Encrypt-It for Microsoft Windows

High Performance Secure Data Protection for Windows

Help for **Encrypt-It** is accessed two ways: pressing F1 (when no menu is highlighted) or using the Help pulldown menu. General help areas are listed below. 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.

Encrypt-It Commands Index

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.

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 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 tested 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.

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 US 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. Lightning fast proprietary methods are provided as the basic level. You can optionally add the slower, but very secure, Data Encryption Standard (DES) encryption 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 US!

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.

File Statistics

The File Stats 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 Stats 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.

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 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 password that only you know. Nobody else can access the file unless they know the password. The password must be at least 5 characters long and may contain numbers, letters, punctuation and spaces. Note that the password is *case sensitive*. We recommend you do not use a space character as the first or last character in your password.

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 - Only supported when you are encrypting one file at a time. **Encrypt-It** automatically gives you a suggestion. If you are encrypting multiple files, **Encrypt-It** automatically names the encrypted files 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. Use proprietary only if you can't afford the longer encryption times of DES, or need only minor 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.

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 password 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 password is *case sensitive*.

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 file's name is embedded and encrypted in the encrypted file's header, so you don't need to provide it.

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.

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.

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.

2. Several methods are supported for selecting files in the File Select list box.

   a. Click the left mouse button to select a single file, or drag the highlight with the left mouse button held down to select a contiguous group of files.

   b. Select a file with the mouse. Then, use the Shift key plus the left mouse button to select another file. This selects the entire range of files between the two selected files.

   c. Use the Ctrl key plus the left mouse button to select groups of files. This method is the most powerful and flexible. Files don't have to be next to each other. You can select several groups of files at a time.

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.

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 no additional information screens.
2. Unlimited support - written or by phone.
3. Low cost upgrades (only $10 plus $5 S&H).
4. Notification of enhancements.
5. The registered version of **Encrypt-It** has all the Data Encryption Standard (DES) functions enabled. Because of this, it can't be sold outside the U.S. or Canada.

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.