithm (formula) to produce an encrypted message.

pass phrase
A word or phrase which must be entered in order to encrypt or decrypt a message using the private (secret) key.
You need this word or phrase to read a message encrypted with your public key; or to affix an electronic signature to a file or message.

PGPPASS
The name of a DOS environment variable which can store the PGP pass phrase. If the pass phrase is found here, PGP will not prompt the user for the pass phrase.

plaintext
Text which can be read by an ordinary text editor, and which does not require decryption or a particular application program to read.

Pretty Good Privacy (PGP)

A DOS-based cryptography which uses public-private key encryption. PGP is widely available and has become the international standard for high security encryption.

private key
The half of a public-private key which is kept secret by the owner. It is used to decrypt messages which others have encrypted using the public key, or to add an "electronic signature" which can be verified by someone having the corresponding public key.

public key
The half of a public-private key pair which is freely distributed. Someone wishing to send a message to the owner of the key uses that key to encrypt a message, which can only be decrypted by the recipient using his private (secret) key.

public key repository
A source, such as a BBS or an Internet site, for public keys for many users.

public keyring
A file which contains a collection of public keys and which is used like an address book for encrypting messages. These keys are used to send encrypted messages to others, or to verify electronic signatures on messages sent by others.

public-private key cryptography

A system of cryptography which uses a matched pair of keys. Either key can be used to encrypt a message which can only be decrypted by the other. In practice, one of these keys – the public key – is made widely available; the other key – the private key or secret key – is kept secure.

Quick View
A file-viewing program which is included on the Microsoft Windows 95 CD or which can be obtained at the Microsoft Internet site, www.microsoft.com.

Quick View Plus

A file viewing program for Windows 95 by Inso Corporation. Quick View Plus offers enhanced capabilities in comparison to the file viewers included with Windows 95.

RAMdrive

The creation of a virtual disk in computer memory. While the computer treats the RAMdrive as a disk, when the computer is powered down its contents disappears. While the use of a RAMdrive for performance purposes under Windows 95 is not recommended, the fact that the contents are volatile makes a RAMdrive useful for temporary storage of sensitive data.

REGEDIT
The Windows 95 utility used for editing configuration settings in the Windows 95 registry.

Registry
The database in which Windows 95 stores configuration settings.