Lock & Key 1.5.0: An Introduction

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 password, 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.

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

 New Features in Version 1.5.0

- 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*.

- LOCK & KEY stores last settings for encryption, decryption, output and signature options in the registry, so that the last settings used will be restored when the program is next run. This makes use of the programs more convenient for those whose preferences differ from the previous defaults. *NOTE THAT THE PASS PHRASE IS NOT SAVED IN THE REGISTRY. IT MUST BE ENTERED EACH TIME UNLESS THE PGPPASS ENVIRONMENT VARIABLE IS SET.*

- LOCK32 now 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.

- LOCK32 saves the original filename extension when encrypting files. KEY32 automatically restores this extension when the file is decrypted and saved as a file.

- Registered users' registration password, supplied when LOCK & KEY is registered, is stored in the registry rather than as a file. This resolves certain problems when the programs try to read the registration password. *NOTE THAT THE REGISTRATION PASSWORD IS UNRELATED TO YOUR PGP PASS PHRASE AND DOES NOT AFFECT SECURITY OF YOUR PASS PHRASE.*

New Features in Version 1.4.1

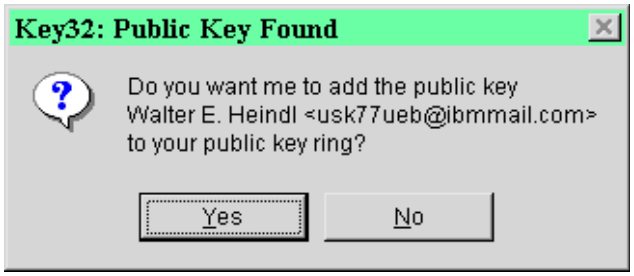
LOCK & KEY version 1.4.1 has the following new features and enhancements:

- The installation program now supports alternatively installing LOCK32.EXE to the \SendTo folder, for compatibility with the MS Office toolbar. *(More information below.)*

- When LOCK32.EXE is placed in the \SendTo folder, long file names are supported.

- An uninstall option has been added.

- KEY32 will now detect whether a .PGP file is an encrypted file or a public key file. If it is a public key file, KEY32 will offer to add the public key to the default public key ring.



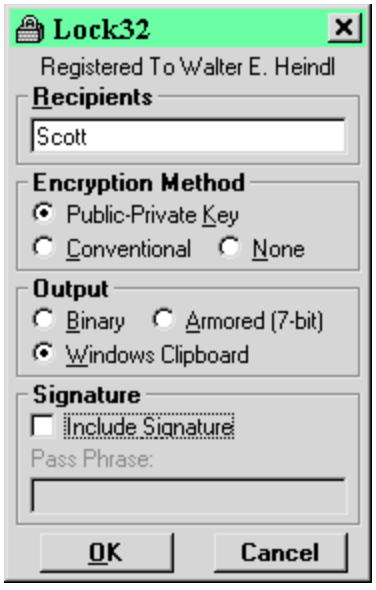
New Features in Version 1.3.0

LOCK & KEY version 1.3.0 now supports the clipboard for both input and output operations. This makes it even easier and faster to encrypt and decrypt electronic mail messages!

If LOCK32 is run without a file specified on the command line, it will encrypt any text contained in the Windows clipboard. Thus, you can write a message in any text editor, copy it to the Windows clipboard, and run LOCK32 to encrypt it. **Supports Rich Text (RTF) as well as plain text!** You can use WordPad as your editor, and create e-mail messages which the recipient can view with full rich text formatting (if the recipient has QuickView, WordPad, MS Word, or any program that can view RTF).

Note: if you choose to save output from the Windows clipboard to disk, in either binary format (.PGP) or armored ASCII (.ASC), the file will be saved as `C:\OUTPUT.PGP` or `C:\OUTPUT.ASC`, respectively.

LOCK32 also now has an option for placing its output (in armored ASCII format) on the Windows clipboard. You can do this whether the input comes from the Windows clipboard, or from a file. Thus, you can select any file in Explorer, encrypt it to the Windows clipboard, paste the result into your e-mail program, and send the file. Simply select the Windows Clipboard option when encrypting:



If KEY32 is run without a file specified on the command line, it will decrypt any text it finds in the Windows clipboard. You can save the result as a file, or view it using QuickView/Quick View Plus.

Thus, the recipient of your e-mail message can select the PGP-encrypted text, copy it to the Windows clipboard, and run KEY32 to decrypt the file.

New Features in Version 1.2.0

- LOCK & KEY version 1.2.0 supports RSA Public Key cryptography or conventional single key cryptography; and can produce either binary (8-bit) or armored ASCII (7-bit) output.

- LOCK & KEY version 1.2.0 allows you to sign files when encrypting, and allows you to see whether an encrypted file has been signed.

- LOCK & KEY version 1.2.0 captures PGP console output and will display this information if an encryption or decryption error occurs.

Installing Lock & Key

Installing LOCK & KEY is very simple. LOCK & KEY 32-bit version requires that you be running Windows 95.

In addition, you must have PGP installed on your computer, and 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:

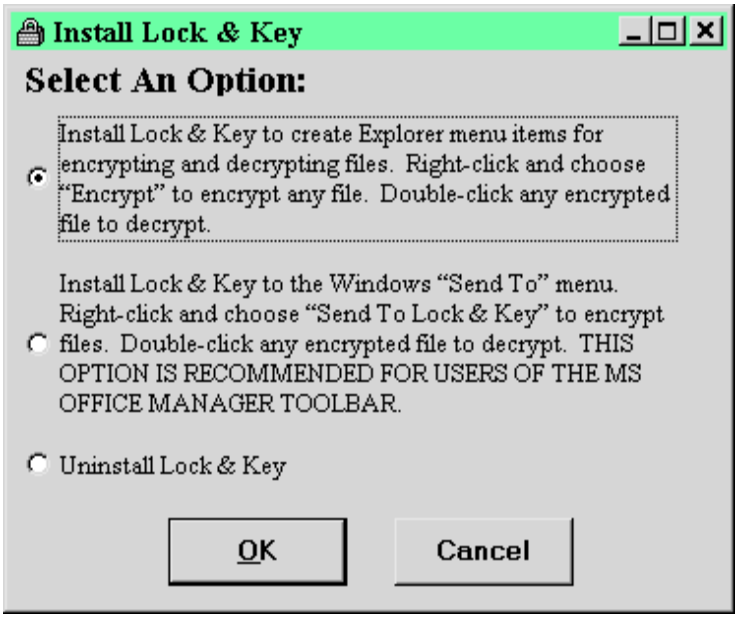
```
SET PGPPATH=C:\PGP
```

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

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

We strongly recommend that you read the documentation which comes with PGP. You will need to use PGP to create your own public and private keys.

To install LOCK & KEY, unzip the files into any directory and run INSTALL.EXE. This will display the following dialog:



Choose the first option for a default installation. This will create a context menu item for encrypting files of any type (right-click and choose Encrypt). Double-clicking an encrypted file will decrypt the file.

The second option will not create a context menu item for encrypting files, but will instead cause Lock & Key to appear as an option on the SendTo menu. Double-clicking an encrypted file will decrypt the file. **THIS OPTION IS RECOMMENDED FOR USERS OF THE MS OFFICE TOOLBAR, DUE TO COMPATIBILITY ISSUES.**

The third option will install LOCK & KEY completely by removing registry entries and deleting the program files.

NOTE: If you choose the first option and later discover compatibility problems with the MS Office toolbar, you can run Install again and choose the second option. This will delete the registry entries that are causing conflict.

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 file for running PGP in your PGP directory. This .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 CLOSE ON EXIT. IT IS IMPORTANT THAT THIS SETTING NOT BE CHANGED, OR LOCK & KEY WILL NOT RUN PROPERLY.

Using Lock32 to Encrypt Files Using Public Key Cryptography

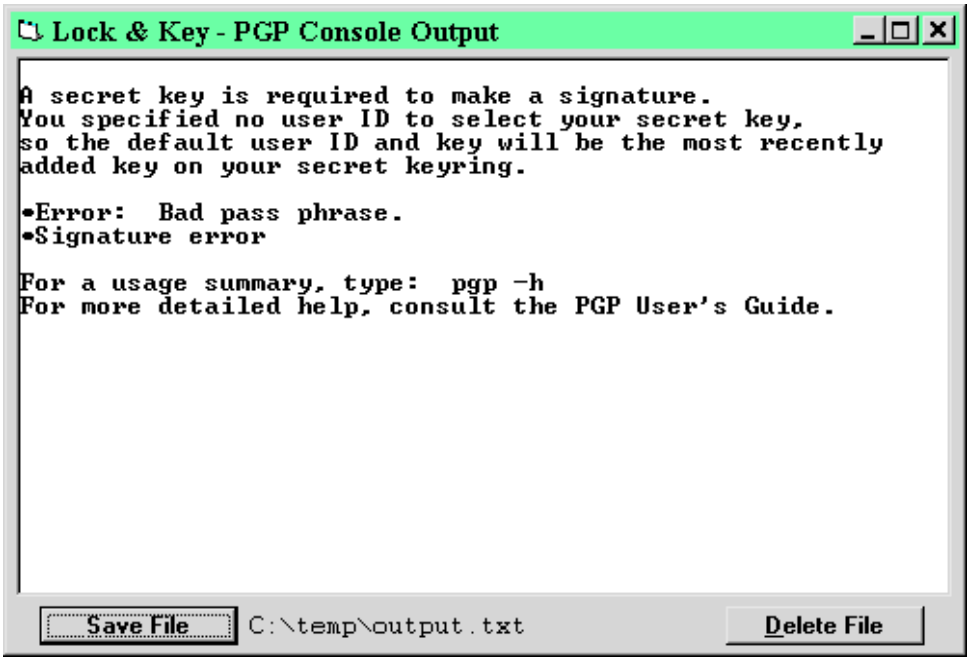
LOCK & KEY automatically adds a new context menu item, Encrypt, for all file types. Simply right-click on any file in Explorer (or on the Windows 95 desktop) and choose Encrypt. This will launch LOCK32:

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. **The unencrypted input file is not affected.**

NOTE: If you have chosen the second installation option, LOCK & KEY will not create a menu item for Encrypt, but will instead place a menu item in the SendTo folder. To encrypt a file, right-click, choose Send To, and choose Lock & Key. **Because MS Office toolbar is incompatible with applications that create context menu entries for all file types, this is the preferred option for users of MS Office toolbar.**

LOCK32 captures PGP console output. If LOCK32 is unable to create an encrypted file, it will report the error and give you an opportunity to view the PGP console output in Windows. This will let you pinpoint the error. Likely causes include the following:

- PGP is not installed correctly.
- 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 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. Note that version 1.5.0 also saves the original extension when encrypting the file, so that SECRET.WK4 becomes SECRET.WK4.PGP when it is encrypted. This enables the original extension to be restored when the file is decrypted and saved as a file.

You can now safely send the encrypted file through insecure channels (such as the Internet) to the intended recipient. Only the intended recipient can decrypt the file using his or her private key.

Using Lock32 to Encrypt Files Using Conventional Cryptography

LOCK32 also supports conventional cryptography using a pass phrase entered at the time of encryption. You will notice that, if conventional encryption is selected, the input box is changed to "Enter Pass Phrase" and input is echoed with asterisks.

Since the same pass phrase must be given to the recipient to decrypt the message, this pass phrase should not be the same as the pass phrase used with your private key.

Using Lock32 to Armor Files

LOCK32 can also be used to armor files (convert them to a 7-bit ASCII code, suitable for sending binary files via e-mail and other text-only channels). Such files are saved with an extension of .ASC. Armoring can be done in connection with pass-phrase encryption (RSA public key or conventional single-key) or by itself (no pass phrase required to decrypt).

Using Key32 to Decrypt Files

Encrypted files have a .PGP 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.

KEY32 will prompt you for your personal pass phrase, used with your own private key. It will also ask whether you want to view the decrypted file (without saving), or save the decrypted file to disk.

Note: PGP supports use of the PGPPASS environment variable as a way to avoid repetitive entry of your pass phrase. Version 1.5.0 will now check for the presence of this environment variable, and, 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.

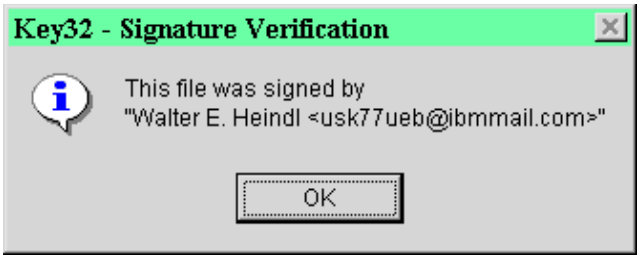
If the pass phrase is correct and the file was encrypted with your public key, then the file will be decrypted. If you choose the option to view the decrypted file, it will be displayed using QuickView or QuickView Plus if one of these is installed. These will enable you to view most common (and many uncommon) word processing, spreadsheet, graphics and other file types. If you do not have QuickView or QuickView Plus installed, and choose to view the file, Notepad will be used. **For security reasons, the decrypted file is overwritten and then deleted if this option is used.**

If you choose to save the file, it will be saved with the same filename, but no extension, in the directory where the encrypted file was located. Note that KEY32 supports Windows 95 long filenames.

Using Lock32 to Sign Files; Using Key32 to Verify 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.

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:



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 Version 1.5.0 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, see the above section on decrypting files.

Using Key32 to Add Public Keys to your Key Ring

Public keys created with PGP have the extension .PGP. If you double-click on any PGP file, KEY32 automatically detects whether the file is a public key, or an encrypted file. If the file is an encrypted file, KEY32 will offer to let the user decrypt the file using his private key. However, if the file is a public key, KEY32 will display the name of the user who created the public key, and offer to add the public key to the user's public key ring.

Revision History

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.

 Registering Lock & Key

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 $15.00 to:

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

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.

Technical Support

For technical support, please visit our Web site:
http://www.voicenet.com/~wheindl

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, usk77ueb@ibmmail.com