Encrypt-It for Microsoft Windows

High Performance Secure Data Protection for Windows

You can access help for **Encrypt-It** two ways: pressing F1 (when no menu is highlighted) or using the Help pulldown menu. General help areas are listed below. Each help area will provide a general overview of the function. You can view them by clicking the mouse button on the topic or by using Help Search.

Encrypting Files - File encryption procedures
Decrypting Files - File decryption procedures
File Statistics - File character distribution, standard deviation, etc.
File Delete - File deletion procedures
File Wipe - Secure file deletion (Quick and Gov't Std)
Clear Key - Clearing your encryption / decryption key
DES - The Data Encryption Standard

Note: First use the File Select menu to pick your files. Then select the action to be performed on the files. Menu items will be grayed at times to show when they are inactive.

Help Usage Overview

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 dialog box which brings up general help. This will bring up an index for the help.
3. Using the help button available on many of the dialog boxes for very specific help. This is the best way to get help. The help will be specific and directly related to the current dialog box.
4. Pressing F1 when in a dialog box or message box. That will bring up this screen.

See the commands help screen for a quick index into all the different major commands. Please 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-It Commands Index

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

File
- Select
- Remove
- File Statistics
- Preferences
  - Encrypt Level
    - DES
    - Proprietary
  - Encrypt Cleanup
    - Delete Source Files
    - Wipe Files (Quick)
    - Wipe Files (Gov't Std)
  - Decrypt Cleanup
    - Delete Source Files
    - Wipe Files (Quick)
    - Wipe Files (Gov't Std)
  - Decrypt Overwrite
    - Warn Before Overwrite

Encrypt

Decrypt

Clear Key!

Email
- File to Email Conversion
- Email to File Conversion

F1=Help
- Index
- Commands
- Print Invoice
- About Encrypt-It

Proprietary Encryption Techniques

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 (DES)

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. NSA has as one of its primary functions 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. This provided 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**) **CANNOT** be exported outside the U.S. or Canada due to the level of data protection they provide.

Encrypting Files

Encrypt-It provides several levels of data encryption to completely protect your important data. They are:

Proprietary - Lightning fast encryption using a mixture of XOR, transposition, and substitution encryption methods. This is the basic level of encrytion.

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

DES - Optionally add the slower, but very secure, Data Encryption Standard (DES) encryption on top of our proprietary methods.

DES+CBC - Optionally add the slower, but 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+.

When you encrypt files, 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.

Note: Because of the level of protection provided by DES, **Encrypt-It** CANNOT be sold outside the U.S. or Canada!

Decrypting Files

Decryption is the opposite of encryption. **Encrypt-It** takes the encrypted file and your key to activate the decryption process. **THERE ARE NO "BACK DOORS" IN ENCRYPT-IT.** If you forget the key used to encrypt the file, you can forget about ever decrypting the file.

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

Removing Files

Encrypt-It provides three methods for removing files. The methods are Delete Files, Wipe Files (Quick), and Wipe Files (Gov't Std). We have provided three methods in order to better meet a wide variety of individual needs.

The remove dialog box contains an option to give you an extra warning before removing files. This is designed to provide you one last chance to say no before the files are removed. See the Preferences area for more information on user installable options.

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.

Other useful statistics are available on the File Statistics screen. Each is explained here:

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

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.

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.

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.

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

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.

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

Max: ***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***.

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.

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**.

Specify your encryption and decryption preferences. Then, use the save option to save the preferences to disk. **Encrypt-It** saves the preferences in a file called EIW.INI in the **Encrypt-It** startup directory. EIW.INI will be automatically loaded and used each time you bring up **Encrypt-It**. Please ensure Windows has the proper default directory specified for **Encrypt-It**.

The preferences area also allows you to optionally specify that the in-memory key is to be cleared when you switch between encryption and decryption modes or vice versa. For example, lets assume you have been careless -- you have encrypted several files and forget to clear the in-memory key or to exit **Encrypt-It** before you rush off to a meeting that you just remembered. Another person could walk up to your computer before the key is automatically cleared (about 10 minutes) and possibly be able to use the in-memory key to decrypt one of your files. Using this option would ensure your key is cleared the instant they try to decrypt any files.

File Delete

The File Delete menu lets you quickly remove any number of files from a directory. Tag as many files as you want and they will be quickly deleted after selecting OK. This is the same type of file deletion that occurs when you use the DOS delete command. For more secure deletion, use the File Wipe command.

File Wipe

The File Wipe function is like File Delete with the added function of securely overwriting the space on the disk occupied by the file, then it deletes the file. This can take a little time. Different patterns are written, one after the other, to ensure no one can ever access any removed files.

If you want just a simple fast deletion, use the File Delete option.

File Wipe comes in two levels:

Quick Wipe makes one overwrite pass on the original file.

Gov't Std performs three 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.

Clear 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. Use the Clear Key option 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**.

Encrypt Dialog Help

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

Encryption key - This is the unique key that only you should know. Nobody else can access the file unless they know the key. The key must be at least 5 characters long and may contain numbers, letters, punctuation and spaces. Note that the key is *case sensitive*. We recommend you do not use a space character as the first or last character in your key since leading and trailing spaces are easy to forget. For security reasons, *s will be shown when you enter the key. You will also need to verify the key by entering it again in the verify key area. **Encrypt-It** will compare the two keys and will require that the two keys be the same before allowing encryption to take place.

Output directory - Once the file is encrypted, where should it be placed? By default, the file will be placed in the current directory as it is encrypted. You may send the encrypted file to another drive or directory by entering a path name here. Any valid drive on your system, including network and floppy drives, may be used as a destination.

Output file name - **Encrypt-It** automatically provides a suggested file name for this entry. If you are encrypting a single file, the file name entered here will be used as the name of the encrypted version of that file. If you are encrypting multiple files, **Encrypt-It** will use the file name for the *first file only.* The encrypted versions of the remaining files will be automatically named using a combination of the original file names and the extension ".~00" for the first file, ".~01" for the second, etc.

Encrypt level - Recommend using DES+CBC. Use one of proprietary levels or DES only if you can't afford the longer encryption times of DES+CBC, or need slightly less secure protection for your data.

Encrypt cleanup - Would you like your unprotected source file erased after it is encrypted? Normally you will want to delete the original file. **Encrypt-It** supports leaving the encrypted file intact, plus three levels of removing it. Choose the cleanup level you need. With the Gov't Std file wipe, nobody will ever be able to access your unprotected file again!

Notes:

1. The **Selected File Name(s)** area shows the name(s) of the file(s) you selected for encryption. If you selected multiple files, the names of the first three files are displayed in a scrolling listbox. To see the remaining files you selected, click the mouse on the scroll bars at the right end of the listbox.

2. The **# Files** area shows how many files you selected to encrypt.

3. The **Make Key** button allows **Encrypt-It** to automatically generate a 10 character long key for you. The key is randomly generated using upper and lower case alphabetic characters only. Other characters, such as numbers and punctuation, won't be used in the automatically generated key because it is often hard to discern a zero (0) from an upper case letter O, a one (1) from a lower case letter l, or an apostrophe (') from an accent mark (`) . However, you may modify the automatically generated key by using any key on your keyboard. In any case, you are still responsible for keeping the key secret. **Encrypt-It** can't do this for you. Please note that the Make Key button updates the key based on a random number. The random number generator is initialized with a system clock time seed each time you use the Encrypt Dialog. The random key will become your first key. You will ba asked to type the key a second time for verification. Since *s are shown on the screen for the key, it is essential that you enter the key a second time for verification.

4. When you simply **delete** a file, it isn't really erased. Someone can come along later with a disk utility and access your file. You should be aware of this. Only **wiping** a file destroys the original data and denies access to its contents.

Decrypt Dialog Help

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

Decryption key - What key was used as the key to encrypt the file? If you don't know this, you won't be able to decrypt the file. Note that the key is *case sensitive*. For security reasons, *s will be shown when you enter the key. You will also need to verify the key by entering it again in the verify key area. **Encrypt-It** will compare the two keys and will require that the two keys be the same before allowing decryption to take place.

Output directory - Once the file is decrypted, where should it be placed? By default, the file will be placed in the current directory as it is decrypted. You may send the decrypted file to another drive or directory by entering a path name here. Any valid drive on your system, including network and floppy drives, may be used as a destination. The original file's name is encrypted and embedded in the encrypted file's header so you don't need to provide it during decryption. Additionally, the date and time of the decrypted file will be the same as the original file before it was encrypted.

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 three 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.

Notes:

1. The **Selected File Name(s)** area shows the name(s) of the file(s) you selected for decryption. If you selected multiple files, the names of the first three files are displayed in a scrolling listbox. To see the remaining files you selected, click the mouse on the scroll bars at the right end of the listbox.

2. The **# Files** area shows how many files you selected to decrypt.

3. When you simply **delete** a file, it isn't really erased. Someone can come along later with a disk utility and access your file. You should be aware of this. Only **wiping** a file destroys the original data and denies access to its contents.

File Select Dialog Help

Selecting files is very easy. The screen shown before you contains a filename box at the top where you can type in your desired file's name or use a wildcard like *.DOC for all files ending with DOC.

Once a valid file is selected, the file related information will be updated. Information on the file's size, date, estimated encryption/decryption time, etc. will be displayed in the boxes on the right.

A special group operations box is available for selecting and unselecting all the files shown in the files listbox. Several common masks have been added (*.* for all files, *.~* for all encrypted files, *.A* for all mail files, etc.) to make selection easier.

Notes:

1. For decryption, use an initial file name mask of ***.~*** to select all encrypted files. **Encrypt-It** automatically uses a tilde (~) as the first character of the extension for encrypted files. **Encrypt-It** automatically uses a A as the first character of the extension for email files (A was chosed as being unlikely to conflict with other common file extensions). Then use the group operations area to select all files shown in the files list box.

2. You can select and unselect files in the File Select list box using the mouse or keyboard.

    a. Click the left mouse button to select a single file, or press the space bar to select the file.

    b. If a file has already been selected, clicking the left mouse button or pressing the space bar will unselect the file.

3. For the Drives/Directories list box, ensure there is a diskette in the drive before selecting it. Otherwise, you will get an error message saying **Encrypt-It** can't access the drive.

4. The Selected File Information area will contain details on the file selected if it is a valid, unique filename and the file exists. This information will be updated constantly as you change drives or modify the file's name.

5. The File Select list box 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.

6. **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.

File To Email Conversion

Many people today communicate electronically using a number of different information services. These electronic information services can't handle the normal files that we use in our computer. Because of this, **Encrypt-It** provides functions to convert files into different formats to make electronic communications easier.

Typical electronic services today limit the information that you can transmit over it to somewhere around half of the normal character range. **Encrypt-It** provides conversion routines to change your files to and from email.

Encrypt-It allows you to choose a number of different options for the file to email conversion process. Please note that you are not able to alter the source files that you have selected using the file select option. You are able to specify the destination directory and destination filename on a file by file basis. To do this, use the convert option and specify new information for each individual file. Use the convert all option only if you want **Encrypt-It** to use its auto generated file names and specified path.

Information services typically allow a narrow range of characters in file names. Because of this, **Encrypt-It** generates file names where the extension starts with an A. The email name will normally default to the main body of your file's name followed by an extension of A00. This extension will automatically be bumped up to A01, A02, etc. to guarantee that the automatically email name will be unique. **Encrypt-It** will automatically restore your email file back to its initial file name during the reverse email to file translation.

Notes:

1. Due to the limited email character range, you can expect a file to grow by about 40% as it is converted from standard file format to limited email format.

2. **Encrypt-It** stores the initial filename, date, time, and length within the email file. This information will be used later when you convert the file back into standard file format from email.

3. **Encrypt-It** adds a cyclic redundancy check (CRC) into the email file structure for extensive error checking. During email to file conversion, this information can be used to let you know when your email has been corrupted during the file transfer through the electronic information service.

Email To File Conversion

Encrypt-It provides this function to convert email back into normal file format. Please note that this function **ONLY** works with email files previously generated using **Encrypt-It**. All specifics of the original file will be restored using this function to include initial file name, date, time, and size.

Notes:

1. Do not try to translate anything but **Encrypt-It's** special email format using this command. Other email formats do not embed all the addition information to allow restoration of all aspects of the initial file. **Encrypt-It** checks each email file and will prompt you with the initial file name provided you haven't chosen the convert all command. This command uses the embedded file name from the email to automatically convert all the selected email files in a batch mode.

2. This area of **Encrypt-It** was designed to minimize the amount of information you need before you can convert from email back into regular file format.

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

Registration benefits include:

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 hard copy 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.