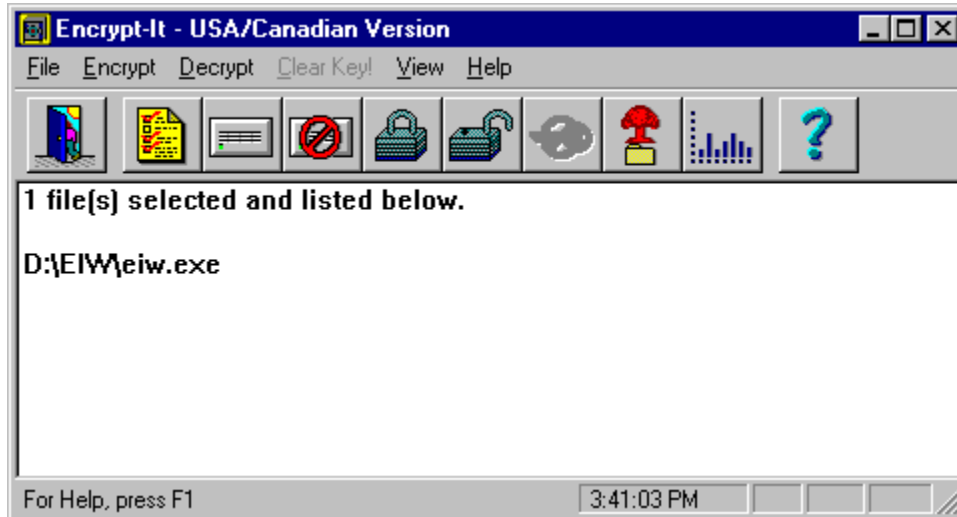


Encrypt-It for Windows

The main screen for **Encrypt-It** (shown below) consists of a menu, a tool bar, and a list of selected files. From this opening window you will select the file(s) of your choice to be encrypted or decrypted and begin the encryption/decryption process. In addition you can also look at a histogram which displays the relative occurrence of each character in the file.

Click on an area of the window shown below for detailed information on that part of the window.



Encrypt-It for Microsoft Windows 95
High Performance Secure Data Protection for Windows

ENCRYPT-IT © 1991-1996 MaeDae Enterprises
5805 Prospero Road, Peyton, CO 80831 (719) 683-3860

To get help while looking at a specific window in **Encrypt-It**, press F1 or click the Help button in that Window. For general help, press the F1 key from the main **Encrypt-It** window or use the Help menu item. You can also click below for other kinds of help with **Encrypt-It**.



Mean

The *mean* is computed by taking the sum of all the values and dividing by the number of values. For example, the *mean* of (58, 67, 60, 84, 93, 98, 100) is 80, equal to the sum of all 7 values (560) divided by 7.

Maximum

Max is the number of occurrences of the most common character in the file. The decimal ASCII value of the most common character in the file is the value of **mode**.

Minimum

Min indicates the number of occurrences of the least common character in the file.

Standard Deviation

Standard deviation describes how much the data deviates from the **mean**. **Encrypt-It** calculates this using the "entire population" of characters in the file.

Index of Commands

The main **Encrypt-It** menu commands are:

File

Select

Clear List

Remove

Statistics

Preferences

Encrypt

Encryption Level

Encryption Cleanup

Decrypt

Decryption Cleanup

Remove

Remove Files Preference

Miscellaneous

Key Length

Clear Key

Hide File List

Exit

Encrypt

Decrypt

Clear Key!

View

Tool Bar

Status Bar

File List

Help

Index

Using Help

About **Encrypt-It**

Proprietary Methods

Encrypt-It provides several layers of encryption as its basic level of data protection. Our proprietary encryption algorithm uses the industry standard XOR, transposition, and substitution forms of encryption. These are applied to your data, one on top of the other, providing multiple layers of encryption. A Proprietary+ encryption algorithm is also provided for more security. The Proprietary+ technique provides several additional layers on top of the proprietary level.

It is extremely unlikely that anyone will ever go to the expense to break our proprietary level of encryption. To eliminate even this small possibility we also support adding the secure DES and DES+CBC on top of our proprietary encryption.

Data Encryption Standard

Where did DES come from?

In 1972 the National Bureau of Standards (NBS) asked for proposals to encrypt commercial computer data traffic (just like the data in your PC today). In 1974, the NBS asked the National Security Agency (NSA) for assistance since they received an extremely poor response to their original request for proposals. One of NSA's primary functions is the development and breaking of data protection techniques (codes and cyphers). An algorithm developed by IBM became the Data Encryption Standard (DES) and was issued by the National Bureau of Standards in 1977, providing an approved and secure standard for protecting computer data against possible theft or unauthorized access.

How well does DES protect your data?

The designers of the DES algorithm maintain that the time needed to decrypt a DES encrypted file makes it unprofitable to use trial and error techniques. Some estimates to break DES are as high as \$200 million to try all 72 quadrillion possible keys.

What is DES+CBC and how well does it protect your data?

Cipher Block Chaining (CBC) is an extension of DES that provides additional data protection by encrypting each block of the data (using XOR) with the contents of the previous block then applying DES on top of that. DES+CBC is much harder to break than DES alone.

Warning: *DES is intended to provide protection for unclassified data which does not affect national security. Software packages which incorporate DES (such as **Encrypt-It US/Canadian Version**) CANNOT be exported outside the U.S. or Canada due to the level of data protection they provide.*

An international version with the proprietary encryption methods is available for export outside of the US and Canada. Click Help from the main menu, then About for details.

Help for Encrypting Files

USE THE BROWSE BUTTONS ABOVE (<< OR >>) TO MOVE FORWARD OR BACKWARD IN THIS DESCRIPTION OF ENCRYPT-IT. CLICK THE CONTENTS BUTTON TO RETURN TO THE TOP.

Encrypt-It provides several levels of data encryption to completely protect your important data. Whether you want to protect your data from unauthorized access in your absence or you want to protect your data from interception by electronic mail hackers, **Encrypt-It** provides it all. There are four ways that **Encrypt-It** works. They are:

Proprietary - A lightning fast encryption method using a combination of exclusive OR (XOR), transposition, and substitution encryption processes. This is the basic level of encryption you get with **Encrypt-It**.

Proprietary+ - You also use several additional layers of proprietary encryption in a method we call Proprietary+.

DES - The slower, but very secure, Data Encryption Standard (DES) encryption is added to our proprietary methods.

DES+CBC - The most secure level is the DES+CBC. The price you pay for the added security is time. It takes longer to use this method of encryption, but you get the very secure Data Encryption Standard (DES) encryption plus Cipher Block Chaining (CBC) on top of our proprietary methods. This provides the ultimate in data encryption; we call it DES+.

(Note: Because of the level of protection provided by DES, **Encrypt-It** CANNOT be sold outside the U.S. or Canada! An international version without DES is available when you register. Click Help and About from the main menu.)


Along with the data, the original file's name, date and time of creation or last modification are embedded within the encrypted version of the file. This is done so that when you decrypt your files, they will be exactly like the original file in all respects.

Select Your File or Files

USE THE BROWSE BUTTONS ABOVE (<< OR >>) TO MOVE FORWARD OR BACKWARD IN THIS DESCRIPTION OF ENCRYPT-IT. CLICK THE CONTENTS BUTTON TO RETURN TO THE TOP.

You can select one or more files on which to perform the encryption process. From the main **Encrypt-It** window, select File from the main menu bar, then select Select... from the drop-down list. The Select Files dialog box will appear.



Alternatively, you can click the  button to get to the Select Files dialog box. Once in the Select Files dialog, choose your files selecting the drive and/or directory and click one or more files from the file list. Note as you select a file name, the group boxes on the right display information about the file (date, time, size) and about the time to encrypt the file.

When you've selected the files you want to encrypt, click OK and you are returned back to the main **Encrypt-It** window, which now lists your files.

(Note: If you happen to go back to the Select Files dialog to add another file, you will have to rebuild the list from the start because **Encrypt-It** does not allow you to append files to the list.)

Mode

Mode is the value or property which occurs most frequently in the data. Thus, if you are interested in the most frequently occurring character in a file, the **mode** provides that information. For example, if you count the number of occurrences of each letter in the previous sentence, the **mode** will be 32. That's the decimal value of the ASCII code for the **space** character, which typically occurs most frequently in text. In binary object files, you will often see a **mode** of 0, representing the ASCII **null** character frequently found in these files.

Encryption Setup

The Key: The key is a group of letters and/or numbers (case sensitive) that will be fed into the encryption process to produce a file that no one else can read unless they have the same key. You can let **Encrypt-It** create the key for you, or you can use your own set of letters and/or numbers as a key. You need at least 5 characters. Choose a group of characters that someone won't easily guess, but preferably something that you'll remember. If you forget it, you won't get your original file back!

The Directory: Let **Encrypt-It** store the encrypted file in the same directory as the source file, or you can choose another directory on your system.

The Encryption Level: Choose one of four levels of encryption.

The Clean-up Method: Choose one of four methods for cleaning up.

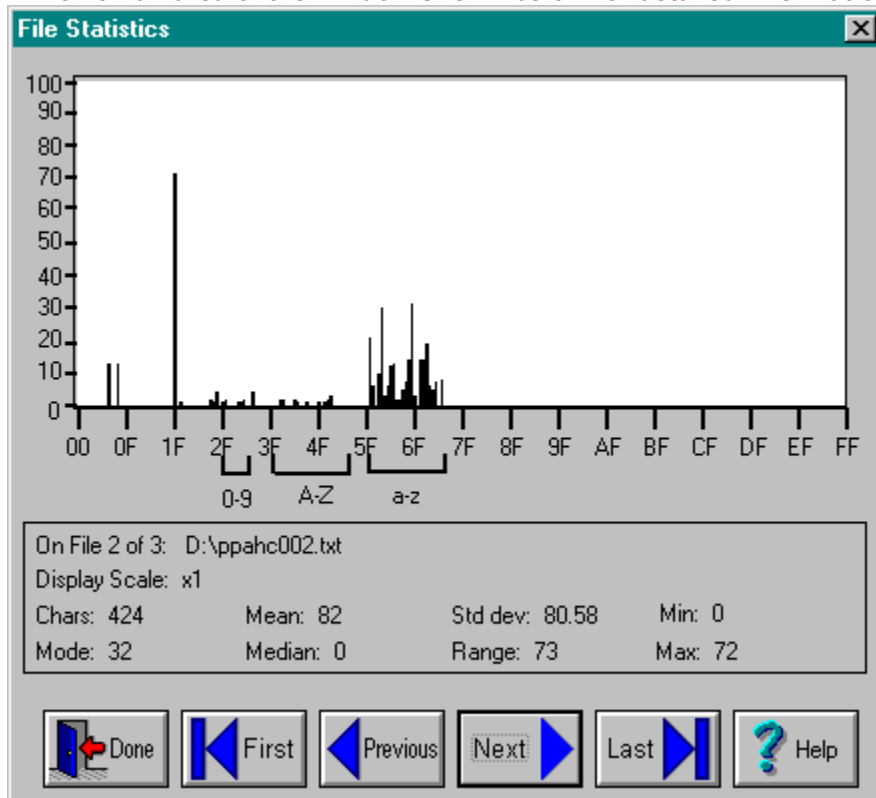
Help for File Statistics

The File Statistics function lets you look at any of your files in much the same way as someone trying to decrypt or break into your files. File Statistics performs statistical analysis on the file to see how well **Encrypt-It** protected your data.

The File Statistics screen shows a scaled frequency distribution histogram of character occurrences in the file. The closer the bars come to being all the same length, the better your data is hidden. Experts are able to use the frequency of occurrence of characters to decrypt files. This is possible because English (and most other Roman languages) have been well documented as to how frequently every character occurs in most types of human readable text.

ASCII characters range in value from 0 decimal (00 hex) to 255 decimal (FF hex). The x axis of the histogram shows the full range of ASCII characters in hex (due to space limitations). Below the hex labels are regions indicating where the more common characters are located, i.e., the numbers 0 - 9 and the letters A - Z and a - z. In normal text files, you will likely see tall bars on the histogram in these areas and for the space (20 hex), carriage return (13 hex) and linefeed (10 hex) characters.

Click on an area of the window shown below for detailed information on that part of the window.



To see the results (and value) of encryption, encrypt a text file, then compare the histograms of the original text file and encrypted file. You will be able to see how well **Encrypt-It** works at hiding the original information. After encryption, all your files will have virtually even distribution throughout the entire ASCII character set. It completely masks the type of source file.

Note: You may also use the numeric keypad keys to move around between selected files. Please ensure that the Num Lock key is not enabled. Use PgUp, PgDn, Home, and End in addition to the keyboard and mouse interfaces.

Help for Setting Program Preferences

Most of the options within **Encrypt-It** may be saved and automatically used each time you run **Encrypt-It**. The preferences dialog box lists the encryption and decryption defaults in a form you will normally see during the actual use of **Encrypt-It**.

[[Encryption](#) | [Decryption](#) | [Remove](#) | [Miscellaneous](#)]

Encryption: Select either a proprietary or DES level of encryption. Then choose whether you want to keep or erase the source files. If you want to erase them, specify the level of erasure.

Decryption: Choose whether you want to keep or erase the encrypted version of the file after you have decrypted the file. If you want to erase them, specify the level of erasure.

Remove: Specify your level of erasure when you remove files from your disk drive.

Miscellaneous: Set miscellaneous options for **Encrypt-It**. The Miscellaneous Preferences area allows you to specify that the current key is cleared when you switch between encryption and decryption modes or vice versa. For example, let's assume you have been careless -- you have encrypted several files and forgot to clear the in-memory key or to exit **Encrypt-It** before you rush off to a meeting. Another person could walk up to your computer before the key is automatically cleared (about 10 minutes) and possibly use the current key to decrypt one of your files. You can also enforce specifying a minimum key length of 5 to 40 characters. Finally you can hide the files list until you force the list to be displayed.

Number of Characters

This is the total number of all characters found in the file. This value includes all printable (displayable) characters and all special characters in the file.

Statistics Buttons

Use these buttons to move through the list of files for which you are viewing the statistics. Use the First button to view the statistics for the first file in your list. Use the Previous button to view the previous file in the list. Use the Next button to view the next file in the list. Finally, use the Last button to view the statistics for the last file in the list.

Click the Done button to return to the Main **Encrypt-It** window. Click the Help button for help with **Encrypt-It**.

Help for Clearing Key

The key is the secret element used in the encryption or decryption of files. The key can be compromised if you leave the computer unattended with **Encrypt-It** running. **Encrypt-It** will protect your files if, and only if, **YOU** do not compromise your key. Click this button, the Clear Key button, to clear the key before you leave the computer.

Additionally, if your computer is left idle (no keyboard or mouse activity) for 10 minutes with **Encrypt-It** running, your encryption key will be cleared automatically. This protects your key from unauthorized disclosure should you walk away from your computer while encrypting or decrypting files and forget to clear your key or exit **Encrypt-It**.

Help for Encryption Preferences

Encrypt Level - There are four levels of encryption included in **Encrypt-It**: Three Way Proprietary, Multilayer Proprietary Plus, Data Encryption Standard (DES) and Data Encryption Standard plus Cypher Block Chaining (DEC+CBC). For maximum security protection, use DES+CBC. Use one of the other two proprietary levels or DES only if you can't afford the longer encryption times of DES+CBC, or if you don't require the added protection for your data.

Encrypt Cleanup - Would you like your unprotected source file deleted from your drive after it is encrypted? **Encrypt-It** supports four ways to handle the cleanup. If you are protecting the files from someone else and you are the only person expected to see the files, then you will want to delete the original file. If you are encrypting the files before sending them via electronic mail, you may want to keep the original files for further editing. Then you will want to retain the original file.

Help for Decryption Preferences

Before decrypting a file you need to specify several items. Each is described below.

Decrypt Cleanup - What should be done with the original encrypted file after it is decrypted? Normally you will want to delete the encrypted file. **Encrypt-It** supports leaving the encrypted file intact, plus four levels of removing it. Recommend allowing **Encrypt-It** to delete the encrypted versions of files after you decrypt them to save disk space on your system.

Warn Before Overwriting Files: If you leave this box unchecked, **Encrypt-It** will overwrite any files with the same name as the name being used to decrypt the current file. Leaving it checked will prevent you from accidentally overwriting a file and losing data.

Median

The **median** is the central value in an ordered list of values. For example, the **median** of (1, 4, 7, 11, 23) is 7 because there are an equal number of values above and below the value 7. In the case of an even number of values, the **median** is calculated as the average of the two central values. For example, in (1, 4, 7, 11, 23, 31), the **median** is $(7 + 11) / 2 = 9$. Note that **median** is determined by position in an ordered list of values.

Help for Selecting Files

The Select Filenames window contains a file name field at the top where you can type in either a file name to append to the Selected Files list, or a file name filter using wildcard characters (* or ?) to list only certain files. For example, you can type in *.DOC to list only files ending in DOC.

Some common filters are available for displaying files in the Files list box. Click on one of the Group Operations for Files buttons to see only a certain group of files in the Files list. You can list all the files in the current directory (*.*) or only files of the form *.* or *.DOC.

You can also select one or more files by using the mouse and clicking once on each file name that you want to include in the selected files list.

When you type in a valid file name in the File Name field, or click on a file name in the Files list, the Size, Date and Time information for that file is displayed in the Selected File Information section of the window, and the Time to Encrypt/Decrypt File is also updated.

Notes:

1. For decryption, click the *.* button in the Group Operations for Files area to select only the files encrypted by **Encrypt-It**. (**Encrypt-It** automatically uses a tilde (~) as the first character of the extension for encrypted files.)
2. You can select or unselect all files in the Files list by clicking the Select All or Unselect All buttons with the mouse or keyboard.
 - a. Click the left mouse button or press the space bar to select a single file.
 - b. If a file has already been selected, clicking the left mouse button or pressing the space bar will unselect the file.
3. The files listed in the Files list will respond to double clicks ONLY if you have selected a single file. In the single file instance you will be able to immediately work with that file. If multiple files are selected, the double click will be mapped to a single click for file selection. This allows rapid single file selection while decreasing the chance of accidental processing of a list of files under a single file double click action.
4. **Encrypt-It** estimates the encryption/decryption time by encrypting a small block of data in memory and measuring how long it took. We have chosen a small time interval to limit the amount of time you have to wait. Any Windows related activity (such as moving the mouse) will decrease the amount of work **Encrypt-It** is able to perform during the timing test resulting in lower performance figures. Performance statistics are calculated the first time you use the file select function and maintained throughout the current session. That is why the first file select access take a little longer than subsequent uses. The performance statistics are calculated using a very small time interval, resulting in fairly rough estimates. The performance statistics estimates may vary by as much as 50% between different sessions. We felt the best tradeoff was to allow you to access the file area with as little delay as possible and to have the performance statistics be rough estimates.

Range

Range is the difference between the largest and smallest values in the list of values. For example, the **range** of (1, 4, 7, 11, 23) is 22.

Shareware Help: What is Shareware?

Shareware is copyrighted commercial software that you are allowed to try out before you make the purchase decision. It is a marketing concept, not a type of software.

Shareware marketing is typically used when the author doesn't have a huge advertising budget. High end software like Lotus 1-2-3, dBASE IV, etc. may have advertising budgets of over a million dollars. A full page advertisement in a magazine like PC Magazine can cost over \$10,000 an issue. Smaller software companies, like MaeDae Enterprises, usually don't have that type of advertising budget so shareware marketing is used.

Many people question whether software distributed via shareware is of as high a quality as the software they see advertised in commercial magazines. Good commercial advertising can sell almost any software regardless of its quality. Shareware must be of equal or higher quality than commercially available software for users to register. You, the user, have the opportunity to evaluate the shareware and find the real gems. With commercial software, you purchase the software and then hope it works as advertised.

Note: Don't feel guilty about passing around copies of shareware. You are helping the author distribute his software. Even though shareware is commercial software, you are encouraged to pass around evaluation copies!

Registration Benefits

1. The latest version of **Encrypt-It** with registration information screens removed.
2. Unlimited support - written or by phone.
3. Low cost upgrades.
4. Notification of enhancements.
5. All Data Encryption Standard (DES) functions are enabled. Because of this, it can't be sold outside the U.S. or Canada.
6. A Windows installation program. It completely automates the installation process, including the creation of a program group!
7. Extensive user's manual.

Notes:

1. Shareware relies on you, the user, for its existence. Your registration will help ensure **Encrypt-It** continues to improve. When you register, please take the time to fill out the suggestion form. We want **Encrypt-It** to evolve so it can better meet your needs.
2. DES functionality is disabled in the unregistered shareware version of **Encrypt-It**. This is mandated by the technology export restrictions placed on the DES algorithm by the U.S. Government. Users who register the program, and have a shipping address within the U.S. or Canada, will receive a version of **Encrypt-It** with the DES algorithm fully functional. Sorry for this inconvenience, but it's the law! **Encrypt-It** is not crippled in any other way. The proprietary encryption/decryption function of **Encrypt-It** is very secure and provides excellent data security.

Levels of File Wiping

Encrypt-It supports four ways to handle removing or deleting files. The first way is simply to not remove the file but only clear the file list. Three other methods are:

Delete the Source Files: Deleting the source files is identical to using the DOS Delete command. Keep in mind that this method does not erase the data from your drive; it merely marks the sectors so the operating system will know that the space occupied by that data is available. Anyone knowledgeable with the MS-DOS operating system can recover that data as long as the operating system has not overwritten those sectors with new data. There is little protection for your original data by using this method.

Either method of wiping the files overwrites the data so it cannot be easily recovered. Both methods take additional time. Different data patterns are written, one after the other, to ensure no one can ever access any removed files. You can change the number of passes performed in the Remove Preferences window.

Quick Wipe makes one or more overwrite passes over the original file.

Government Standard Wipe performs multiple passes to completely erase any trace of your data. This complies with the National Computer Security Center standard, CSC-STD-005-85, *Department of Defense Magnetic Remanence Security Guideline*, 15 Nov 85, Section 5.3.1.

Help IDs

```
#define HID_SHAREWARE          10
#define HID_BENEFITS           20
#define HIDD_GETDECRYPTINFO     0x2008D
#define HIDD_GETENCRYPTINFO     0x2008C
#define HIDD_GETFILENAMES      0x20088
#define HIDD_PREFERENCES       0x20082
#define HIDD_REMOVEFILES       0x20089
#define HIDD_STATISTICS        0x20086
// preferences F1 help ids for tabs
#define HIDD_PREFER_ENCRYPT      0x20098 **
#define HIDD_PREFER_DECRYPT     0x20099 **
#define HIDD_PREFER_MISC       0x2009A
#define HIDD_PREFER_REMOVE     0x2009B
// main window F1 help id - I think...
#define HIDR_MAINFRAME         0x20080 **
```

Tool Bar

The tool bar is a set of buttons that are short-cuts for some of the more commonly used items in the **Encrypt-It** menu.

Help for Miscellaneous Preferences

Enforce a Minimum Key Length: **Encrypt-It** requires a minimum of 5 characters to be effective at encrypting your files. However, if you wish to require that more than five characters are used, you can specify the minimum number of characters that **Encrypt-It** will allow for a key. Whether you allow **Encrypt-It** to automatically produce a key or you create the key manually, you will not be able to encrypt a file unless you use at least the minimum number of characters specified.

Clear Key Between Encryption/Decryption Mode Swaps: If you check this box, **Encrypt-It** will remember the key that you last used. The next time you encrypt a file or decrypt a file, the key field will already be filled in. You will still have to enter the key in the validation field in order to complete the encryption/decryption process. If you leave this box checked, you will have to enter the key and the validation fields in order to encrypt/decrypt files.

Hide the File List: Click this box to hide the list of files being encrypted or decrypted.

Title Bar

Besides containing the name of the program **Encrypt-It**, the Title Bar also contains four small icons. From the left, a small yellow, **Encrypt-It** icon is the Control Menu. Double click here to close **Encrypt-It**. At the far right of the Title Bar are three small icons. The left one, a horizontal bar, reduces **Encrypt-It** to a task on the Task Bar of Windows 95. This keeps **Encrypt-It** active but gets it out of the way if you are doing other tasks concurrently, such as word processing. The center icon toggles **Encrypt-It** between a full-screen program and a less-than-full-screen program, allowing you to either see nothing but **Encrypt-It** or to see any other applications running. Clicking the right icon, the X, will close **Encrypt-It**.

Exit Encrypt-It

Click this button to quit **Encrypt-It** and return to Windows 95.

Clear Selected File List

Clicking this button will remove all files from the Selected Files list in the main **Encrypt-It** window. You will be asked to confirm you want to clear the list before the list is actually cleared.

Help

Encrypt-It provides several ways of accessing its built-in help. They are:

1. Accessing the help through the pulldown menu options available on the main menu. This provides an easy way for you to call up the general area you are interested in.
2. Pressing F1 when NOT in a window which brings up general help. This will bring up an index for the help.
3. Using the help button available on many of the windows for very specific help. This is the best way to get help. The help will be specific and directly related to the current window.
4. Pressing F1 when in a window or a message box is displayed.

See the commands help screen for a quick index into all the different major commands. Note that you can use the help system to search for specific topics. An extensive cross reference of search topics is built into **Encrypt-It**.

Encrypt Your Files

USE THE BROWSE BUTTONS ABOVE (<< OR >>) TO MOVE FORWARD OR BACKWARD IN THIS DESCRIPTION OF ENCRYPT-IT. CLICK THE CONTENTS BUTTON TO RETURN TO THE TOP.

Now all that's left is to encrypt the files. To encrypt the files, you need to specify four things: a key, the directory to store the encrypted file, the encryption level, and the clean-up method. Select Encrypt from



the menu, or click the button.

The Key: There is nothing magical about a key. It is simply a group of letters and/or numbers (case sensitive) that will be fed into the encryption process to produce a file that no one else can read unless they have the same key. You can let **Encrypt-It** create the key for you, or you can use your own set of letters and/or numbers as a key. You need at least 5 characters. Choose a group of characters that someone won't easily guess, but preferably something that you'll remember. If you forget it, you won't get your original file back!

The Directory: Let **Encrypt-It** store the encrypted file in the same directory as the source file, or you can choose another directory on your system.

The Encryption Level: Choose one of four levels which run the gamut from fast but low protection, to slow but high protection. It depends on your requirements. If you're encrypting a casual note to a friend, you probably don't need high protection if you want to get it encrypted fast. If you transferring bank account numbers or credit card numbers, you will probably want to spend the extra time to provide the highest protection **Encrypt-It** offers. For small files, the difference is only a few seconds. For very large files on slower computers, you might wait many, many minutes. The choice is yours.

The Clean-up Method: This really has nothing to do with the actual encryption of your data, rather it has to do with what you want to do with the original file after you've encrypted it. Do you want the original data to remain on your system? If your system contains sensitive data and you leave your system unprotected when you're not around, you might want to encrypt your data and erase the original data to keep prying eyes from discovering your secrets. If you are encrypting a letter for transmission via electronic mail, you would probably encrypt for transmission and leave the original on your system in its original form.

There are four methods for cleaning up. The first is to leave the original file on your system. No protection is offered. Secondly, you can choose to "Delete the Source Files" which is identical to using the DOS Delete command. Keep in mind that this method does not erase the data from your drive, it merely marks the sectors so the operating system will know that the space occupied by that data is available. Anyone even slightly knowledgeable with the MS-DOS operating system can recover that data as long as the operating system has not overwritten those sectors with new data. There is little protection for your original data by using this method.

The third method deliberately overwrites the original file making typical methods to undelete files futile. However if your data is valuable enough and someone has expensive equipment capable of detecting remnants of magnetic fields, data can be recovered at significant expense.

Finally, the fourth method follows a US government method of overwriting the original file multiple times alternating zeros and ones which will practically eliminate any chance of data recovery even with the expensive magnetic detection equipment.

Decrypt Your Files

USE THE BROWSE BUTTONS ABOVE (<< OR >>) TO MOVE FORWARD OR BACKWARD IN THIS DESCRIPTION OF ENCRYPT-IT. CLICK THE CONTENTS BUTTON TO RETURN TO THE TOP.

Decryption is basically the opposite of encryption. You must specify three of the four items that were specified during the encryption process. The only thing you don't have to specify is the method. Since the files have already been encrypted, **Encrypt-It** will automatically detect the method and decrypt accordingly. You will need the original key in order to decrypt the files.



To decrypt the files, select Decrypt from the menu, or click the button.

Levels of Encryption

Proprietary - A lightning fast encryption method using a combination of exclusive OR (XOR), transposition, and substitution encryption processes. This is the basic level of encryption you get with **Encrypt-It**.

Proprietary+ - You also use several additional layers of proprietary encryption in a method we call Proprietary+.

DES - The slower, but very secure, Data Encryption Standard (DES) encryption is added to our proprietary methods.

DES+CBC - The most secure level is the DES+CBC. The price you pay for the added security is time. It takes longer to use this method of encryption, but you get the very secure Data Encryption Standard (DES) encryption plus Cipher Block Chaining (CBC) on top of our proprietary methods. This provides the ultimate in data encryption; we call it DES+.

Remove Files Preference

Encrypt-It provides four methods for removing files. The first is to leave the files as they are but clear the file list. The other three are: Deleting files, Quick Wiping files, or Government Standard Wiping files. Together these four methods meet a wide variety of individual needs.

You can also force **Encrypt-It** to warn you one more time before it actually removes the files from the disk.

Histogram

This histogram lets you view any of your files in the same way as someone trying to decrypt or break into your files. Statistical analysis is performed on the file to see how well **Encrypt-It** protected your data. The histogram graphs the American Standard Code for Information Interchange (ASCII) character set (all 256 characters, 00 to FF hex) along the x axis. Below the hex labels are regions indicating where the more common characters are located, i.e., the numbers 0-9 and the letters A-Z and a-z.

The number of occurrences of each character in the current file is shown along the y axis. Character occurrences in a file are normalized to the range 0-100. To determine the actual number of occurrences for a specific character in a file, multiply the height of the bar for that character by the display scale shown above the histogram.

Text files are usually characterized by having an equal number of occurrences of the characters at 0Ah (the linefeed) and 0Dh (the carriage return). This character pair represents the hard carriage return at the end of a paragraph of text. Another feature characterizing text files is a spike at 20h (the space character). The space is typically the most frequently occurring character in text files.

Before a file is encrypted, one will see large quantities of spaces and carriage returns, and most other characters will fall in the ranges of the numbers 0-9 and the sets of upper and lower case letters (a-z and A-Z). This sample is an unencrypted file. After a file is encrypted, the histogram will show that other ASCII characters have been introduced in the file. The occurrences of characters now does not follow any statistical pattern, making it difficult to impossible to use statistical analysis to decrypt this file.

Decryption Setup

The Key: The key you enter and verify must be exactly the same as the key that was used to encrypt this file. It is a group of letters and/or numbers (case sensitive) that will be fed into the decryption process to recover the original information that was encrypted. If you don't have the correct, you will not be able to recover the original information.

The Directory: Let **Encrypt-It** store the decrypted file in the same directory as the source file, or you can choose another directory on your system.

The Clean-up Method: Choose one of [four methods for cleaning up](#).

Warn Before Overwriting: If you leave this box unchecked, **Encrypt-It** will overwrite any files with the same name as the name being used to decrypt the current file. Leaving it checked will prevent you from accidentally overwriting a file and losing data.

Clear Key Between Encryption/Decryption Mode Swaps: If you check this box, **Encrypt-It** will remember the key that you last used. The next time you encrypt a file or decrypt a file, the key field will already be filled in. You will still have to enter the key in the validation field in order to complete the encryption/decryption process. If you leave this box checked, you will have to enter the key and the validation fields in order to encrypt/decrypt files.

Removing Files

Removal Method: Choose one of four methods to remove these files from the disk.

Extra Warning Before Removing Files: Check this box to force **Encrypt-It** to confirm that you really want to delete these files from your disk.

View

Selecting View from the menu gives you three choices to customizing the main **Encrypt-It** window:

View Tool Bar: Displays or hides the tool bar.

View Status Bar: Displays or hides the status bar at the bottom of the main **Encrypt-It** window.

View File List: Displays or hides the list of files that you have selected for encryption or decryption.

