Mac*Encrypt*

File Encryption for the Macintosh

Version 1.0

by
J. Clarke Stevens

Mac*Encrypt*

What Is It?

MacEncrypt is an application that uses the Data Encryption Standard (DES) to scramble the bits of your files until they are totally unrecognizable.

Why Would I Want It?

Scrambling your bits (or encrypting) is useful if you don't want other people knowing what is in your files. The bits are scrambled with a secret key that you type in. Unless someone discovers your key it is practically impossible for them to unscramble (decrypt) your files.

MacEncrypt is intuitive and convenient. You can encrypt files from within the application using standard file dialog boxes or use the "drag and drop" technique to encrypt one or many files automatically. You can decrypt a file from within the application or by simply double-clicking on an encrypted file.

How Do I Use It?

You can probably run MacEncrypt without reading this document, but just for the record, here is what you need to do.

Encryption

Encryption is the process of reading an unsuspecting file, scrambling its bits with an encryption password, and writing the

scramble bits out to the file again. MacEncrypt uses the Data Encryption Standard (DES) for file encryption. If you want to know more about DES, a brief overview is included in this document.

Selecting the File

The first step in the encryption process is selecting a file or group of files to be encrypted. This can be done in two ways with MacEncrypt. The method is to open the file from within MacEncrypt. The second method is to use the "drag and drop" technique from the finder.

From the Application

To select a file for encryption from the application, open MacEncrypt by double-clicking on its icon (the TOP SECRET manila folder with an "application" hand). You should see a menu bar appear with "File" and "Options" menus. There is also an "About MacEncrypt" item under the apple menu.

Choose the “Encrypt…” item from the “File” menu and you should get a standard file dialog box. Use the regular techniques for selecting a file to be encrypted.

From the Finder

You can also select a file or group of files to be encrypted using the “drag and drop” technique. To do this, use the shift-click combination to select any files you want to encrypt. Release the shift key and click on one of the hilighted files. While holding down the mouse button, drag the files and drop them (release the mouse button) on the MacEncrypt application icon. MacEncrypt will open automatically and ask for an encryption key.

Entering the Key

The Data Encryption Standard requires a user-supplied encryption key. After you have selected a file to encrypt, a dialog box will appear requesting that you type an encryption key. The encryption key is a string of typable (and possibly some untypable) characters. All the standard letters, numbers, and symbols on the keyboard can be used. In addition, some of the keys that have no “character” associated with them (such as the “home” key) can be used to make your key particularly hard to guess.

It is important to note that the Data Encryption Standard only uses 64 bit (i.e. eight character) keys. Anything you type for the key that is beyond eight characters is ignored, but longer strings are supported so that any length of password (up to 255 characters) can be used for convenience. A password of zero length is also allowed.

Visibility

You can have the passwords you type be visible or invisible. In the visible password mode, characters will appear on the screen as you type them. In the invisible mode, a bullet character (•) will appear instead of the character you type. MacEncrypt remembers the characters you type, but someone looking over your shoulder will not be able to see the password. You can turn password visibility on and off by selecting the “Visible Passwords” item under the “Options” menu.

Verification

There is a danger in using invisible passwords that you might accidentally type a character in your password and not realize it. If a file were encrypted with such a password, you would probably not be able to type the right password during decryption and your file would be lost forever. In order to avoid this situation, you

are required to type the password twice before encrypting a file. If the passwords match, the file will be encrypted. If they don't match, you will be asked to type them again. This is true for visible as well as invisible passwords because there are some characters which can be typed but not drawn on the screen. These can be useful in passwords, but you need to type them intentionally. Password verification can help ensure that you know your password.

Encrypting

When your password is verified, MacEncrypt immediately begins to encrypt the selected file. During encryption, an animated cursor (a Morse code key set) will indicate that the file is being encrypted. MacEncrypt encrypts about three kilobytes per second on my

Mac IIsi. Your mileage may vary. When the encryption is complete, the cursor will return to normal. If you started the encryption from within MacEncrypt, you can select another file to encrypt or decrypt or quit the application. If you started from the finder, MacEncrypt will automatically quit and return you to the finder.

It is handy to put MacEncrypt on the desktop near the garbage can. When you want to encrypt a file, simply drag it to the MacEncrypt Icon and type the encryption password. The encryption will take place and you will be returned to the finder ready to continue your tasks.

Decryption

Decryption is the process of reading an encrypted file and unscrambling its bits using a decryption password. If the password is correct, the file will be returned to its original unencrypted state.

Selecting the File

The process for selecting a file to encrypt is similar to the process used to select a file to encrypt. You can select the file from within MacEncrypt using standard file dialog boxes or start MacEncrypt from the finder by using the "drag and drop" technique or by double-clicking an encrypted file.

From the Application

To select a file for decryption from within MacEncrypt, first open MacEncrypt by double-clicking on its icon. The MacEncrypt menu bar should appear. Choose the "Decrypt…" item from the "File" menu. A standard file dialog box should pop up. You can then select the file to be Decrypted using the standard file dialog navigation techniques.

From the Finder

There are two ways to start the decryption process from the finder. The first process is using the "drag and drop" technique. Simply use the shift-click method to select the files to decrypt, then drag and drop the files on the MacEncrypt application icon. Each of the files will ask for a password and then be decrypted. The encryption process can also be started this way.

The second way to initiate decryption from the finder is to double-click on an

encrypted file or to select a file and choose “Open” from the finder “File” menu. Since encrypted files belong to the MacEncrypt application, double-clicking on an encrypted file will start the process to open the file using its creating application (MacEncrypt).

Entering the Key

After the file is selected, you will be requested to supply a decryption key. The MUST be the exact same key used to originally encrypt the file. If you type the right key, the file will be decrypted, if you type the wrong key, nothing will happen.

Visibility

The visibility option in decryption works just as it does in encryption. If the visibility option is on, the characters will appear as you type them. If it is switched off, only bullet characters (•) will appear. You can toggle the visibility option by selecting the "Visible Passwords" item under the "Options" menu.

Verification

It is only necessary to type the decryption password once since typing the wrong password will only mean that you have to try again. If you type the wrong password, a dialog box will appear indicating that the password entered was incorrect. If you type the correct password, decryption will begin immediately.

Decrypting

As in the encryption process, during decryption an animated cursor will indicate that the file is being decrypted. Decryption occurs at the same rate as encryption (about 3 kBytes/sec on my Mac IIsi). The cursor will return to normal when encryption is complete. If the decryption process was started from within MacEncrypt, you will be returned to MacEncrypt and can encrypt or decrypt other files. If you started from the finder, either the next file in the group will be processed (encrypted or decrypted) or control will be returned to the finder.

Options

There is only one item in the "Options" menu. This is the "Visible Passwords" item. If the item is marked with a check mark, passwords will be visible and characters will appear as you type them from the keyboard. If the item is not check-marked, password will show up as a string of bullet-characters (•). The status of this flag is saved when you quit MacEncrypt, so you don't need to worry about adjusting it each time the application is started.

How Do I Pay For It?

MacEncrypt is NOT free. It is shareware. If you keep it for

more than a month (30 days) you are obligated to pay for it. Please send the shareware fee of $10.00 (U.S.) to:

J. Clarke Stevens
MacEncrypt
1118 Forrest Blvd.
Decatur, GA 30030
U.S.A.

As a benefit of registration, I will provide limited support (limited to e-mail or U.S. Mail) and will be more likely to implement suggestions you have for future versions. I will also notify you of all future versions of the program as well as other programs I produce. Support shareware to encourage the development of quality, try and buy, affordable software.

How Does It Work?

Data Encryption Standard (DES)

For those of you who are curious, I have included the following information on the history of the Data Encryption Standard and the encryption methods used in DES. Much of this information is a summary of the presentation by Dominic Welsh in his book *Codes and Cryptography* (Oxford Scientific Publications, 1989).

DES History

Motivated by the increase in digital data communications in the early seventies, the U.S. government decided to adopt a standard for data security. The National Bureau of Standards sponsored a search for a scheme that could be implemented on a single chip and mass-produced. The winner of the search was IBM.

The scheme proposed by IBM was an adaptation of a scheme they had previously developed called Lucifer. The main difference between Lucifer and the Data Encryption Standard is the size of the encryption key. Lucifer uses a 128 bit key while DES uses a 64 bit key (eight of which are discarded by the algorithm).

The size of the key has generated quite a controversy. A paper by M.E. Hellman and W. Diffie of Stanford University pointed out that a key length of 56 bits is uncomfortably short. A subsequent New York Times article by D. Kahn fueled the fire. As a result, the National Bureau of Standards sponsored workshops to discuss the issue. The problem was further complicated by the refusal of IBM do disclose some of the design principles used because they were classified.

The conclusion of most attending the workshops was that DES would be acceptably secure for about 10 years (DES was adopted in 1977). However, the only known method for breaking the code is an exhaustive search. That means 2^{55} attempts. Since with current computing power, this is not practical, your data is reasonably safe. You don't need to worry about someone breaking you code with a personal computer.

Encryption Methods in DES

The following methods are used in DES:

1. A 64-bit block is broken into left (L) and right (R) halves.
2. The right half of the block (R) becomes the input to the left half (L') of the next

stage.

3. The input to the right half of the next stage (R') is calculated by
   a. scrambling and diffusing R to make it 48 bits,
   b. forming the modulo-2 sum with one bit of the key,
   c. passing it through the infamous S-boxes (a non-linear transform) to make it 32 bits,
   d. permuting it by the operation P,
   e. summing it modulo-2 with L to get R'.
4. Finally, the left and right halves are combined again using the inverse of the initial permutation matrix.

Each of the S-boxes transforms six input bits to four output bits. There is an S-box for each bit of the key. For a more detailed explanation, read the section on DES in the book by Dominic Welsh.

How Hard Is It To Break?

Breaking the DES algorithm is equivalent to solving an NP-hard (nondeterministic polynomial time) problem. Solving algebraic equations modulo 2 is an NP-hard problem. There is no fast algorithm known for solving any NP-hard problem. In other words, breaking a cryptosystem based on an NP-hard problem is equivalent to finding a fast algorithm to solve the problem. DES is based on an NP-hard problem. The only way known to break it is to use an exhaustive search of all the 2^{55} possible passwords. This would take the fastest known computer years to complete. Your data is pretty safe, but theoretically not totally safe, if you encrypt it using DES. The weak link is the password, if someone discovers your password, your data is at risk!

Who Is Responsible?

MacEncrypt was written by J. Clarke Stevens using knowledge of the Data Encryption Standard gleaned from a graduate class on codes and cryptography in the department of Electrical Engineering at Georgia Tech. I was disappointed when I could find no simple shareware program for implementing the algorithm on the Macintosh, so I decided to fill the void myself. The DES engine is based on public domain DES code written by Phil Karn and Jim Gillogly. MacEncrypt was written using Symantec's THINK C.

Once you register, I will be happy to respond to bug reports and suggestions you may have for future versions of MacEncrypt.

Bug Reports and Suggested Improvements

You can send bug reports and suggestions for enhancements to MacEncrypt to me using the following methods.

Internet

This is my preferred means of communication. I can usually respond in a matter of minutes. My address is:

clarke.stevens@gtri.gatech.edu

FidoNet

I also communicate via FidoNet. This takes a bit longer, but you can just write up a note on your computer and you don't need to buy a stamp. My address is:

1:133/110.2

U.S. Mail (SnailMail)

If you can't send e-mail, you can always reach me eventually with conventional mail at:

J. Clarke Stevens
MacEncrypt
1118 Forrest Blvd.
Decatur, GA 30030
U.S.A.

Liability

I have tested this program quite extensively and have used it on my own files. I believe it to be quite safe and have found no evidence to the contrary. That notwithstanding, the following statement applies.

Legal Junk follows:
MACENCRYPT IS A COPYRIGHTED COMPUTER PROGRAM OF J. CLARKE STEVENS AND SUPPLIED AS-IS. J. CLARKE STEVENS MAKES NO WARRANTIES, EITHER EXPRESS OR IMPLIED REGARDING THE ENCLOSED SOFTWARE PROGRAM OR ITS SUITABILITY FOR ANY PARTICULAR PURPOSE. J. CLARKE STEVENS WILL NOT BE LIABLE FOR ANY DAMAGES THAT MAY OCCUR AS A RESULT OF USING THIS PROGRAM.