Private File™ User's Guide

July 1997

Aladdin Systems, Inc.

165 Westridge Drive

Watsonville, California 95076

Product Manager:	Rakesh Chabra
Engineering:	Serge Volkoff, Leonard Rosenthol
Quality Assurance:	Cathi Schorr, Marc Duisenberg, Randy Birch
Support Lead:	Walt Darson, Margie Downs
Marketing:	Brad Peppard
Documentation:	Christi L. Hembree
Graphic Design:	Mark Kawakami, Kevin Williams

Private File is Copyright© 1996-1997 Aladdin Systems, Inc. All Rights Reserved. PF Encrypt, PF Decrypt, True Finder Integration, StuffIt, StuffIt Deluxe, StuffIt SpaceSaver, Aladdin Desktop Tools, and Magic Menu are trademarks of Aladdin Systems, Inc. All other product names are trademarks or registered trademarks of their respective holders. Our lawyers are happy.

Registration Number(s)

If you require additional items, such as another CD-ROM or User's Guide, or the software on 3.5" floppy disks, you may order any or all of them for FREE, plus shipping.

Items available include:

- Private File for Windows on 3.5" floppy disk
- Private File for Macintosh on 3.5" floppy disk
- Additional Private File (Dual OS) on CD-ROM
- Additional Private File User's Guide

When placing your order, we will need the following:

- your registration number
- your name and address
- which of the above items you would like to receive
- payment or credit card information (include the name on the card, the card number, and expiration date)

To order, use one of the following methods:

- call Customer Service at 1-408-761-6200
- fax your order to 1-408-761-6206
- email your order to sales@aladdinsys.com
- write to:

  Aladdin Systems Customer Service
  Attn: Private File Fulfillment
  165 Westridge Drive
  Watsonville, CA 95076 USA

Aladdin Systems accepts checks, money orders, and credit cards (VISA, MasterCard and American Express). All orders subject to a $9.95 shipping charge (US$19.95 outside of the US and Canada). Offer limited to one order per 2-user pack purchased.

The type used is Times. Text and graphics were generated using FrameMaker.

Table of Contents

Chapter 1: Introduction 1

Welcome 1
What is encryption? 1
Why do you need to encrypt files? 2
Why use Private File to encrypt? 2
Helpful Terms 4
How to use this User's Guide 4
Contacting Aladdin 5

Private File for Windows 7

Chapter 2: Installation 9

Requirements 9
Before You Install 9
Installation 9
Uninstall 12

Chapter 3: Encryption 13

Encrypting Files 13
Password Selection 15
Menu Commands 16
Options 19

Chapter 4: Decryption 23

Decrypting Files 23
Password Verification 25
Options 25

Chapter 5: Help and Other Options 31

View menu 31

Help menu....32
Private File for the Mac OS 33
Chapter 6: Installation 35
Requirements.... 35
Before You Install....35
Installation....35
Chapter 7: Encryption 39
Encrypting Files....39
Password Selection.... 41
Preferences....42
Chapter 8: Decryption 45
Decrypting Files....45
Password Verification....46
Preferences....47
Chapter 9: Magic Menu 51
Encrypting Files....51
Decrypting Files....53
Preferences....54
Index 61

Chapter 1: Introduction

Welcome

Welcome to Private File™, the easiest way to protect your information. Private File allows you to encrypt and decrypt information with two easy-to-use drop boxes: PF Encrypt™ and PF Decrypt™. Private File also provides functionality allowing you to immediately and easily send your newly encrypted information via email. Private File is designed to work seamlessly cross-platform. You can easily transmit documents between Windows and Macintosh computers.

Private File can prevent the wrong people from seeing your sensitive information. By a process called encryption, your data is transformed from readable information to an unreadable encoded version. Once your information is encrypted, only you and those you allow can decrypt it back to its original readable form.

What is encryption?

Encryption is the art of deliberately transforming information into unreadable form. Decryption is the method of undoing the encryption to return the information to its original readable form.

Encryption has been around for thousands of years. Early civilizations, for example, used simple methods to encrypt military information. Modern cryptography uses complex mathematical algorithms to encode information. Many governments limit the level of encryption that is available outside their country. This chapter contains terminology related to encryption that may help your understanding as well as some benefits of using Private File for encrypting.

Why do you need to encrypt files?

Both businesses and private individuals can benefit from encrypting information. In today's technological world, an increasing amount of information is being distributed in a wide variety of ways. Information is more vulnerable than ever. Thus the need for stronger, more secure encryption is growing.

Consider everyone that potentially has access to the information on your computer– your children, spouse, friends, coworkers, employers, not to mention any number of other individuals on the internet that can intercept email, file attachments, and file transfers.

Now think about the types of information you keep on your computer– salary, bank accounts, employee/employer reviews, tax files, journals, contact information, to name a few. As more and more individuals use computers to store information and networks to transmit it, a lot can be at stake.

Businesses rely on internal and external networks every day to send critical information to customers, employees, and vendors. In business, information is the key to remaining competitive. This commodity needs to be protected against the increasing threat of technological espionage. Information important to the survival of a company must not fall into the wrong hands.

With the increasing use of the Internet for communication, businesses and private individuals alike must protect themselves.

Why use Private File to encrypt?

Powerful Encryption

When you select files to encrypt, you are also asked to select a password. Private File takes this password and processes it through an industry standard algorithm called MD5. This process takes the original password and reduces it to a reasonably unique pattern of 16 bytes (128 bits). The encryption key is then taken from this pattern. The international version uses 5 bytes while the domestic version uses all 16. This encryption key is then used by the industry standard RC4 encryption algorithm to encrypt the data. The domestic version of Private File uses 128-bit encryption. The international version uses 40-bit encryption.

Secure Deletion

Private File securely deletes the original file if you set the preferences to do so. The deletion process is done in accordance with the U.S. Department of Defense standards. These standards consist of a three-pass deletion process. The first pass writes over the old data file using new data consisting of all bits set to zero. The second pass overwrites the file with data consisting of all bits set to one. The third pass is exactly like the first where the file is overwritten using data consisting of all bits set to zero. Once these passes are complete, Private File then directs the operating system to remove all references to the file from the disk.

Cross-Platform

Private File allows you to easily transfer files to and from the Mac OS and Windows 95/NT platforms. By intelligently handling and storing the appropriate information, decryption of files from either platform is a seamless process.

- Private File is equipped to handle issues that arise when transferring files cross-platform. For instance, different platforms use a variety of characters to specify the end of a line. Without changing any preferences or options, Private File will transparently handle the different end-of-line characters for the machine on which you are decrypting.
- Transmitting files that are usable cross-platform, such as pictures, sounds, and plain text files is just a step away. When you encrypt this information with Private File, you have no worries about the decryption on either platform. There is nothing you have to set up for a particular platform.
- On Windows 95 and Windows NT, all encrypted files generated by Private File are compressed before encryption, and MacBinary-encoded after encryption. MacBinary encoding allows files of the right type to be generated during transfer from Windows to the Mac OS.

Compression

Compressing data prior to encrypting can have significant benefits.

Compression is the process by which a file is made smaller without losing any of its information. A compression program uses an algorithm, or method, for compressing the information in a file in a more efficient manner, thus taking up less disk space.

Compression works by minimizing or eliminating redundancy and empty space. A file containing the characters “AAAABBBBBBB” typically would take up ten locations. However, this file could be compressed by one algorithm into “4A6B” and would take up only four locations.

Private File utilizes compression to create a smaller file, thus the amount of hard disk spaced used by the encrypted file and the time needed to transmit the file are less than if the file was not compressed.

Helpful Terms

The glossary provides a list of terms commonly associated with encryption. Many are used in other parts of this manual. The more familiar you are with these terms, the better your understanding of the technology will be.

Encryption	the act of transforming a readable message or piece of information into an unreadable format.
Decryption	the reverse act of transforming an encrypted, unreadable message or piece of information into a readable format.
Archive	a document that can contain multiple files and folders and is compressed.
Cryptography	the science of encrypting information.
Cryptanalysis	the science of breaking encryption schemes (ciphers).
Stream cipher	symmetric cipher methods that encrypt a single bit of plaintext at a time.
Block cipher	symmetric cipher methods that encrypt groups of plaintext bits at a time.
Key	a password or code that is used to encrypt or decrypt information.
Symmetric	a method of encryption where the encryption key can be calculated from the decryption key and vice versa. The secrecy of the key is paramount to the security of the information.

How to use this Users’ Guide

This User's Guide applies to both the Windows and Macintosh versions of Private File. The Introduction provides general information that relates to both platforms. The main functions of the program have been separated into a Windows section and a Mac OS section. Refer to the section that is appropriate for you computer.

This User’s Guide assumes you know how to operate a computer running Windows or the Mac OS, and that you are familiar with common terminology such as point, click, drag, and alias or shortcut. If you are not familiar with these terms, please refer to the User’s Guide of your computer to learn the basic operations.

Where applicable, numbered steps are given for completing a procedure.

The User’s Guide is designed to help you utilize all aspects of the program.

Contacting Aladdin

Registration and Updates

Be sure to fill out and mail the enclosed Registration card. Doing so will ensure you are notified of updates and new releases. You will also be eligible for Technical Support.

Comments and Suggestions

Aladdin Systems, Inc. is open to any suggestions that can enhance the usability and features of Private File. Please address your correspondence to Product Manager - Private File, and use any of the addresses listed below.

Technical Support

If you cannot find an answer in this User's Guide, don't forget to check for additional information in the Read Me (and, if it exists, the User's Guide Addenda) in the Private File folder on your computer. Technical Support is available to all registered users via email, phone, fax, or mail. Please be sure to have the following information available prior to calling Aladdin, or include it in your email, fax, or letter:

- Write down your question or have a clear idea of the problem.
- Be prepared to duplicate the problem. Write down the steps you took that caused the problem.
- Note any error messages.
- Note your computer model.
- Note your system version.
- Note the amount of RAM.
- Note your Private File version number.

Internet (Windows): win.support@aladdinsys.com
Internet (Mac OS): support@aladdinsys.com
Compuserve: 75300,1666
Web: http://www.aladdinsys.com
FTP: ftp://ftp.aladdinsys.com

Phone: 408-761-6200
Fax: 408-761-6206

Mail:
Aladdin Systems, Inc.
Technical Support
165 Westridge Drive
Watsonville, CA 95076
U.S.A

Private File for Windows

This section contains instructions on how to use Private File on a computer running Windows 95 or NT 4.0. Instructions on how to use Private File on a computer running the Mac OS are contained in the section “Private File for the Mac OS”.

Chapter 2: Installation

This chapter describes how to install Private File for Windows.

Requirements

Private File operates on any Intel 80x86 or Pentium computer running Windows 95 or Windows NT 4.0, with 4 MB of free disk space, and a CD-ROM drive.

Note: If you do not own a CD-ROM drive, contact Aladdin Systems to request Private File on diskette. Instructions are located immediately before the Table of Contents.

Before You Install

We suggest you take a few moments now to complete the registration card and send it to Aladdin Systems (it's postage paid). If you register, we can notify you of upgrades, new products, and special offers. You will also be eligible for Technical Support.

Installation

The installation process puts several items into your system and creates a Private File directory on your hard disk.

1. Insert the Private File CD into your computer.

Important: If you have not modified the properties of your CD-ROM in your System control panel, the installation program will automatically begin once you insert the CD. You should skip steps 2 - 4 and proceed now to step 5. If you have disabled the 'Auto insert notification' setting, you will need to follow all the steps listed below.

2. **Double-click (open) My Computer (the icon for your hard drive).**

3. **Double-click (open) the CD-ROM drive containing the installation CD.**

4. **Double-click the Private File.exe icon.**

   The Startup window appears. If you would like to proceed with installation, click Yes. Clicking Cancel will abort the installation.

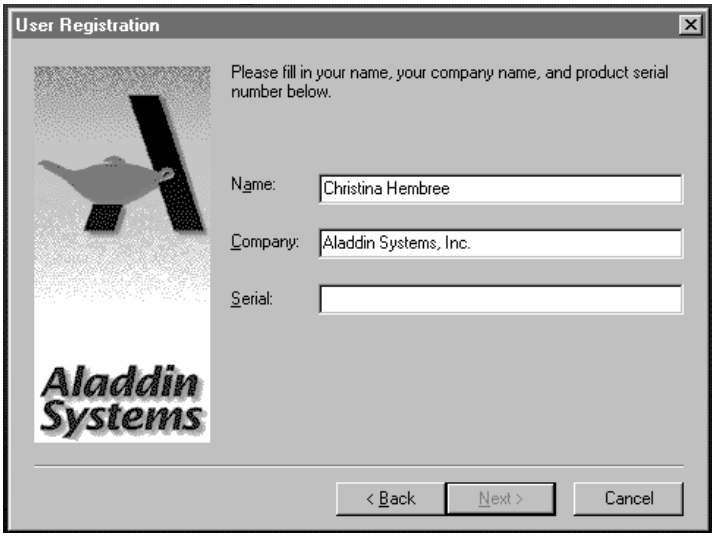
5. **Click "Yes."**

   A number of progress dialogs appear that indicate the progress of the installation preparation. A Welcome window appears. Read the text for important information.

6. **Click "Next."**

   The Registration window appears asking you to register your copy of Private File.

7. **Enter your name, company name, and registration number.**



Some fields may be automatically filled in but you can modify them. A company name is required, however you can type "none" if this

is your personal copy. The registration number can be found on the first page of this User's Guide and on the Registration card. Make sure to enter it exactly as it appears.

8. Click "Next" when you have finished entering the information.

The Confirmation window appears. To confirm the information you entered in the Registration window, click "Yes." To change any of the information you entered, click "No" and repeat steps 7 and 8.

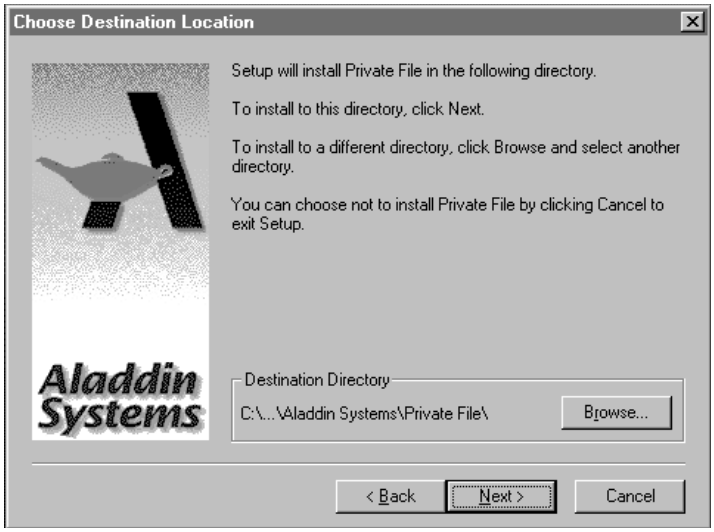
After you click "Yes", the Software License Agreement appears. Please read this entire document. If you do not accept the terms, click No.

9. Click "Yes" when you have read the Software License Agreement.

A dialog appears that lets you choose where to install the software. You can use the default or click the Browse button to navigate to a different location.

10. Click "Next" to install the software into the specified folder.

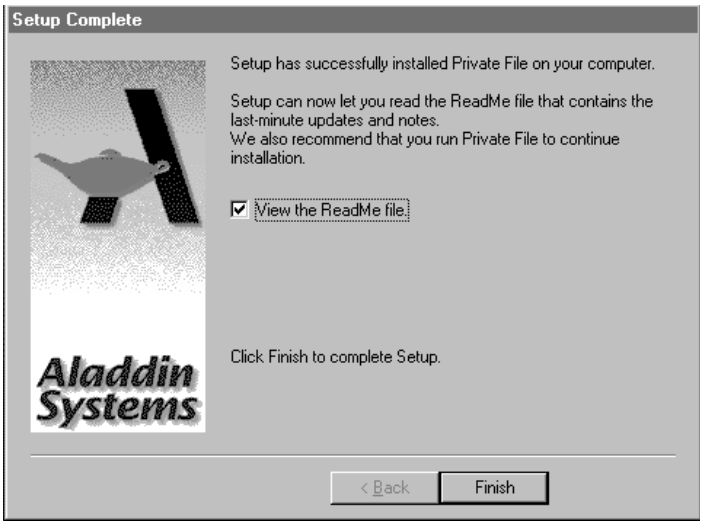
A dialog appears that lets you choose where to install the shortcuts under the Start menu. You can use the default or click the Browse button to select a different folder in which to place the shortcuts.



11. **Click “Next” to install the shortcuts into the specified folder.**

    The setup program then finishes installation. You will see a progress bar indicating its status. Once complete, a window appears that allows you to immediately view the Read Me file. We recommend that you read this file now for important last minute information.

12. **Click “Finish.”**



13. **You have now finished the installation process.**

Uninstall

If you decide to remove Private File:

1. **Select “Uninstall Private File” from the Private File folder in the Programs menu under the Start menu.**

2. **Click “Yes” in the confirmation window.**

   The progress of the uninstall will be displayed.

Note: Any files in the Private File folder that were not installed by Private File will not be deleted.

Chapter 3: Encryption

Under Windows, the Private File application is installed in the Start menu, and two shortcuts, PF Encrypt and PF Decrypt, are installed on the desktop. Both shortcuts launch Private File. There are a variety of ways to access the functions of Private File. Each aspect of PF Encrypt and the encryption capabilities of Private File are described in detail in this chapter.

Encrypting Files

PF Encrypt

There are a variety of ways to access the functions of Private File.

- You can drag and drop files and folders onto the desktop shortcut or the application window.
- You can use the commands from the Encrypt menu in the application.
- You can select files and folders in Explorer and use the right mouse button to access the shortcut menu.

There are also several locations to which you can save the encrypted files.

- You can save them to your hard drive in any folder you specify. Use drag and drop or the “Encrypt” command.
- You can save them directly to a floppy disk, a specified folder, or make them available to a program immediately after encrypting. Use the “Encrypt and Send To” command.
- You can immediately attach them to an email to send to another user. Use the “Encrypt and Mail” command.

Each method of encrypting files and folders as well as the locations to which you can save them are described in the associated sections below. The methods are listed first, followed by how to enter passwords, then additional information on the locations.

Using drag and drop

Private File provides easy drag and drop features to allow quick, hassle-free encryption. You can use the drag and drop features either with the desktop shortcut or with the application window. When you drag and drop with the left mouse button, this is equivalent to selecting “Encrypt” from the Encrypt menu. When you drag and drop to the application window with the right mouse button, a shortcut menu will appear from which you can choose any option.

1. **Select the files and folders to be encrypted with the left mouse button.**

   To select more than one file or folder, hold down the appropriate modifier key. The Shift key allows you to select consecutive files; the Control key allows you to select non-consecutive files.

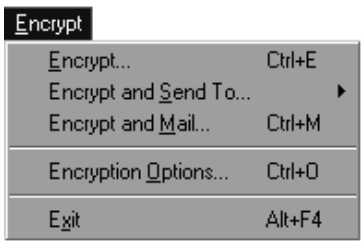
2. **Drag them onto the PF Encrypt desktop shortcut or into the Private File application window.**

   When the selected files and folders are over the desktop shortcut or application window, the cursor will change appearance to include a plus sign (+). The application window is the window with the words “DROP FILES HERE TO ENCRYPT AND DECRYPT.”

   Release the mouse button to encrypt the files and folders.

Using application menu commands

You can encrypt files by launching Private File and using the commands on the Encrypt menu. The commands are described in detail further in this chapter.



1. **Double-click the PF Encrypt desktop shortcut or select Private File from the Programs pop-up menu under the Start menu.**

2. **Select a choice from the Encrypt menu.**

3. **In the dialog window, select the files you want to encrypt.**

   To select more than one file, hold down the appropriate modifier key. The Shift key allows you to select consecutive files; the Control key allows you to select non-consecutive files.

4. **Click “Open.”**

Using the right mouse button in Windows Explorer

Using the right mouse button to select files is the easiest method for encrypting files. It gives you easy access in Explorer to all functions of Private File. There is no need to launch the application.

1. **Select the files and folders to be encrypted.**

   To select more than one file or folder, hold down the appropriate modifier key. The Shift key allows you to select consecutive files; the Control key allows you to select non-consecutive files.

2. **Right-click any of the icons after you have made your selection.**

   In the shortcut menu that appears, you can access the Private File sub-menu. Select an item from the sub-menu to encrypt your selected files and folders.

Password Selection

Once you have indicated which files and folders to encrypt, you must enter a password. Private File, by default, will then create a file in the same folder as the original files and folders you selected. (You can change the destination by changing the options. This is discussed later in this chapter.) If you choose to encrypt a single file or folder, i.e. “file.doc,” the encrypted file will be named “file.doc.pf.” If you choose to encrypt more than one file or folder, the encrypted file will be named “item.pf,” where “item” is the name of the first file or folder, alphabetically, in the files to be encrypted.

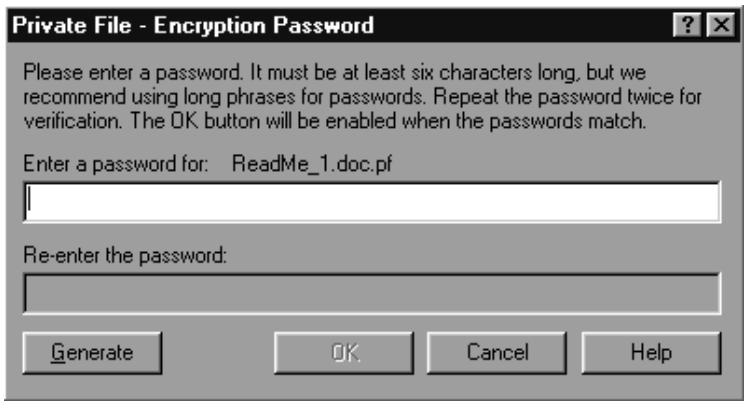
Important: It is very important that you remember the password. Once a file is encrypted there is no alternate method for retrieving the information without the password.

1. **Enter a password in the box.**

   The password must be at least six characters in length. It can contain any letters, numbers, or symbols. As you enter the password, the characters are displayed as asterisks.

   Private File can generate a password for you. To do so, click the “Generate” button. A readable random password is then displayed. You can modify this password.

2. **Click in the second box, or press Tab, once you have entered a password.**



3. Re-enter the password in the second box.

As you re-enter the password, the characters are displayed as asterisks. Once the password matches, the “OK” button will become available.

4. Click “OK” once you have re-entered the password.

You will see a window containing four progress bars. The first progress bar indicates the compression of the files into a temporary archive. The second progress bar indicates the encryption of the archive. The third progress bar indicates the secure deletion of the temporary archive. The fourth progress bar indicates the secure deletion of the original files, if the options are set to do so.

A copy of the files and folders you originally selected are now encrypted and can be stored on your machine, filed as a backup, or transmitted to another user - all securely.

Menu Commands

You can encrypt files by launching Private File and using the commands on the Encrypt menu. Each command is described below.

Encrypt

The “Encrypt” command saves the files you specify to the location set in the Destination Preferences. This is typically a folder on your hard drive. If you have not changed the default, the encrypted file will be saved to the same folder as the files and folders you choose to encrypt.

Encrypt and Send To

The “Encrypt and Send To” command enables you to save encrypted files automatically to a floppy disk, or make them available to a program immediately after encrypting. (To make a new program available, see the next section.) This is a convenient way to save files and folders to a floppy disk for transferring to another computer or user.

Adding a menu item

You can customize the “Encrypt and Send To” menu by adding or deleting items. Use the process outlined below to include new destinations or applications to which you will want to send encrypted files.

1. **Click the Start button with the right mouse button.**
2. **Select “Explore” from the pop-up menu.**

   The Windows Explorer window appears.
3. **Double-click the “SendTo” item in the left side of the window.**

   The right side of the window will display the items in that folder. These are the items that appear in the “Encrypt and Send to” pop-up menu.
4. **To add an item, create a shortcut to it in this folder.**
5. **To delete an item, delete the shortcut from this folder.**

If you are unsure how to create a shortcut or perform any other actions described above, refer to the User’s Guide for your computer or Windows for more information.

Encrypt and Mail

One of the most common methods of transmitting data across the Internet is via email. Many users attach files to send to customers, employees, and potential clients. Valuable information may be transferred. Private File gives you the ability to easily encrypt files and mail them.

The “Encrypt and Mail” command allows you to encrypt files and folders and immediately attach them to an email. This is a convenient way to encrypt and send sensitive information over the Internet.

Windows Messaging (MAPI) is a subsystem of Windows that allows programs to accept commands from other programs. Some programs can

be MAPI servers and thus can create an email, attach a file, address it, and other options. To determine whether your mail program is MAPI compatible, check the User's Guide or contact the developer. You may need to enable the MAPI server in your mail program in order for it to function with Private File. For an example on how to make your mail program MAPI compatible, read the next two sections.

Enabling Windows Messaging

If Windows MAPI Messaging support is not installed, you will need to install it to use the "Encrypt and Mail" option. To do so, follow the steps below.

1. **Choose Control Panels from the Settings pop-up menu under the Start menu.**
2. **Double-click "Add/Remove Programs."**
3. **Select the "Windows Setup" tab.**
4. **Check the "Microsoft Exchange" or "Windows Messaging" checkbox.**
5. **Click "Apply."**

Windows Messaging should be enabled and you should be able to use Encrypt and Mail. For an example of how to enable a specific mail program, read the next section.

Enabling Eudora as a MAPI server

If you want to use an email program other than the System default email program, you will need to ensure it is enabled as a MAPI server. Below are directions for setting up Eudora as a MAPI server.

1. **Launch Eudora.**
2. **Select "Options..." from the Tools menu.**
3. **Select the "MAPI" Category in the left column.**
4. **Click the "Always" radio button for the "Use Eudora MAPI server" option.**

Eudora should now be used when you select "Encrypt and Mail."

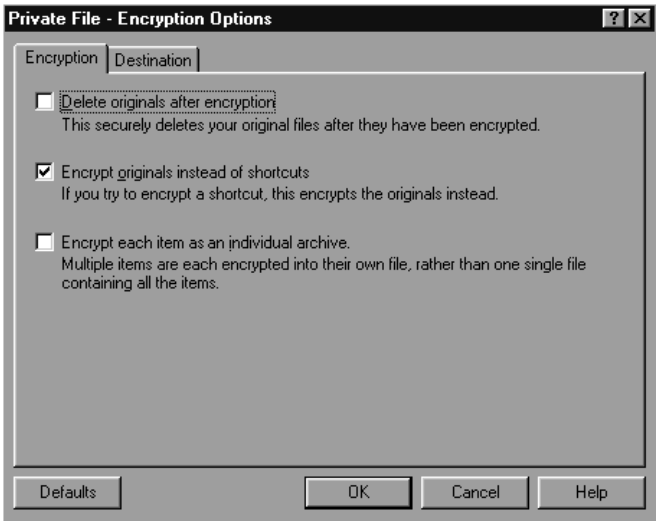
Options

To access the encryption options for Private File, double-click the PF Encrypt desktop shortcut or, from the Start menu, select the Private File program icon. Then select “Options...” from the Encrypt menu.

Encryption

Delete originals after encryption

If this option is checked, the files and folders you choose to encrypt will be securely deleted when the encryption process is complete. Enabling this option can be useful if you want to delete the original files and folders a majority of the time. *Use this option with caution. If you are unsure whether you will want the original, it is best to leave this option off.* This option is off by default.



Encrypt originals instead of shortcuts

If this option is checked, choosing to encrypt a shortcut will cause the original file to be encrypted instead, leaving the shortcut untouched. If you really want to encrypt the shortcut, uncheck the box. This option affects shortcuts for both files and folders. This option is on by default.

Encrypt each item as an individual archive

If this option is checked, when you select multiple files and folders to encrypt, each one is encrypted into a separate file. If this option is disabled, all the files and folders you select are encrypted into one common file. This option is off by default.

Note: If this option is checked, you will be asked to enter a new password for each encrypted file. You can choose to cancel the encryption on a single file or folder when you are prompted for its password. However, only that one file or folder will not be encrypted. You will continue to be asked for a password for each subsequent file or folder.

Destination

If you set the option to "**Ask each time**," you will be prompted each time for the location of the encrypted file. You can also modify the name of the encrypted file.

If you set the option to "**Use:**," you can specify the same folder to be used every time. To select a folder, click the "Browse" button and navigate to the desired location. You can also type it in manually. If the destination folder does not exist, Private File will prompt you to confirm its creation.

The default destination for an encrypted file is "**Same folder as original files**." This will create the encrypted file in the same folder as the original.

Default Options

On each panel of options, there is a “Defaults” button in the lower left corner. Selecting this button reverts the options on that panel only to the default settings.

One-time Options

Using the right mouse button to select files gives you the ability to set one-time options for an encryption process. These options only take effect for the current encryption process. Once finished, they will revert to their previous settings. You can use one-time options while selecting files on your desktop or by dragging to the application window.

On the desktop

Follow these steps to set one time options by selecting files on your desktop.

1. **Select the files and folders to be encrypted.**

   To select more than one file or folder, hold down the appropriate modifier key. The Shift key allows you to select consecutive files; the Control key allows you to select non-consecutive files.

2. **Right-click any of the icons after you have made your selection.**

   In the shortcut menu that appears, you can access the Private File sub-menu. Select an item from the sub-menu to encrypt your selected files and folders.

3. **Select “Encrypt with Options” from the Private File sub-menu.**

   The options window will be displayed and you can modify the options.

With the application window

When you drag and drop to the application window with the right mouse button, you will see a shortcut menu from which you can choose “Encrypt with Options.”

1. **Select the files and folders to be encrypted with the left mouse button.**

   To select more than one file or folder, hold down the appropriate modifier key. The Shift key allows you to select consecutive files; the Control key allows you to select non-consecutive files.

2. **Drag them into the Private File application window.**

   The Private File shortcut menu appears.

3. **Select “Encrypt with Options” from the Private File shortcut menu.**

   The options window will be displayed and you can modify the options.

Chapter 4: Decryption

Under Windows, the Private File application is installed in the Start menu, and two shortcuts, PF Encrypt and PF Decrypt, are installed on the desktop. Both shortcuts launch Private File. There are a variety of ways to access the functions of Private File. Each aspect of PF Decrypt and the decryption capabilities of Private File are described in detail in this chapter.

Decrypting Files

There are a variety of ways to access the functions of Private File.

- You can drag and drop files and folders onto the desktop shortcut or the application window.
- You can use the commands from the Decrypt menu in the application.
- You can select files in Explorer and use the right mouse button to access the shortcut menu.

Each method of decrypting files is described below as well as how to enter passwords.

Using drag and drop

Private File provides easy drag and drop features to allow quick, hassle-free decryption. You can use the drag and drop features either with the shortcut or with the application window. When you drag and drop with the left mouse button, this is equivalent to selecting “Decrypt” from the Decrypt menu. When you drag and drop to the application window with the right mouse button, you will see the shortcut menu from which you can choose any option.

1. **Select the files to be decrypted with the left mouse button.**

   To select more than one file or folder, hold down the appropriate modifier key. The Shift key allows you to select consecutive files; the Control key allows you to select non-consecutive files.

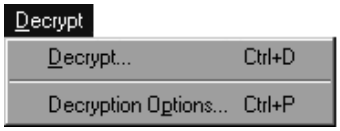
2. **Drag them onto the PF Decrypt desktop shortcut or into the Private File application window.**

   When the selected files and folders are over the desktop shortcut or application window, the cursor will change appearance to include a plus sign (+). The application window is the window with the words "DROP FILES HERE TO ENCRYPT AND DECRYPT."

   Release the mouse button to decrypt the files.

Using application menu commands

You can decrypt files by launching Private File and using the commands on the Decrypt menu.



1. **Double-click the PF Decrypt desktop shortcut or select Private File from the Programs pop-up menu under the Start menu.**

2. **Choose "Decrypt..." from the Decrypt menu.**

3. **In the dialog window, select the files you want to decrypt.**

   To select more than one encrypted file in a specific folder, hold down the appropriate modifier key. The Shift key allows you to select consecutive files; the Control key allows you to select non-consecutive files. All the selected files must be Private File files.

4. **Click "Open."**

Using the right mouse button in Windows Explorer

Using the right mouse button to select files is the easiest method for decrypting files. It gives you easy access in Explorer to all functions of Private File. There is no need to launch the application.

1. **Select the files to be decrypted.**

   To select more than one file or folder, hold down the appropriate modifier key. The Shift key allows you to select consecutive files; the Control key allows you to select non-consecutive files.

2. **Right-click any of the icons after you have made your selection.**

   In the shortcut menu that appears, you can access the Private File sub-menu. Select an item from the sub-menu to encrypt your selected files and folders.

Password Verification

Once you have indicated which files to decrypt, you must enter the password used to encrypt the files. If the password you enter is correct, you will see a window containing four progress bars. The first progress bar indicates the decryption of the file you selected into a temporary archive. The second progress bar indicates the decompressing of the archive. The third progress bar indicates the secure deletion of the temporary archive. The fourth progress bar indicates the secure deletion of the original encrypted files, if the options are set to do so.

If the password you enter is incorrect, a dialog will appear to inform you. The program does not provide a second chance to enter the correct password. To retry, you will need to begin the decryption process again.

That's it - you now have the original, decrypted information.

Options

To access the options for PF Decrypt, double-click the PF Decrypt desktop shortcut or, from the Start menu, select the Private File program icon. Then select “Options...” from the Decrypt menu.

Decryption

Delete originals after decryption

If this option is checked, the items you choose to decrypt will be securely deleted when the decryption process is complete. Enabling this option can be useful if you want to delete the original items a majority of the time. *Use this option with caution. If you are unsure whether you will want the original, it is best to leave the option off.* This option is off by default.

Warn if any selected or dropped files cannot be processed

When this option is checked, a dialog will be displayed when some selected files were not encrypted files and thus cannot be decrypted. If you uncheck the box, no dialog will be displayed and files that are not encrypted will not be decrypted.

Destination

Destination

If you set the option to "**Ask each time**," you will be prompted each time for the destination folder of the decrypted items.

If you set the option to "**Use:**," you can specify the same folder to be used every time. To select a folder, click the "Browse" button and navigate to the desired location. You can also type it in manually. If the destination folder does not exist, it will prompt you to confirm its creation.

The default destination for the decrypted items is "**Same folder as original files**." This will create the decrypted items in the same folder as the original encrypted file.

Create Surrounding Folder

This option allows you to specify when a surrounding folder is created for the files in an encrypted file.

If the option is disabled, the decrypted files will be decrypted into the destination folder.

If the option is set to "**Always**," the decrypted items will always be placed inside a newly created sub-folder of the destination folder. The name of the sub-folder is based on the name of the encrypted file.

If the option is set to "**When the archive contains multiple files**" and the encrypted file contains more than one file or one folder, the decrypted items will be placed inside a newly created sub-folder of the destination folder. The name of the sub-folder is based on the name of the encrypted file. No surrounding folder is created if only one item is encrypted.

The default is "When the archive contains multiple files."

Cross-Platform

Convert text files to Windows format

Different systems use a variety of characters to specify the end of a line.

If the option is disabled, Private File does not convert any end of line characters in decrypted text files.

If the option is set to "**When they contain text**," Private File converts all decrypted files that contain text to the format used by Windows.

If the option is set to "**Always**," Private File always converts any end of line characters in decrypted text files to the format used by a Windows.

Important: If you set this option to "Always," any binary file that is decoded will be damaged. You should only use the "Always" setting if you are positive the encrypted file contains no binary files.

The default is "When they contain text."

Save files in MacBinary format

Most Macintosh files may contain one or two 'parts' (forks): a data fork and/or a resource fork.

If the option is disabled, Private File does not preserve the resource fork in any decrypted files.

If the option is set to "**When they contain a resource fork**," Private File preserves the resource fork in all decrypted files that contain a resource fork.

If the option is set to "**Always**," Private File always preserves the resource fork in all decrypted files. *"Always" will always output a MacBinary file. Use this option with caution.*

The default setting is with the option disabled.

Default Options

On each panel of options, there is a "Defaults" button in the lower left corner. Selecting this button reverts the options on that panel only to the default settings.

One-time Options

Using the right mouse button to select files gives you the ability to set one-time options. These options only take effect for the selected decryption process. Once finished, they will revert to their previous settings. You can use one-time options while selecting files on your desktop or by dragging to the application window.

On the desktop

Follow these steps to set one-time options by selecting files on your desktop.

1. **Select the files to be decrypted.**

   To select more than one file or folder, hold down the appropriate modifier key. The Shift key allows you to select consecutive files; the Control key allows you to select non-consecutive files.

2. **Right-click any of the icons after you have made your selection.**

   In the shortcut menu that appears, you can access the Private File sub-menu. Select an item from the sub-menu to encrypt your selected files.

3. **Select “Decrypt with Options” from the Private File sub-menu.**

   The options window will be displayed and you can modify the options.

With the application window

When you drag and drop to the application window with the right mouse button, you will see the shortcut menu from which you can choose "Decrypt with Options."

1. **Select the files and folders to be decrypted with the left mouse button.**

   To select more than one file or folder, hold down the appropriate modifier key. The Shift key allows you to select consecutive files; the Control key allows you to select non-consecutive files.

2. **Drag them into the Private File application window.**

   The Private File shortcut menu appears.

3. **Select "Decrypt with Options" from the Private File shortcut menu.**

   The options window will be displayed and you can modify the options.

Chapter 5: Help and Other Options

Private File allows you customize the look of the program. The View menu allows you to display or hide various features of Private File. There is also extensive online help. The Help menu lists the ways to access help.

View menu

The View menu contains two options: Toolbar and Status Bar.

The Toolbar is the display of icons that is originally placed immediately below the menu bar. It is a detachable toolbar that you can move around your screen or “dock” at one of the four sides of the application window.

You can also choose to hide the Toolbar. Select “Toolbar” under the View menu. This removes the check from in front of the menu choice and hides the Toolbar. If at any time you wish to access the Toolbar again, select “Toolbar” under the View menu. This places a check in front of the menu item.

The Status Bar is the area beneath the application window. It displays the status of the current operation or information about the location your cursor is above.

To hide this bar, select “Status Bar” under the View menu. This removes the check from in front of the menu choice and hides the Status Bar. If at any time you wish to view the Status Bar again, select “Status Bar” under the View menu. This places a check in front of the menu item.

Help menu

The Help menu gives you several ways to learn more about Private File. The following options are available:

- Index
- Contents
- Context Help
- How to Use Help
- How to Get Support
- Aladdin on the Web
- About Private File

Index

Index provides a listing of ‘how to’ topics and commands available in Private File. If you are having difficulty with one of the listed items, click it for additional information.

Contents

Contents provides alternate means of accessing Private File’s Help. You can select an item from the Contents panel, view a list of specific topics on the Index panel, or find a particular topic on the Find panel.

Context Help

Context Help gives you the ability to click on an item to obtain information about its function. Once you have chosen Context Help from the Help menu, or Toolbar, the cursor changes to a question mark (?). Private File waits until you click

an item and then displays Help for it.

How to Use Help

How to Use Help shows you simple instructions on how to obtain information on a particular Help topic or item. This section contains Contents, Index, and Find panels for topics on how to utilize Help.

How to Get Support

How to Get Support displays information on contacting Aladdin Systems.

Aladdin on the Web

When you select this item, an attempt will be made to launch your web browser and go to our Web site. Depending on your settings, this may initiate an Internet connection.

About Private File

About Private File displays the startup screen with information about the Private File product team. You can also find your Registration number in this window.

Private File for the Mac OS

This section contains instructions on how to use Private File on a computer running the Mac OS. Instructions on how to use Private File on a computer running Windows 95 or NT 4.0 are contained in the section “Private File for Windows.”

Chapter 6: Installation

This chapter describes how to install the Private File package under the Mac OS.

Requirements

Private File operates on any computer running Mac OS 7.0.1 or later with at least 1 MB of available RAM, a hard drive with approximately 1 MB of available hard disk space, and a CD-ROM drive.

Note: If you do not own a CD-ROM drive, contact Aladdin Systems to request Private File on diskette. Instructions are located immediately before the Table of Contents.

Before You Install

We suggest you take a few moments now to complete the registration card and send it to Aladdin Systems (it's postage paid). If you register, we can notify you of upgrades, new products, and special offers. You will also be eligible for Technical Support.

Installation

The installation process puts several items into your System folder and creates a Private File folder on your hard disk. After installation, refer to the document "What was Installed (and Where)" in the Read Us First! folder, inside the Private File folder, for a complete list of files that are installed.

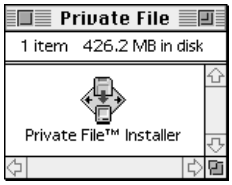
1. **Restart your computer with only the extensions necessary for reading a CD-ROM.**

Under System 7.5 and later, use the Extensions Manager control panel to set up your extensions, then choose Restart from the Special menu. Under System versions prior to 7.5, you will need to manually remove the unnecessary extensions. Doing this disables all unnecessary extensions on your computer. This is important to avoid any extension conflicts during installation. You will restart your computer after you install Private File.

2. Insert the Private File CD into your computer.

Important: If QuickTime™ is installed in your computer and you have not modified the QuickTime™ Settings control panel, the installation program will automatically begin once you insert the CD. You should skip step 3. If you have disabled the 'Enable CD-ROM AutoPlay' setting, you will need to follow all the steps listed below.

3. Double-click the Installer icon on the disk.



A "splash screen" appears.

4. Click "Continue."

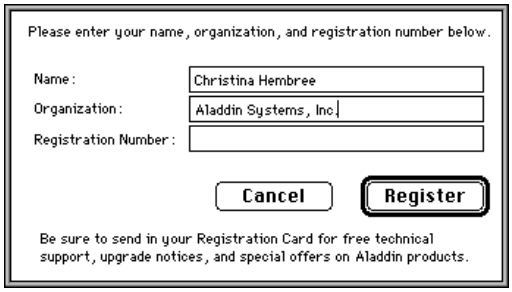
A Welcome window appears. This dialog contains last-minute changes and other important information. You can save or print this information by clicking the appropriate button.

5. Click "Continue" when you have finished reading the information.

The registration dialog then appears, asking you to register your copy of Private File.

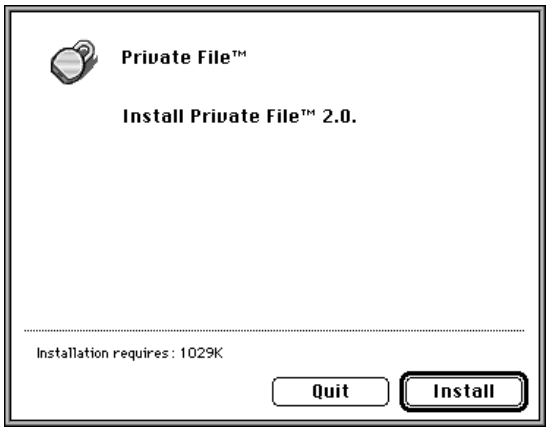
6. Enter your name, organization (if applicable), and registration number.

The registration number can be found on the Registration card and on the title page of this User's Guide. Make sure to enter it exactly as it appears.



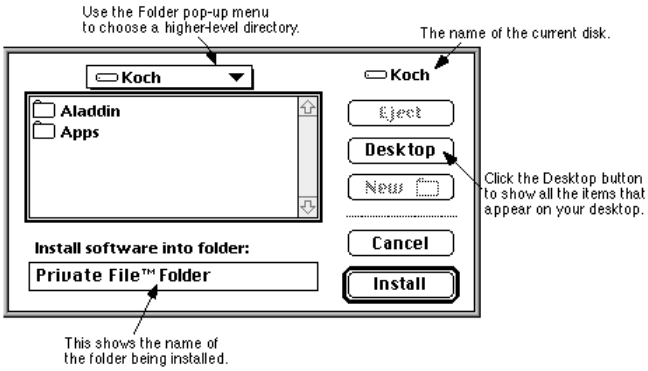
7. Click "Register" when you have finished entering the information.

The Installation dialog appears next.



8. Click "Install" to continue.

A dialog box appears that lets you choose where to install the software.



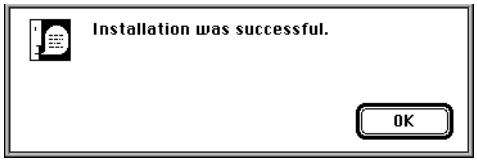
9. **Use this dialog to point to the place on your hard disk where you want to install the Private File folder, then click "Install."**

   You can create a new folder or choose another hard drive as the installation destination.

   Once you have chosen where you want to install Private File and clicked the Install button, a dialog displays the progress of the installation:

Note: The actual number of items that are installed on your computer may vary depending on your system configuration.

   When all the files have been installed, the following dialog box appears:



10. **Click "OK" to complete the installation process.**

    You will need to enable the extensions that were disabled at the beginning of installation. You should also enable the True Finder Integration control panel that was installed with Private File in order to use all of the capabilities of the program. Once you have enabled your extensions, restart your computer.

11. **You have now finished the installation process.**

Chapter 7: Encryption

On the Macintosh, Private File is comprised of two separate applications, PF Encrypt and PF Decrypt, and Magic Menu. Aliases to PF Encrypt and PF Decrypt are installed onto the desktop for easy access. The PF Encrypt alias launches the PF Encrypt application; the PF Decrypt alias launches the PF Decrypt application. You can use drag and drop features with each alias to perform different tasks. Each aspect of PF Encrypt is described in detail in this chapter.

Encrypting Files

PF Encrypt is one of two applications, PF Encrypt and PF Decrypt, installed by Private File. There are a number of ways to access its functionality. You can use the alias or the program icon for drag and drop functions or you can launch the application and use the commands from the File menu.

Using drag and drop

PF Encrypt provides easy drag and drop features to allow quick, hassle-free encryption. You can drag and drop onto the alias on your desktop or onto the program icon in the Private File folder.

1. **Select the files and folders to be encrypted.**

   To select more than one file or folder, hold the Shift key down while single-clicking each one.

2. **Drag them onto the PF Encrypt icon.**

   You can drag the files and folders onto the alias on the desktop or onto the program icon in the Private File folder. When the icon highlights, release the mouse button.

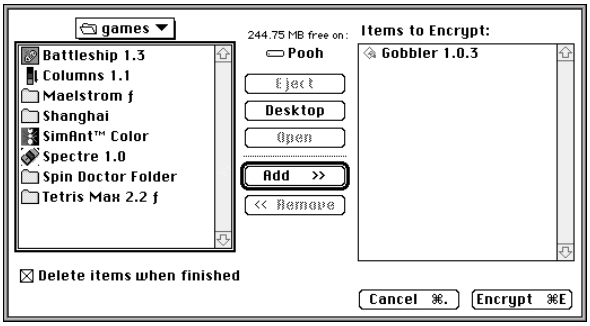
Using the application

Alternately, you can encrypt files and folders by launching Private File and using the commands under the File menu.

1. **Double-click the PF Encrypt program or alias icon.**

2. **Choose “Encrypt...” from the File menu.**

3. **Select the files and folders you want to encrypt in the left side of the window and click “Add.”**



Do this for each file and folder you want to include. The files and folders then appear in the right, “Items to Encrypt:”, column. To add all the files and folders in the left side of the window, hold the Option key down. The “Add” button changes to “Add All.”

To remove a file or folder from the “Items to Encrypt:” list, simply select it and click the “Remove” button. To remove all the files and folders from the right side of the window, hold the Option key down. The “Remove” button changes to “Remove All.”

To delete the files and folders you are encrypting after the encryption process is complete, check the “Delete items when finished” check box.

4. **Click “Encrypt.”**

Once the “Items to Encrypt:” list displays all the files and folders you want in a particular file you can click “Encrypt.”

Password Selection

Once you have indicated which files and folders to encrypt, you must enter a password. PF Encrypt, by default, will then create a file in the same folder as the original files and folders you selected. If you choose to encrypt a single file or folder, i.e. “file,” the encrypted file will be titled “file.pf.” If you choose to encrypt more than one file or folder, the encrypted file will be titled “archive.pf.”

Important: It is very important that you remember the password. Once a file is encrypted there is no alternate method for retrieving the information without the password.

1. Enter a password in the box.

The password must be at least six characters in length. It can contain any letters, numbers, or symbols. As you enter the password, the characters are displayed.

Private File can also generate a password for you. To do so, click the “Generate Random” button. A random password is then displayed. You can modify this password.

2. Click “OK.”

You will be prompted to re-enter the password. This time, the characters of the password are displayed as bullets.

3. Click “OK” once you have re-entered the password.

You may see a number of progress bars depending on the time each operation takes to complete. The first would indicate the compression of the files into a temporary archive. A second progress bar would indicate the encryption of the archive. A third progress bar would indicate the secure deletion of the temporary archive.

If you have modified the preferences to do so, you may also see a fourth progress bar that indicates the secure deletion of the original files.

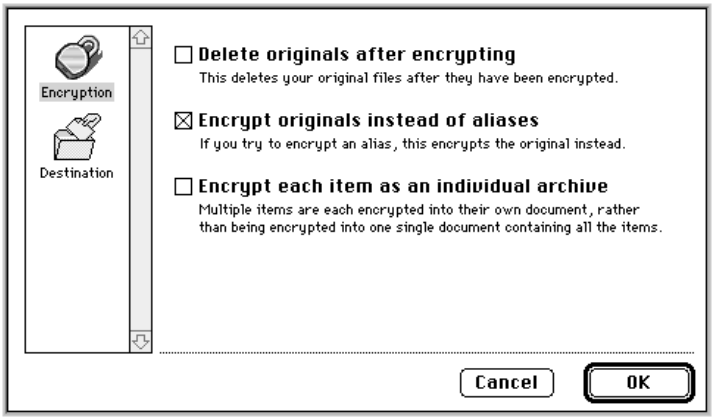
A copy of the files and folders you originally selected are now encrypted and can be stored on your machine, filed as a backup, or transmitted to another user - all securely.

Preferences

To access the preferences for PF Encrypt, double-click the PF Encrypt program or alias icon. Then select “Preferences...” from the File menu.

Note: When you change the preferences, they are also reflected in the preferences for Magic Menu.

Encryption Preferences



Delete originals after encrypting

If this option is checked, the files and folders you choose to encrypt will be securely deleted when the encryption process is complete. Enabling this preference can be useful if you want to delete the original files and folders a majority of the time. *Use this option with caution. If you are unsure whether you will want the original, it is best to leave this option off.* This option is off by default.

Alternately, you can select the “Delete items when finished” check box in the “Items to Encrypt” dialog box when encrypting via the application.

Encrypt originals instead of aliases

If this option is checked, choosing to encrypt an alias will cause the original file to be encrypted instead. If you really want to encrypt the alias, uncheck the box. This option is on by default.

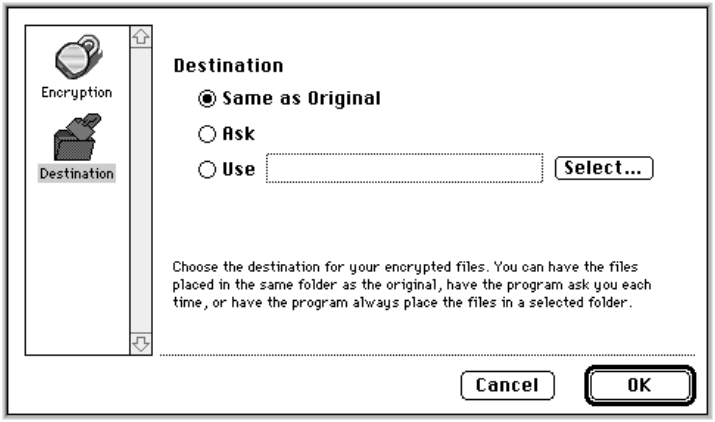
Note: When this option is disabled, it only affects encryption initiated through the Magic Menu or the application’s File menu. This option cannot be disabled for drag and drop operations.

Encrypt each item as an individual archive

If this option is checked, when you select multiple files and folders to encrypt, each one is encrypted into a separate file. If this option is disabled, all the files and folders you select are encrypted into one common file. This option is off by default.

Note: When this option is checked, you will be asked to enter a new password for each encrypted file. You can choose to cancel the encryption on a single file or folder when you are prompted for its password. However, only that one file or folder will not be encrypted. You will continue to be asked for a password for each subsequent file or folder.

Destination Preferences



If you set the preference to "**Ask**," you will be prompted each time for the name and destination folder of the encrypted file.

If you set the preference to "**Use**," you can set a folder into which all encrypted files and folders will be placed. To select a folder, click the "Select..." button and navigate to the desired location.

The default destination for an encrypted file is "**Same as Original**." This will create the encrypted file in the same folder as the orignal.

One-time Preferences

Using the control or option keys gives you the ability to set one-time options for an encryption process. These options only take effect for the current encryption process. Once finished, the preferences will revert to their previous settings.

Option key

If you hold the Option key down while encrypting files and folders, a dialog box appears that lets you change the preferences for that encryption process.

Control key

If you hold the Control key down while encrypting files and folders, the selected file will be securely deleted after successful encryption. *Use this option with caution. If you are unsure whether you will want the original, it is best not to use this option.*

Chapter 8: Decryption

On the Macintosh, Private File is comprised of two separate applications, PF Encrypt and PF Decrypt, and Magic Menu. Aliases to PF Encrypt and PF Decrypt are installed onto the desktop for easy access. The PF Encrypt alias launches the PF Encrypt application; the PF Decrypt alias launches the PF Decrypt application. You can use drag and drop features with each alias to perform different tasks. Each aspect of PF Decrypt is described in detail in this chapter.

Decrypting Files

PF Decrypt is one of two applications, PF Encrypt and PF Decrypt, installed by Private File. There are a number of ways to access its functionality. You can use the alias or the program icon for drag and drop functions or you can launch the application and use the commands from the File menu.

Using drag and drop

PF Decrypt provides easy drag and drop features to allow quick, hassle-free decryption. You can drag and drop onto the alias on your desktop or onto the program icon in the Private File folder.

1. **Select the files to be decrypted.**

2. **Drag them onto the PF Decrypt icon.**

   You can drag the files onto the alias on the desktop or onto the program icon in the Private File folder. When the icon highlights, release the mouse button.

Note: You can also double-click an encrypted file in order to decrypt it. The results are the same as if you had dragged the item onto PF Decrypt.

Using the application

Alternately, you can decrypt files by launching Private File and using the commands under the File menu.

1. Double-click the PF Decrypt program or alias icon.

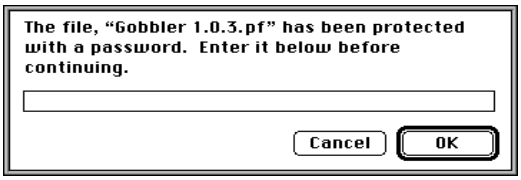
2. Choose “Decrypt...” from the File menu.

3. Select the item you want to decrypt.

4. Click “Decrypt.”

Password Verification

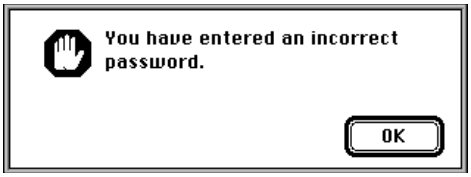
Once you have indicated which files to decrypt, you must enter the password used to encrypt the files.



If the password you enter is correct, you may see a number of progress bars depending on the time each operation takes to complete. The first would indicate the decryption of the file you selected into a temporary archive. A second progress bar would indicate the expanding of the archive. A third progress bar would indicate the secure deletion of the temporary archive.

If you have modified the preferences to do so, you may also see a fourth progress bar that indicates the secure deletion of the encrypted files.

If the password you enter is incorrect, a dialog will be displayed to inform you.



The program does not provide a second chance to enter the correct password. To retry, you will need to begin the decryption process again.

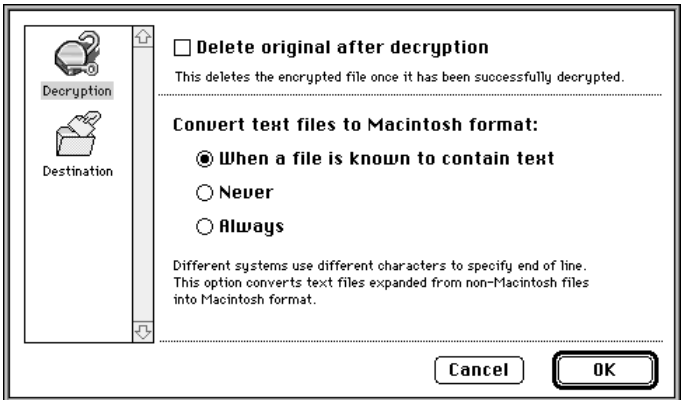
That's it - you now have the original, decrypted information.

Preferences

To access the preferences for PF Decrypt, double-click the PF Decrypt program or alias icon. Then select “Preferences...” from the File menu.

Note: When you change the preferences, they are also reflected in the preferences for Magic Menu.

Decryption Preferences



Delete original after decryption

If this option is checked, the items you choose to decrypt will be securely deleted when the decryption process is complete. Enabling this preference can be useful if you want to delete the original item a majority of the time. *Use this option with caution. If you are unsure whether you will want the original, it is best to leave the option off.* This option is off by default.

Convert text files to Macintosh format

Different platforms use a variety of characters to specify the end of a line.

If the option is set to “**When a file is known to contain text**,” Private File converts all decrypted files that contain text to the format used by the Mac OS.

If the option is set to “**Never**,” Private File does not convert any end of line characters in decrypted text files.

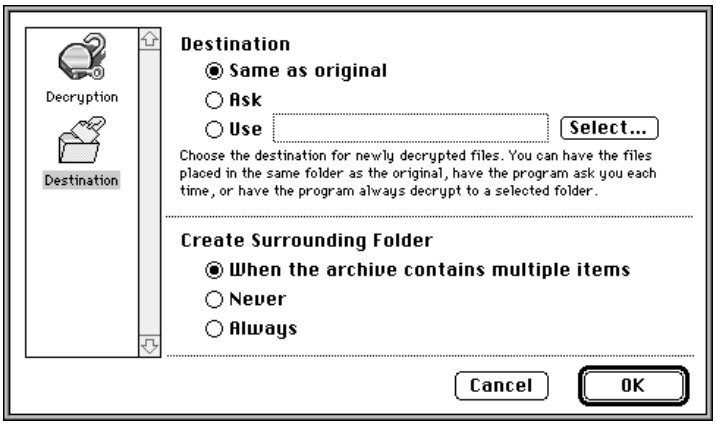
If the option is set to “**Always**,” Private File always converts any end of line characters in decrypted files to the format used by the Mac OS.

Destination Preferences

Destination

If you set the preference to "**Ask**," you will be prompted for the destination folder of the decrypted files and folders.

If you set the preference to "**Use**," you can specify the same folder to be used every time. To select a folder, click the "Select..." button and navigate to the desired location.



The default destination for decrypted files is "**Same as Original**." This will create the decrypted files in the same folder as the original encrypted file.

Create Surrounding Folder

This preference allows you to specify when a surrounding folder is created for the files in an encrypted file.

If the preference is set to "**Never**," the decrypted items will be decrypted into the destination folder.

If the preference is set to "**Always**," the decrypted items will always be placed inside a newly created sub-folder of the destination folder.

If the preference is set to "**When the archive contains multiple items**," and the encrypted file contains more than one file or one folder, the decrypted items will be placed inside a newly created sub-folder of the destination folder. No surrounding folder is created if only one item is encrypted.

The default is "When the archive contains multiple items."

One-time Preferences

Using the control or option keys gives you the ability to set one-time options for a decryption process. These options only take effect for the current decryption process. Once finished, the preferences will revert to their previous settings.

Option key

If you hold the Option key down while decrypting items, a dialog box appears that lets you set one-time preferences for that decryption process.

Control key

If you hold the Control key down while decrypting items, the selected file will be deleted after successful decryption. *Use this option with caution. If you are unsure whether you will want the original, it is best not to use this option.*

Chapter 9: Magic Menu™

Once Private File is installed, Magic Menu appears in the Finder to the right of the Special menu. If you already own StuffIt Deluxe™, StuffIt SpaceSaver™, or Aladdin Desktop Tools™, the Private File items will be added to Magic Menu. Magic Menu makes it easy to perform Private File's tasks while in the Finder. Private File includes the following functions under Magic Menu:

- Decrypt
- Encrypt
- Encrypt and Mail
- Preferences....

Encrypting Files

There are two encryption choices under Magic Menu. To use either method, select the files and folders to encrypt and then choose an option. The methods are described in detail below, followed by instructions on entering passwords.

Encrypt

The "Encrypt" command saves encrypted files to your hard drive. This method provides easy encryption from the Finder.

Encrypt and Mail

The "Encrypt and Mail" command saves encrypted files to your hard drive, launches your email program, and attaches the encrypted file to a new message. This method provides a quick and secure way to encrypt and transfer files over the Internet.

The following email clients are currently supported: America Online 3.0, cc:Mail, Claris EMailer, Eudora, QuarterDeck Mail, and QuickMail Pro.

AOL Note: Only one file can be automatically attached to an email message.

QuickMail Pro Note: If QuickMail Pro is not running, the "Encrypt and Mail" command will only launch the application. If QuickMail Pro is running, a new message will be created with the encrypted file attached.

QuarterDeck Note: QuarterDeck must be running and you must be logged in for the "Encrypt and Mail" command to work.

cc:Mail Note: QuarterDeck must be running and you must be logged in for the "Encrypt and Mail" command to work.

1. **Select the files and folders to be encrypted.**

   To select more than one file or folder, hold the Shift key down while single-clicking each item.

2. **Select an item from Magic Menu.**

   Selecting "Encrypt" will save the encrypted files to your hard drive. Selecting "Encrypt and Mail" will save the encrypted files, launch your email program, and attach the encrypted files to a new message.

Password Selection

Once you have indicated which files and folders to encrypt, you must enter a password. PF Encrypt, by default, will then create a file in the same folder as the original files and folders you selected. If you choose to encrypt a single file or folder, i.e. "file," the encrypted file will be titled "file.pf." If you choose to encrypt more than one file or folder, the encrypted file will be titled "archive.pf."

Important: It is very important that you remember the password. Once a file is encrypted there is no alternate method for retrieving the information without the password.

1. **Enter a password.**

   The password must be at least six characters in length. It can contain any letters, numbers, or symbols. As you enter the password, the characters are displayed.

   Private File can also generate a password for you. To do so, click the “Generate Random” button. A random password is then displayed. You can modify this password.

2. **Click “OK.”**

   You will be prompted to re-enter the password. This time, the characters of the password are displayed as bullets.

3. **Click “OK” once you have re-entered the correct password.**

You may see a number of progress bars depending on the time each operation takes to complete. The first would indicate the compression of the files into a temporary archive. A second progress bar would indicate the encryption of the archive. A third progress bar would indicate the secure deletion of the temporary archive.

If you have modified the preferences to do so, you may also see a fourth progress bar that indicates the secure deletion of the original files.

A copy of the files and folders you originally selected are now encrypted and can be stored on your machine, filed as a backup, or transmitted to another user - all securely.

Decrypting Files

To decrypt files via Magic Menu:

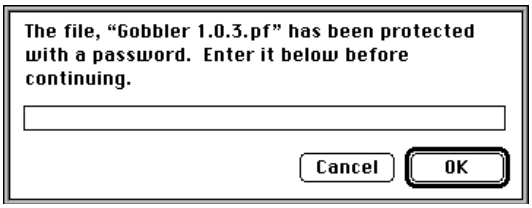
1. **Select the files and folders to be decrypted.**

   To select more than one file or folder, hold the Shift key down while single-clicking each one.

2. **Choose “Decrypt” from Magic Menu.**

Password Verification

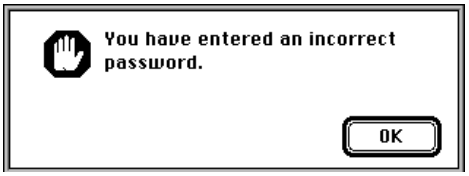
Once you have indicated which files to decrypt, you must enter the password used to encrypt the files.



If the password you enter is correct, you may see a number of progress bars depending on the time each operation takes to complete. The first would indicate the decryption of the file you selected into a temporary archive. A second progress bar would indicate the expanding of the archive. A third progress bar would indicate the secure deletion of the archive.

If you have modified the preferences to do so, you may also see a fourth progress bar that indicates the secure deletion of the original encrypted files.

If the password you enter is incorrect, a dialog will be displayed to inform you.



The program does not provide a second chance to enter the correct password. To retry, you will need to begin the decryption process again.

That's it - you now have the original, decrypted information.

Preferences

To access the preferences for Magic Menu options:

1. Select “Preferences...” from Magic Menu.

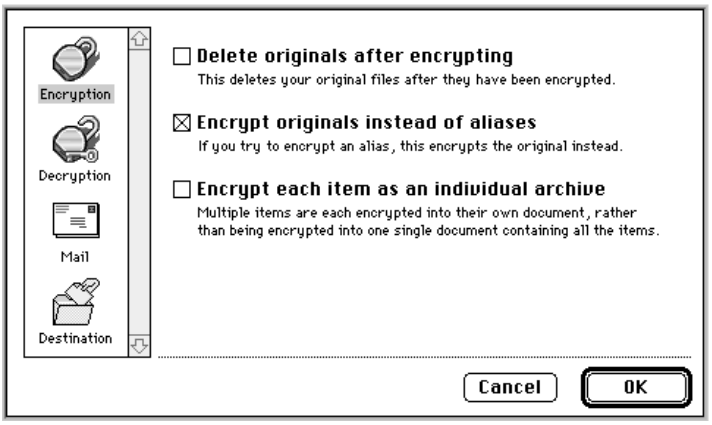
Note: These preference settings are global and will change the preferences in PF Encrypt and PF Decrypt.

Encryption Preferences

Delete originals after Encrypting

If this option is checked, the files and folders you choose to encrypt will be securely deleted when the encryption process is complete.

Enabling this preference can be useful if you want to delete the original files and folders a majority of the time. *Use this option with caution. If you are unsure whether you will want the original, it is best to leave the option off.* This option is off by default.



Alternately, you can select the “Delete items when finished” check box in the “Items to Encrypt” dialog box when encrypting via the application.

Encrypt originals instead of aliases

If this option is checked, choosing to encrypt an alias will cause the original file to be encrypted instead. If you really want to encrypt the alias, uncheck the box. This option is on by default.

Note: When this option is disabled, it only affects encryption initiated through Magic Menu or the application’s File menu. This option cannot be disabled for drag and drop operations.

Encrypt each item as an individual archive

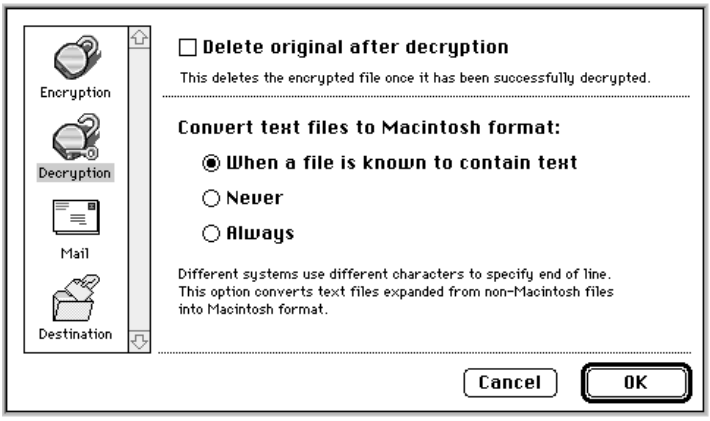
If this option is checked, when you select multiple files and folders to encrypt, each one is encrypted into a separate file. If this option is disabled, all the files and folders you select are encrypted into one common file. This option is off by default.

Note: When this option is checked, you will be asked to enter a new password for each encrypted file. You can choose to cancel the encryption on a single file or folder when you are prompted for its password. However, only that one file or folder will not be encrypted. You will continue to be asked for a password for each subsequent file or folder.

Decryption Preferences

Delete original after decryption

If this option is checked, the files and folders you choose to decrypt will be securely deleted when the decryption process is complete.



Enabling this preference can be useful if you want to delete the original files and folder a majority of the time. *Use this option with caution. If you are unsure whether you will want the original, it is best to leave this option off.* This option is off by default.

Convert text files to Macintosh format

Different platforms use a variety of characters to specify the end of a line.

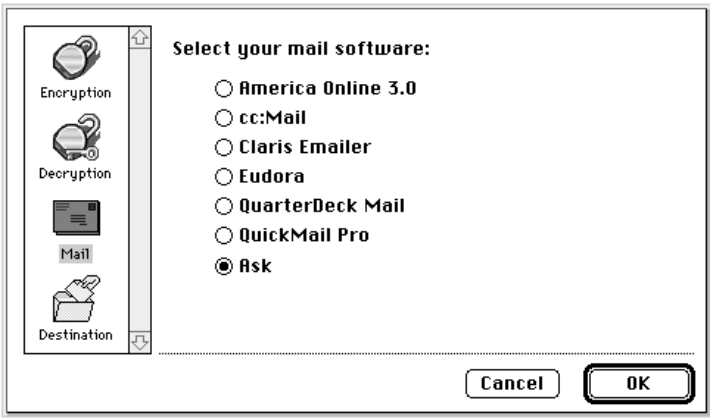
If the option is set to "**When a file is known to contain text**," all decrypted files that contain text are converted to the format used by the Mac OS.

If the option is set to "**Never**," Private File does not convert any end of line characters in decrypted text files.

If the option is set to "**Always**," Private File always converts any end of line characters in decrypted files to the format used by the Mac OS.

The default is "When a file is known to contain text."

Mail Preferences



This preference allows you to specify which mail client to use when you choose to Encrypt and Mail. The following email clients are currently supported: America Online 3.0, cc:Mail, Claris Emailer, Eudora, QuarterDeck Mail, and QuickMail Pro.

You can also set the preference to "Ask" which prompts you to select an email client each time you Encrypt and Mail.

Destination Preferences

Decryption Destination

If you set the preference to "**Ask**," you will be prompted for the destination folder of the decrypted files and folders.

If you set the preference to "**Use**," you can specify the same folder to be used every time. To select a folder, click the "Select..." button and navigate to the desired location.

The default destination for decrypted files and folders is "**Same as Original**." This will create the decrypted files in the same folder as the original encrypted file.

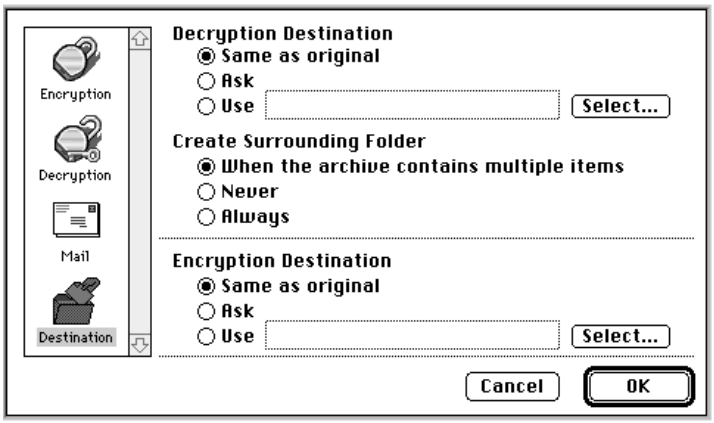
Create Surrounding Folder

This preference allows you to specify when a surrounding folder is created for the files in an encrypted archive.

If you set the preference to "**Never**," the decrypted files and folders will be decrypted into the destination folder.

If you set the preference to "**Always**," the decrypted files and folders will always be placed inside a newly created sub-folder of the destination folder.

The default is "When the archive contains multiple items."



If the preference is set to "**When the archive contains multiple items**" then, if the encrypted file contains more than one file or one folder, the decrypted files and folders will be placed inside a newly created sub-folder of the destination folder. No surrounding folder is created if only item is encrypted.

Encryption Destination

If you set the preference to "**Ask**," you will be prompted each time for the name and destination folder of the encrypted file.

If you set the preference to "**Use**," you can set a folder into which all decrypted files and folders will be placed. To select the folder, click the "Select..." button and navigate to the desired location.

The default destination for an encrypted file is "**Same as Original**." This will create the encrypted file in the same folder as the original.

One-time Preferences

Using the control or option keys gives you the ability to set one-time options for an encryption process. These options only take effect for the current encryption process. Once finished, the preferences will revert to their previous settings.

Option key

If you hold the Option key down while encrypting or decrypting files and folders, a dialog box appears that lets you change the preferences for that encryption process.

Index

A

addresses
  Aladdin Systems 6
Aladdin Systems
  ways to reach us 6
aliases
  PF Encrypt 39
  PF Decrypt 45
America OnLine 52, 57
archive 4

B

block cipher 4

C

cc:Mail 52, 57
cipher
  block 4
  stream 4
cipher text 4
Claris Emailer 52, 57
compression benefits 3
configuring
  Magic Menu 54
  PF Encrypt 19, 42
  PF Decrypt 25, 47
control key 44, 49
cross-platform
  benefits 3
  options 27
cryptography 4
cryptanalysis 4

D

Decrypt
  command 23, 24, 46, 53

decryption
  defined 1, 4
  options 25
  preferences 47, 56
destination
  options 20, 26
  preferences 43, 48, 57
drag and drop
  and PF Encrypt 13, 14, 39
  and PF Decrypt 23, 21, 45

E

electronic addresses of Aladdin Systems 3
Encrypt command 13, 16, 40
Encrypt and Mail command 13, 17, 49
Encrypt and Send command 13, 17
encryption
  defined 1, 4
  method used 2
  options 19
  preferences 55
Eudora 52, 57

F

File menu 40, 46

H

help
  Aladdin on the Web 32
  contents 32
  context 32
  how to get support 32
  how to use 32
  index 32

Help Menu 32
Helpful Terms 4

I

installing
- Mac OS 35
- Windows 95/NT 9

K

key 4

M

Magic Menu
- configuring 54
- Decrypt 53
- decryption preferences 56
- destination preferences 57
- Encrypt 51
- Encrypt and Mail 51
- encryption preferences 55
- mail preferences 57
- one-time preferences 58
- setting preferences 54

mail preferences
- (Magic Menu) 57

mail programs
- AOL 52, 57
- cc:Mail 52, 57
- Claris Emailer 52, 57
- Eudora 52, 57
- QuarterDeck Mail 52, 57
- QuickMail Pro 52, 57

MAPI server
- enabling Eudora as 18

menu
- Decrypt 24
- Encrypt 14
- File 40, 46
- Magic 51

O

one-time options 21, 29
one-time preferences 44, 49, 58
option key
- and one time preferences 43, 49, 58

options (Windows)
- cross-platform 27
- decryption 25
- default 21, 28
- destination 20, 26
- encryption 19
- one-time 21, 29

P

password
- entering 15, 41, 52
- forgetting 15, 41, 52
- selection 15, 41, 52
- verification 25, 46, 54

preferences (Macintosh)
- and the Option key 43, 49, 58
- and the Control key 44, 49
- decryption 47, 56
- destination 43, 48, 57
- encryption 42, 55
- Magic Menu 54
- msil 57
- one-time 43, 49

Q

QuarterDeck Mail 52, 57
QuickMail Pro 52, 57

R

RAM requirements 35
read Me files 9, 35
registration 5
- card 5
- number 9, 35

requirements

RAM 35
System software 9, 35
right mouse button 13, 15, 23, 25

S

shortcuts (Windows)
PF Decrypt 23
PF Encrypt 14
standard installation
Mac OS 35
Windows 9
Status Bar 31
stream cipher 4
symmetric 4
system requirements 9, 35

T

technical support 6
Toolbar 31

U

uninstall 12
User's Guide
conventions 4

V

View menu 31

W

Windows Messaging
enabling 18

Aladdin Systems License Agreement

This is a legal agreement between you and Aladdin Systems, Inc. (“Aladdin”). Be sure to read the following agreement before using the software. BY USING THE SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT PROMPTLY RETURN THE ENTIRE PACKAGE (with all accompanying items) FOR A FULL REFUND.

GRANT OF LICENSE. Aladdin grants to you the non-exclusive right to use the accompanying software program (the “SOFTWARE”) and accompanying documentation (“Documentation”) on the following terms.

This is a two user license. As purchaser of the SOFTWARE, you may make [up to] one additional copy of the SOFTWARE and provide that copy to another user, provided that you provide such user with a copy of this Agreement and such user agrees to be bound by this Agreement. You may not network the SOFTWARE and except as set forth above, you may not make it available for use on more than one computer at the same time.

COPYRIGHT. The SOFTWARE is owned by Aladdin and is protected by United States and international copyright laws. Therefore, you must treat the SOFTWARE like any other copyrighted material (e.g. a book or musical recording) and may not copy the SOFTWARE except as provided herein or (a) make one copy solely for backup or archival purposes, or (b) transfer the SOFTWARE to a single hard disk provided you keep the original solely for backup or archival purposes. You may

not copy the written materials accompanying the software.

OTHER RESTRICTIONS. You may not rent or lease the SOFTWARE, but you may transfer the SOFTWARE and accompanying written materials on a permanent basis provided you retain no copies and the recipient agrees to the terms of this agreement. You may not electronically transfer the SOFTWARE from one computer to another except as provided for herein. You may not modify, adapt, translate, reverse engineer, decompile, or disassemble the SOFTWARE.

DISCLAIMER OF WARRANTY AND LIMITED WARRANTY. THE SOFTWARE AND ACCOMPANYING WRITTEN MATERIALS (INCLUDING INSTRUCTIONS FOR USE) ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND. FURTHER, ALADDIN DOES NOT WARRANT, OR MAKE ANY REPRESENTATIONS REGARDING THE USE, OR THE RESULTS OF THE USE, OF THE SOFTWARE OR WRITTEN MATERIALS IN TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, CURRENTNESS, OR OTHERWISE.

Aladdin warrants that the disks on which the SOFTWARE is recorded is free from defects in materials and workmanship under normal use for a period of ninety (90) days from purchase. You may obtain a replacement disk by returning the original disk to:

Aladdin Systems, Inc.

165 Westridge Drive

Watsonville, California, 95076-4167

United States of America

THIS IS A LIMITED WARRANTY AND IT IS THE ONLY WARRANTY MADE BY ALADDIN. THERE ARE NO OTHER WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE THAT ARE MADE BY ALADDIN ON THIS ALADDIN PRODUCT. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY ALADDIN, ITS DEALERS, DISTRIBUTORS, AGENTS, OR EMPLOYEES SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY, AND YOU

MAY NOT RELY ON SUCH INFORMATION OR ADVICE. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

NEITHER ALADDIN NOR ANYONE ELSE WHO HAS BEEN INVOLVED WITH THE CREATION, PRODUCTION, OR DELIVERY OF THE SOFTWARE SHALL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, AND THE LIKE) ARISING OUT OF THE USE OR THE INABILITY TO USE THE SOFTWARE EVEN IF ALADDIN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOM STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES OR THE LIMITATIONS OF DURATION OF IMPLIEDWARRANTY, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU. Aladdin's entire liability and your exclusive remedy as to the disk and the SOFTWARE shall be, at Aladdin's option, either (a) return of the purchase price or (b) replacement of any defective disk.

EXPORT CONTROLS. Neither the SOFTWARE nor underlying information or technology may be downloaded or otherwise exported or reexported (i) into (or to a national or resident of) Cuba, Iraq, Libya, Yugoslavia, North Korea, Iran, Syria or any other country to which the U.S. has embargoed goods; or (ii) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Deny Orders. By downloading or using the Software, you are agreeing to the foregoing and you are representing and warranting that you are not located in, under the control of, or a national or resident of any such country or on any such list.

In addition, if the SOFTWARE is identified as a not-for-export product (for example, on the box, media or in the installation process), then the following applies: EXCEPT FOR EXPORT TO CANADA FOR USE IN CANADA BY CANADIAN CITIZENS, THE SOFTWARE AND ANY UNDERLYING TECHNOLOGY MAY NOT BE EXPORTED OUTSIDE THE UNITED STATES OR TO ANY FOREIGN ENTITY OR “FOREIGN PERSON” AS DEFINED BY U.S. GOVERNMENT REGULATIONS, INCLUDING WITHOUT LIMITATION, ANYONE WHO IS NOT A CITIZEN, NATIONAL OR LAWFUL PERMANENT RESIDENT OF THE UNITED STATES. BY DOWNLOADING OR

USING THE SOFTWARE, YOU ARE AGREEING TO THE FOREGOING AND YOU ARE WARRANTING THAT YOU ARE NOT A “FOREIGN PERSON” OR UNDER THE CONTROL OF A FOREIGN PERSON.

TERMINATION. This license will terminate automatically if you fail to comply with the limitations described above. On termination, you must destroy all copies of the SOFTWARE and Documentation.

MISCELLANEOUS. This Agreement shall be governed by the laws of the State of California. If for any reason a court of competent jurisdiction finds any provision of this Agreement, or portion thereof, to be unenforceable, that provision of the Agreement shall be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remainder of this Agreement shall continue in full force and effect.

U.S. GOVERNMENT RESTRICTED RIGHTS

The SOFTWARE and documentation is provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subdivision (b)(3)(ii) of The Rights in Technical Data and Computer Software clause at 252.227-7013. Manufacturer is Aladdin Systems, Inc., 165 Westridge Drive, Watsonville, California, United States of America, 95076-4167.

Now our lawyers are happy.