Enigma

Version 2.8 User's Guide

Privacy for Everyone

Next Wave Software, Inc.

Released December 1998
System 7.0 or later required

Table of Contents

What is Enigma?

Enigma is an application designed to completely protect your privacy at very low cost. If you would prefer your neighbors not see your personal finance data, your coworkers not see your performance appraisal, or your competitors see your trade secrets then Enigma is an application you will find very valuable.

It is easy to use a computer to search for, analyze and copy data. Only encryption such as that provided by Enigma can defeat this easy access.

Although Enigma is named after the famous German encryption system of World War II, it implements the modern Data Encryption Standard (DES). DES is the current standard for commercial and unclassified data protection. The freeware version distributed on a variety of networks and local BBSs implements a much weaker level of encryption based on the DES algorithm. This weaker level of encryption is proof against casual snoopers and those without access to sophisticated computers. It is not adequate protection against a knowledgeable and dedicated attack. If you need the stronger protection you can purchase a version of Enigma that implements the complete DES algorithm.

US law does not allow export of the full DES algorithm outside the United States and Canada. Stupid though it sounds, DES is considered a "munition" by the US government. Export of DES outside the United States and Canada is a rather severe felony if the Justice Department should decide to prosecute. The freeware version implements a limited version that is significantly less secure so it does not violate US law. Technical details are discussed in the section describing the DES algorithm.

Please write your members of Congress and let them know you oppose restrictions on strong cryptography. Support non-government encryption solutions such as that provided by RSA and PGP and ignore government standards with built in back doors such as Clipper. [Yes I know DES is a government developed algorithm, but at least it contains no obvious back doors, and has survived the test of time.]

Enigma 2.8 Requirements

Enigma 2.8 requires System 7.0 or later (fully compatible with Mac OS 8.5). It requires about two megabyte of memory, and about 400K of disk space. There are no known hardware or init conflicts.

What's new in version 2.8?

- Multiple vaults can now be opened and files can be dragged between vaults.
- Minor bug fixes, and updates to keep the software fully compatible with system 8.5.

- Updated contact information for Next Wave Software, Inc.

Getting Started

The simplest operation you can perform with Enigma is to encrypt or decrypt a single file. There are two ways you can select a file. First you can drag the desired files to the Enigma icon and release the mouse button. You will be prompted for a key. The files are automatically encrypted and/or decrypted depending on their type. Depending on the options you have selected you will need to enter a key and output filename for each file dragged to Enigma.

Alternatively you can select files from within the Enigma Application by selecting "Open..." from the Enigma file menu.

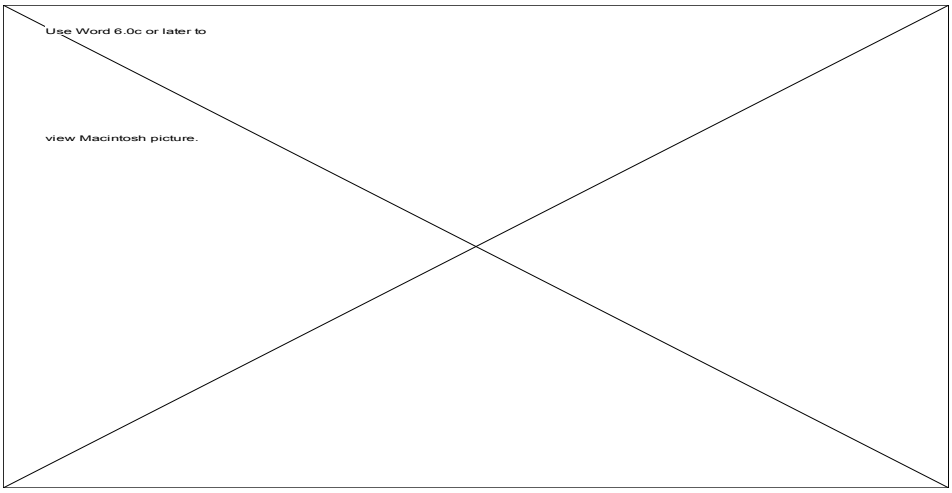

Figure 1: Key Entry Dialog Box

Enigma determines if the file should be encrypted or decrypted. However, you can manually override this during key entry if you desire. The only reason to ever override Enigma's default selection is if you are double or triple encrypting a file; or decrypting a file encrypted on a PC that does not have the default file extension. Figure 1 shows the key entry dialog box.

If you have the freeware version of Enigma you will not be able to deselect the "Use Limited DES" check box.

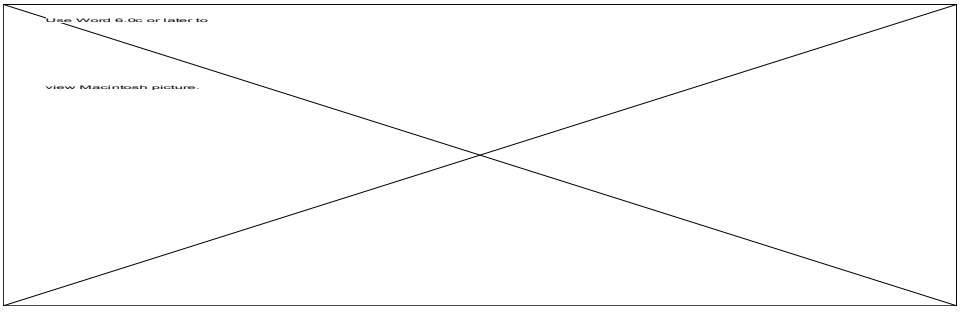

Figure 2: Encryption Status Dialog Box

During encryption or decryption a dialog box showing progress will be displayed. Figure 2 shows this dialog box. You can select cancel at any time to abort the process (Any file that would have been overwritten by the encryption operation will be restored). You can also move the status window around the screen, or push Enigma into the background by clicking on the window of another open application. In the background Enigma will continue to encrypt/decrypt at a somewhat slower pace. Cryptography is very CPU intensive so expect some slowdown of other applications even when Enigma is in the background.

Enigma has many options that will allow you to customize and streamline the encryption/decryption process. Refer to the section *"Customizing Enigma"* for details.

Vaults

Vaults are like a locked file cabinet. You can put a bunch of unrelated files in the vault, take files out, rename them, and destroy them if you know the key. You can use folders inside the vault to organize your files. If you don't have the key you can't get in the vault. Even the names and lengths of files in the vault are protected with the same amount of encryption as the file contents [no more need to use cryptic names for encrypted files!] Unregistered users are restricted to only 5 files in a vault; registered users have room for as many as 800 files in the vault.

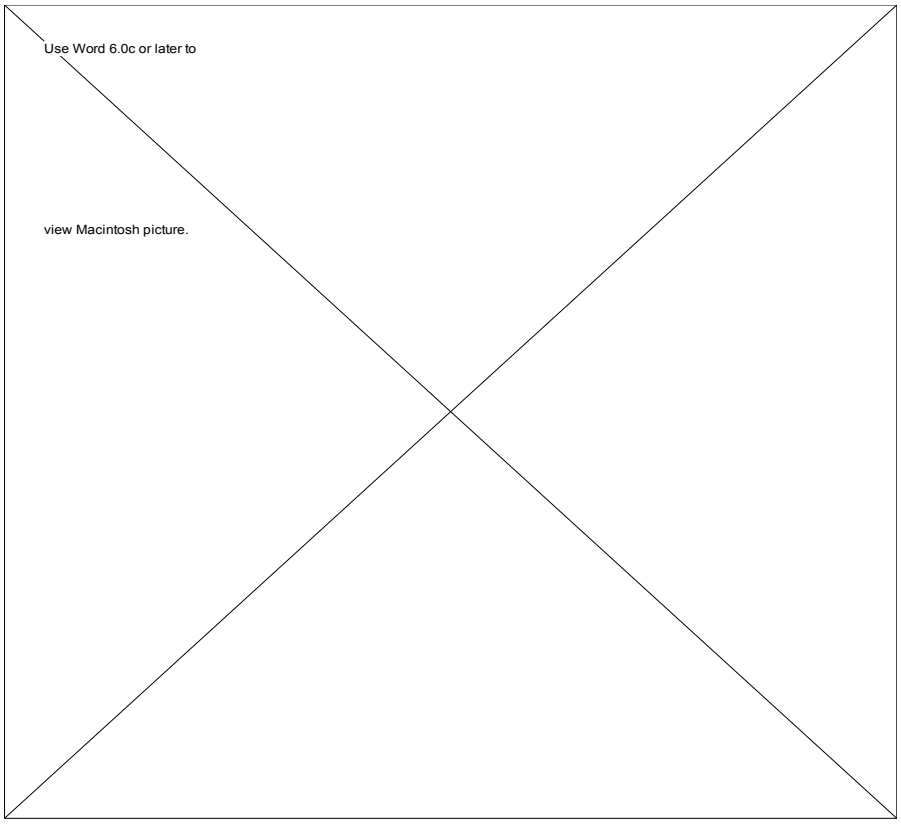

Figure 3: An Open Vault

Opening or Creating a Vault

To open a vault, select the "Open Vault..." command from Enigma's file menu. You will be asked for a key. If the correct key is entered, the vault will be opened. Figure 3 shows an example of an open vault.

To create a new vault select "New Vault..." under the File Menu. After entering a key, an empty vault will be displayed on the screen. It looks identical to figure 3 except that there will be no files or folders in it.

Vaults are completely protected by encryption. No clear-text data about the vault or its contents exists. For those with slower machines note that the larger the maximum capacity of the vault the longer it will take to open.

Vault Operations

Once opened, Enigma will bring up a window with a list of files and folders at the top level of the vault hierarchy. At the bottom of this window are six buttons: "Add", "Extract", "Rename", "Delete", "Info" and "Folder". The commands "Extract", "Rename", "Delete", and "Info" are unavailable unless there is at least one file selected.

Select a single file by clicking on its name in the list. You may select disjoint groups of files by command-clicking. A selection may be extended after an initial selection by shift-clicking.

Add

Clicking on the Add button (or selecting "Add..." from the vault menu) allows you to add files to the vault. It will bring up a dialog box which allows you add multiple files and folders to the vault. You can also drag files and folders from the Finder to the vault window to add them.

Delete

Clicking on the Delete button (or selecting "Delete" from the vault menu) will delete all selected files from the open vault. You may be asked to confirm this operation depending on the settings of the vault delete options [See Customizing Enigma].

Extract

Clicking on the Extract button (or selecting "Extract..." from the vault menu) will extract the selected files from the vault. Depending on the options you have selected you may be requested for a file name. If you have a folder highlighted when this option is selected all files and folders within that folder are extracted. You can also drag the selected items out of the vault window to the Finder for extraction. This drag always performs a copy out of the vault, the files are not removed from the vault.

Folder

Clicking on the Folder button (or selecting "Folder..." from the vault menu) allows you to create a folder in the current vault directory. You will be prompted to name the folder. The folder will appear in the vault list after it is created.

Navigating through the folders in a vault works just like it does in the Standard Get File routines. Double click on a folder to open it. To move up the hierarchy, use the pop up menu centered above the list of files in the vault. The root directory always has the same name as the name of the open vault.

Info

Clicking on the Info button (or selecting "Info..." from the vault menu) allows you to get information about a file or folder. The information displayed is nearly identical to that which you get from the Finder's Get Info function. It shows size, true file name, encryption date, creation date, and a comment which you can edit. For folders the number and size of files in the folder is shown. Any comments you enter in the Info window will be saved and protected by encryption. When you close the vault or quit Enigma all open info windows are closed as well. Note: the Info button will provide only very

limited information (and no comment capability) if the vault was originally created by a version of Enigma prior to version 2.3.

Rename

Clicking on the Rename button (or selecting "Rename..." from the vault menu) allows you to rename files and folders in the vault. For each selected file or folder you will be prompted for a new name which replaces the old name. If you use ":" as a character in the file name you will not be able to extract the file until you rename it again to a name that does not contain a ":".

Drag and Drop

You can also use drag and drop to add files to vaults. You can drag files from the Finder into a vault window to add those files to the vault. You can extract files from a vault by dragging from the vault to a finder winow, and you can copy files from one vault to another by dragging files between vault windows.

Compacting Vaults

There is an option in the File Menu entitled "Compact Vault..." the reason it is there needs to be explained. Files are added to a vault in what is known as "first fit" order. Old files deleted from a vault leave gaps. If a new file is less than or equal in size to a previously deleted file, the new file will re-use the space. If there is not space within the vault, the vault is made larger and the file added at the end. This means that vaults are not necessarily as small as possible. Select the compact vault function when you wish to eliminate all this wasted space. The process will take a couple of minutes and is completely safe. If something goes wrong before the compaction is finished (even something as drastic as a power failure) your original vault will be unharmed. You will need free disk space on the volume with the vault at least equal to the size of the vault being compacted.

One reason I'm discussing how files are allocated in a vault is because it affects the maximum number of vault files you can have. Although nominally there is room for five files in the freeware version of Enigma the following effect should be noted. Lets say you add 5 files (the maximum vault capacity), each 25K. And then delete the middle file, leaving room for a 25K file in the middle of the vault. If you try to add a file larger than 25K to the vault you will get an error message saying the vault is full. A file smaller than 25K will be successfully added. In this case you should compact the vault as described in the previous paragraph. In practice this should be at most a minor annoyance because I've found that files are not deleted from a vault very often.

The number on the right side of the vault status line shows the percentage of unused space. This is space that will be reclaimed by compacting the vault.

Self Extracting Vaults

Self extracting vaults allow you to send encrypted files to friends and associates without requiring that they have the Enigma application (or any encryption program). They can double click on the self extracting vault icon, enter a key, and then get a vault window similar to the regular Enigma vault window. Enigma can open self extracting vaults to add, rename, and delete files as normal. Receivers of self-extracting vaults can only extract files, not add or rename. Self extracting vaults are protected with the same level of protection as the version of Enigma which created the vault.

To create a self extracting vault select the "Create Self Extracting Vault..." from the file menu. It will prompt you for a filename and password. Once those are entered a normal looking vault window appears. Add, delete, or rename files as you normally would. After you close the vault you will see the self-extracting vault's icon on your desktop.

If you are a registered user the self-extracting vaults you create will be protected by full DES. You are free to send self-extracting vaults to anyone, including those with the limited DES version and those who have never heard of Enigma. But there is one thing you should be aware of. Although a receiver of a self-extracting vault can not use it for encryption it contains the DES algorithm and as such it might be a violation of US export law to send one to non-US/Canadian citizens. I'm not sure, if it's an issue for you then consult a lawyer.

Self extracting vaults do not have all of the capabilities of Enigma 2.8 vaults. You will not be able to create folders in self extracting vaults. Nor can you add comments. Self extracting vaults are limited to a capacity of 5 files in the freeware version and 200 files in the registered version. Drag and drop is not supported in self-extracting vaults.

Clipboard Encryption

Enigma allows you to edit, encrypt and decrypt the contents of the clipboard. The encrypted contents is saved as 7 bit ASCII text suitable for pasting into any electronic mail document.

Clipboard encryption functions are accessed from the Edit Menu. The menu commands and their meaning are:

Encrypt Clipboard

Selecting this command will encrypt the current contents of the clipboard. If necessary you will be asked to enter a key. The contents will be encrypted and saved as 7 bit ASCII text. If you are using a registered version of Enigma with full DES encryption you might want to consider selecting the “Use Limited DES” checkbox if the receiver of the message does not have a registered copy of Enigma.

Once encrypted the clipboard may be pasted into any Macintosh document.

The encrypted text is limited to a total of 32K. Because encrypted text takes up more space than the original clear text it is possible that the contents would exceed the 32K limit after encryption. If this situation applies Enigma will notify you. In this case consider splitting your message into two parts or using a self-extracting vault to send your message. The self-extracting vault will have to be binhexed before it can be emailed.

Decrypt Clipboard

Enigma will attempt to decrypt the contents of the clipboard using the key provided by the user. Extraneous text on the clipboard (such as a short clear-text note at the beginning of the message) will not affect Enigma's ability to decrypt the contents. You must make sure that the header lines Enigma places at the beginning of the encrypted block are untouched. If Enigma can not find any encrypted text you will be notified. In that case the most likely problem is that the header has been corrupted somehow.

The clipboard contents will be replaced by the decrypted text. Note that the entire contents are replaced so that any information besides the encrypted block will no longer be on the clipboard.

Edit Clipboard

Selecting this command allows you to view and edit the current clipboard contents. When you switch back to Enigma from another application the clipboard contents will automatically be updated.

As mentioned above you can not create or edit a clipboard using Enigma that exceeds 32K. Attempting to paste or type more information into the clipboard will result in a polite error message from Enigma.

Customizing Enigma

The preferences menu for Enigma contains three items: "Key Management...", "File Handling...", and "Vault Options...".

As you read through this section of the manual you might want to notice that the checked options are what I recommend as the settings for the most convenient usage of Enigma. When first installed NO options are selected.

Key Management

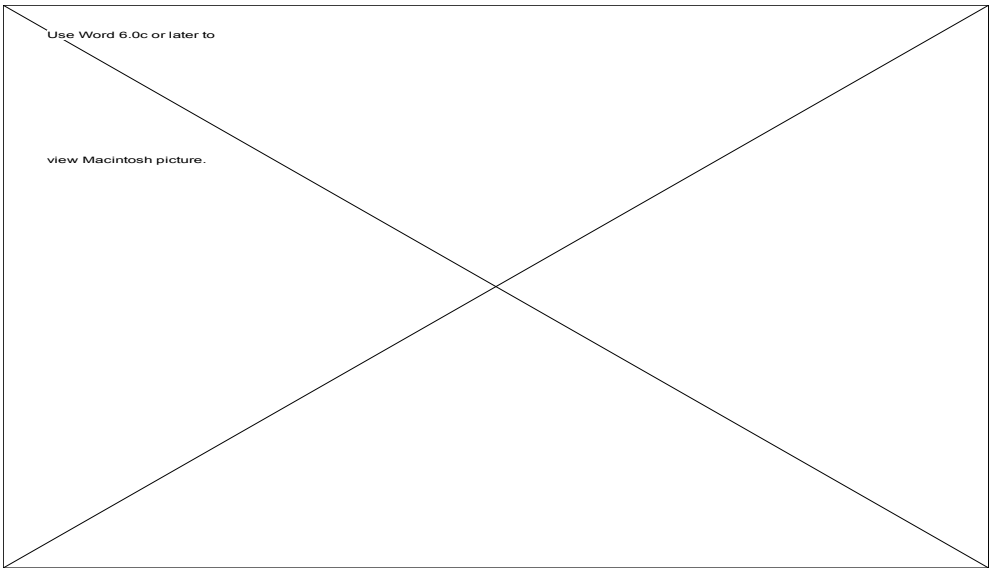

Figure 4: Key Management Options Dialog Box

Selecting "Key Management..." from the Options menu brings up the dialog box shown in figure 4. Each option is described in detail below

Remember Key During Session

Selecting the *Remember Key* option will use the first key entered by the user for the entire session. The key will be erased from memory just before the application exits. If you wish to enter a new key during a session select "Clear Key" from the Options menu. If you accidentally open a file with a different key from the "remembered" one, you will get an error message saying the key entered was invalid. If this happens the key is automatically cleared so you will be asked for a key again the next time you try to open a file or vault, even if the *Remember Key* option is on.

This option when combined with the *Use default file names for output* option [under File Handling options] will make it much easier to process large numbers of files at once. With both these options selected Enigma can operate unattended after a key is entered for the first file.

Hide Key While Entering

If this option is selected your key will be displayed with question marks in place of the characters you type. You will be asked to confirm your key entry to be sure you didn't make a mistake. You won't be able to use edit functions such as cut, paste, or the arrow keys. Only the delete/backspace key can be used to backup and change characters you know you mistyped. The confirmation process will assure that you don't enter an unintended key. Confirmation isn't done for decryption operations because the consequences of a mistyped key are much less drastic.

Beep When Encryption/Decryption Complete

This option, if selected, will cause the computer to either beep or play a sound when encryption is complete. If the system file contains a sound called Enigma Sound (name must be exact) that sound will play when an encryption or decryption operation is complete; otherwise a normal system beep will be played. If this option is not selected Enigma will not make any sound when an encryption or decryption is complete.

Clear Key/Close Vault After X Minutes Idle

If this option is selected you will be protected from accidentally leaving Enigma running unattended, possibly allowing someone else access to your files. If Enigma detects no activity for the specified period of time it will clear the key from memory and close any open vault. Any open info windows are closed as well.

File Handling

Options available under this menu selection allow you to control how Enigma deals with files. It allows you specify what sorts of confirmation messages you want, and if you want to make files invisible or saved as binhex.

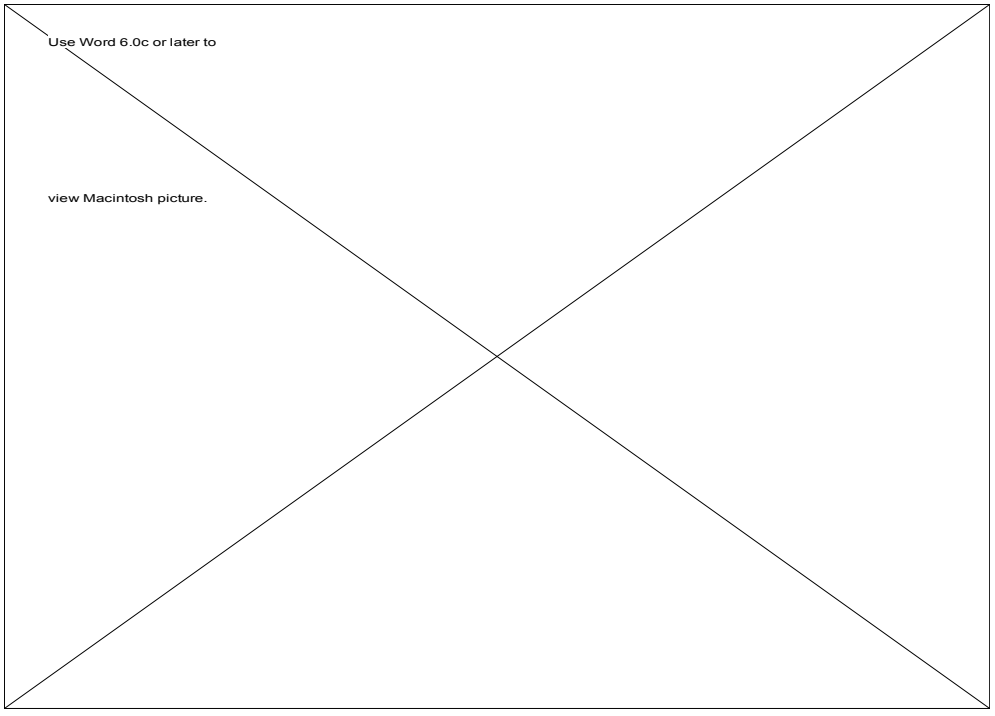

Figure 5: File Handling Options Dialog Box

Use Default File Names for Output

Selecting the *Use Default Names* option keeps Enigma from prompting you for an output name. If a file is being encrypted the output name will be the

original name plus ".???". If a decryption is being done the output name will be the name of the document or application when it was being encrypted. (Enigma stores this information when the file is encrypted. The name is encrypted as well so it is as secure as the rest of the file.) Note: During decryption: if *Use Default Names* is selected any other file with the same name in the current folder will be deleted without confirmation unless the appropriate *Confirm Overwrite* option has been selected.

Destroy Plain Text File After Encryption

This option does exactly what it says it does. After a successful encryption the original plain text file is destroyed by overwriting the data with zeros. This option does NOT delete an encrypted file after a successful decryption. Be careful with this option, once encrypted the original is irretrievably gone except through decryption.

Confirm Overwrite of Plain Text

Selecting this option will require Enigma to ask before overwriting a plain text file during a decryption operation.

Confirm Overwrite of Cypher Text

Selecting this option will require Enigma to ask before overwriting an encrypted file during an encryption operation. Note this option does not apply to vaults but a similar option is available for them [see Vault Options below].

Make Encrypted Files Invisible

If this option is selected vaults and encrypted files will be made invisible when they are created. They will continue to show up in Enigma's file selection dialog boxes so that you can access them. This provides only a very crude level of security as there are many applications which can make these files visible again. If you need a utility to make files visible again, I recommend the shareware utility *File Buddy* or *Resedit*.. Although some applications filter invisible files from the standard file dialog box others display them so it is best not to save invisible files in a commonly accessed folder or on the desktop.

Save Encrypted Files as Binhex

Binhex is a coding standard designed to send Macintosh files over simple text networks such as the Internet. Selecting this option saves encrypted files in a form suitable for emailing or uploading to a computer network that is not Mac literate. When the file is unbinhexed the user will be left with the encrypted document. Enigma must be used by the receiver to get to the contents. When this option is selected Enigma actually creates two copies of the encrypted file on your disk. The normal encrypted file and a separate binhexed file with the same name plus a .hqx file extension.

There are currently a couple of limitations regarding binhexed files. You can not directly decrypt a binhexed file. You must first unbinhex it using one of the many utilities available to do this (such as Stuffit Expander™). Secondly vaults can not be saved as binhex. Obviously it makes sense to have these features (particularly for self-extracting vaults) and I plan on adding them sometime in the future.

Vault Options

The third options dialog available from the options menu is entitled "Vault Options...". This dialog box lets you specify the maximum size of vaults and set various confirmations for potentially dangerous delete and replace operations.

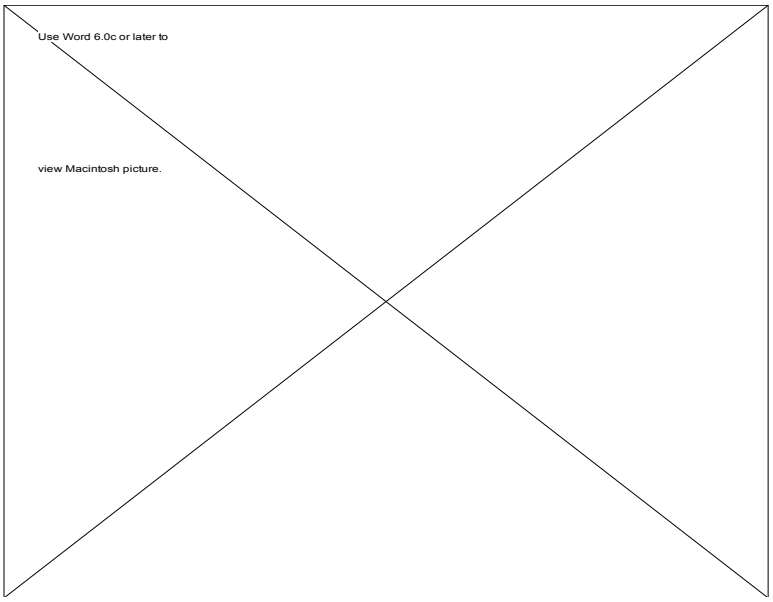

Figure 6: Vault Options

Verify File Deletes

Selecting this option will allow you to confirm deleting a file from a vault. If more than one file is selected for deletion you can press the Delete All button in the confirmation dialog box to simultaneously confirm the deletion of all selected files.

Verify Folder Deletes

Selecting this option will allow you to confirm deleting a folder from a vault. If more than one folder is selected for deletion you can press the Delete All button in the confirmation dialog box to simultaneously confirm the deletion of all selected files.

If you have selected a mixture of files and folders for deletion the Delete All button will delete all files and folders without further confirmation.

Replace Existing Files Without Asking When Adding to Vault

If this option is selected Enigma will replace files already in a vault with files being added. This option is very convenient if you often extract a file, edit it in some way and then add it back in.

If a folder being added has the same name as a folder already in the vault the files being added are simply added to the existing folder.

Vaults Have Room For X Items

Users of the freeware version of Enigma will not be able to change this setting from its default vault of 5.

This option allows you to control the maximum number of files and folders in newly created vaults. Once created there is no way to change the maximum number of files and folders a vault can contain. You must specify a number between 10 and 800.

There are two reasons to choose a number smaller than 800. First the larger the maximum number of files the larger the initial size of the vault. This effect is not dramatic though as even an 800 file vault uses only 86K when empty.

The second reason to choose fewer than 800 files in a vault is that slower machines will take noticeably longer to open large vaults. There is also a slight slow down in redrawing the vault contents and changing directories with larger vaults.

Simply experiment till you find the right size for your needs. By default Enigma creates vaults with room for 500 files which has acceptable performance on slower machines and provides plenty of room for lots of files.

Saving your Configuration

If you click on the "Save" button in any preferences dialog the options will be saved in a preferences file in the system folder. You can also select the cancel button if you are not satisfied with your changes to the option selections.

Resedit Hacks

The default vault name of "vault" and the default extension of ".???" can be changed using Resedit or a similar resource editor application. Using Resedit is not for people who are timid about computers; but these changes are pretty safe compared to some of the hacks I have.

First of all, make a back up copy of enigma.

Use Resedit to open the enigma application.

Double-click on the 'str#' resource

Edit string #2 to change the default vault name

Edit string #3 to change the default file extension [**must** be less than 10 characters and can not be empty]

Close the file and quit Resedit.

Run Enigma to verify your changes work correctly (try creating a new vault and new encrypted file)

If during any part of this procedure you are concerned you did something wrong simply quit Resedit. If you think you did something really wrong then restore the backup you made [you did make a backup didn't you?].

What is DES?

History

The Data Encryption Standard (DES) was developed in the 1970s by the National Bureau of Standards with the help of the National Security Agency. Its purpose is to provide a standard method for protecting sensitive commercial and unclassified data. IBM created the first draft of the algorithm, calling it LUCIFER. DES officially became a federal standard in November of 1976.

Algorithm

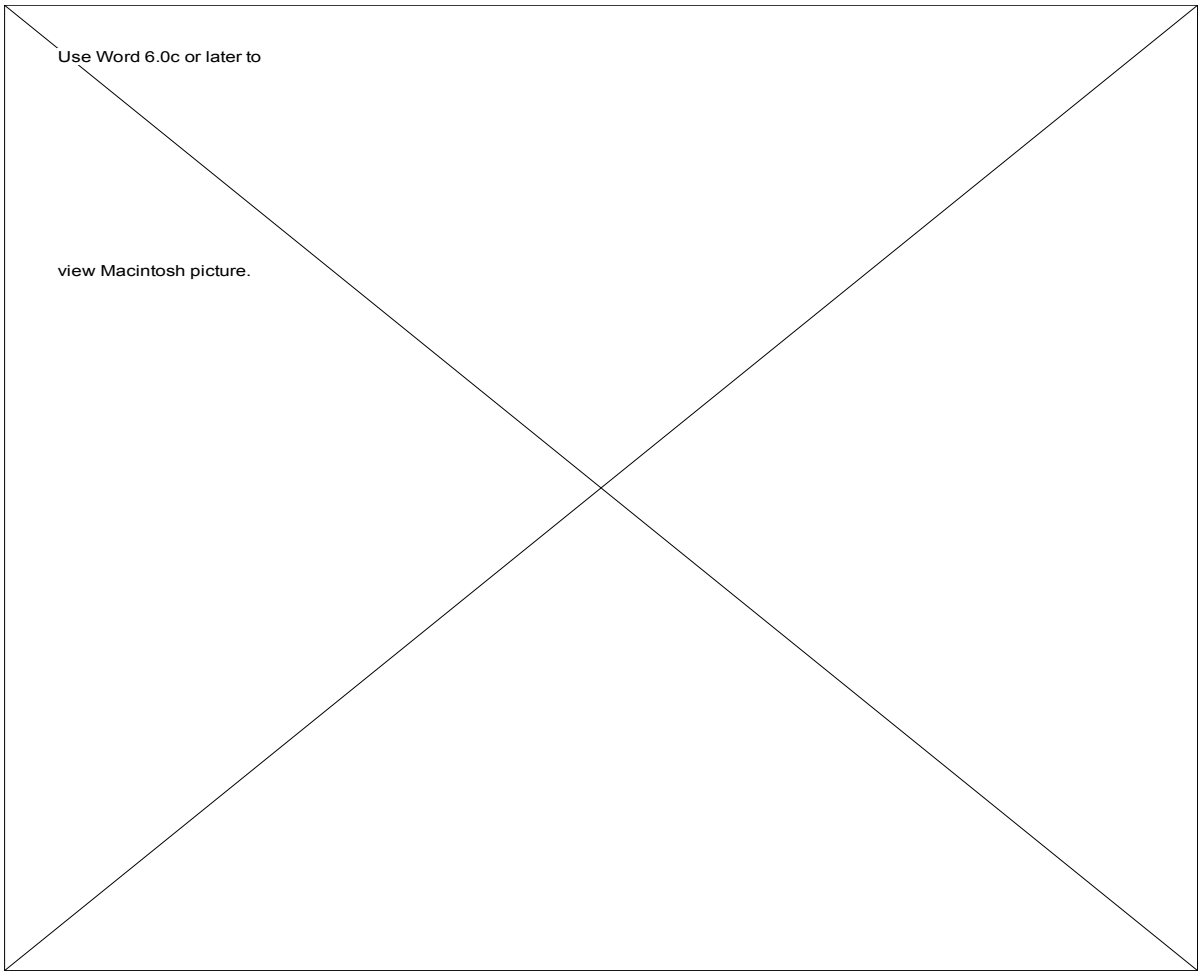

Figure 5: DES Block Diagram

Fundamentally DES performs only two operations on its input, bit shifting, and bit substitution. The key controls exactly how this process works. By doing these operations repeatedly and in a non-linear manner you end up with a result which can not be used to retrieve the original without the key. Those familiar with chaos theory should see a great deal of similarity to what DES does. By applying relatively simple operations repeatedly a system can achieve a state of near total randomness.

DES works on 64 bits of data at a time. Each 64 bits of data is iterated on from 1 to 16 times (16 is the DES standard). For each iteration a 48 bit subset of the 56 bit key is fed into the encryption block represented by the dashed rectangle above. Decryption is the inverse of the encryption process.

The "F" module shown in the diagram is the heart of DES. It actually consists of several different transforms and non-linear substitutions. Consult one of the references in the bibliography for details.

What is the Limited DES that Enigma Implements?

The limited DES mode available in the freeware version of Enigma modifies the DES standard in two ways. First of all, a 32 bit key is used instead of 56 bits [note: 32 bits, NOT 28 bits]. Secondly the data is iterated on only 4 times instead of 16. These changes reduce the computational complexity of the algorithm by at least 2^26 times. Nevertheless a naive user would still have to guess on average 2 billion times before the correct key was determined. However, by using only 4 iterations over the F module there are known attacks better than brute force which could be used for a more sophisticated attack.

What is Cipher Block Chaining?

The full DES version of Enigma takes the basic DES algorithm one step further by adding what is known as cipher block chaining. Without modification the standard DES algorithm encrypts data in 64 bit blocks independent of their context. Cipher block chaining increases security by exclusive ORing the previous 64 bit block with the current 64 bit block. This makes the encrypted value of a block context dependent, making it much more difficult to decipher. [Note this capability is only implemented in full DES versions of Enigma starting with version 2.3.]

How Secure is DES?

Users of Enigma will most likely be subject to ciphertext only attacks. That is an attack in which the cryptographer has access only to encrypted documents. Under such conditions there is no known method of attack better than randomly guessing keys. This discussion assumes you meet this condition.

The limited DES version of Enigma has 2^32 or 4,294,967,296 possible keys. The full DES version of Enigma has 2^56 or 72,057,594,037,900,000 possible keys. To determine the time it will take to break a file protected by Enigma multiply the number of keys by the time it takes your computer to try one key (times one half because on average you will guess the key by the time you have tried half the keys).

For comparison I have done some rough (but conservative) calculations. Using brute force a Mac 7300/200 can break into a file protected by the free version of Enigma in about 1 hour of non-stop computing. It would take that same Mac almost a 100,000 years to break into the same file protected by the full DES version. Equivalent numbers for a single Cray super computer (estimate somewhat rougher) would be about 10 minutes versus 3,000 years.

What about back doors?

Because the NSA was involved in the development of DES there has been a constant concern there is a back door. Here DES's greatest weakness that it was developed almost 20 years ago is a strength. In those 20 years no one has ever described a way to break DES except by brute force (ciphertext ONLY

attacks). Concerns about DES's weakness are centered solely on how fast it will take a computer to try those 72 quintillion possible combinations. Massively parallel computers are a significant threat because each processor can be assigned a small piece of the total problem. Nevertheless even the most optimistic estimates place the cost of a theoretical DES breaking machine into the several millions of dollars range. This is not to say that no one can read a message protected by DES. If the NSA decides they need to read your document, they will.

It is easy to be paranoid when it comes to encryption, but keep this in mind. It is in the US Governments interest to provide a good encryption standard. If the NSA could read industrial and technology secrets protected by DES than so could the KGB. It is my opinion that DES was designed to balance the competing interests of a government reading its citizens secrets and being sure that no other government could read them. I believe that this resulted in an algorithm of very high security, but one that can be broken through brute force by a truly massive assault. The inevitable march of technology has slowly eroded the amount of technological know-how needed to break DES but the hurdle remains high for the next decade or two.

Protecting Your Privacy

A few simple precautions need to be taken to assure the absolute secrecy of your data. First of all, NEVER run enigma with virtual memory on, an image of the clear-text or key could be left on your hard disk. See the memory control panel for this switch. This caution applies to the new “enhanced” virtual memory tools such as OptiMem and RamDoubler as well. If you can’t live without these utilities just be sure to always run Enigma when you have plenty of free (real) RAM.

Secondly, remember that deleting a file (such as the plain-text version of a just encrypted file) does not remove the data from the disk. Use an application which overwrites deleted files with null data. I have written an application that does this. It is called Burn and should be available from the same place that you got Enigma from. Further, Enigma allows you to specify that it destroy a plain-text file after encryption (See the section on Customizing Enigma.)

The introductory discussion on how secure Enigma is assumes that your key can not be guessed. I can not over-emphasize the importance of this, your data is not secure if your password can be guessed or contains only common words. Keys should be more than a few characters long (13 for maximum security). Do not choose obvious things like people, place or pet names, nor should every word of your key be in a standard dictionary. The more unconnected a key is from you and your life the harder it will be to guess.

Enigma has a somewhat unusual keying system that increases the security of files you protect using it. All characters typed as a key are converted to a 5 bit representation. You should always use the 26 letters of the alphabet (upper or

lower case doesn't matter), the 10 digits 0-9, and the space bar for your key. Any other characters are mapped into this space by using the 5 least significant bits of their ASCII value. The packing algorithm used ensures maximum data security even though a restricted character set is used. The benefit is an easy to remember password that provides maximum security.

You might be a little unsure how restricting the possible characters in a key can actually enhance security. This scheme works because even in the best case you can't realistically choose from more than about 75 characters for each character of your key. If no packing were done someone searching for a key would only need to examine those 75 characters for each 8 bits (256 characters) of the key. By using only five bits per character there are no "gaps" that can be ignored by someone searching for your key. For maximum security a key should be 13 characters. Characters beyond 13 are ignored.

Another important point regarding nearly all encryption algorithms is that they are much easier to break if the cryptanalyst has access to the plaintext and ciphertext version of any document encrypted with the key he is trying to break. The lesson here is to be sure that plaintext versions of encrypted files should not be left laying around even if the particular file is not of high value; it can be used to make breaking your key easier.

Finally, because the encryption engine source code is available you can be absolutely certain that the full DES algorithm is implemented and that there are no back doors or vulnerabilities. No other DES type encryption package for the Macintosh exists which provides this certainty. Note: starting with version 2.0 complete source code is not available to protect my investment. Source for the complete Enigma 1.2 application remains available. Because of the new CBC encryption mode, Enigma 1.2 no longer produces encrypted results identical to Enigma 2.5. However, I will include with the source code an example of how to modify the DES algorithm to implement CBC mode (it is only a few lines of code).

Frequently Asked Questions

Enigma for Windows is available. The current version is 1.0 which provides only file encryption. Enigma for Windows provides an effective cross-platform encryption solution for environments running both Mac and Windows.

Can you send source code for the limited DES version outside the United States and Canada?

I wrestled with this one for awhile. But the answer is no. The source code is just too similar to the full algorithm. Sure you could disassemble the object code, and with that, a real talent for assembly language, and an intimate knowledge of DES you could probably patch together a full DES version. But a person like that could write Enigma from scratch over a couple weekends and doesn't need the source code.

Is it legal to send encrypted messages over international networks?

Yes, absolutely. Nothing in US law says you can't use encryption to communicate. Its just that you can't export the algorithm in the form of a program (or any other way). Encrypted messages are just data. How someone else reads the message is their problem. If you want to do a lot of private email communication I recommend using PGP instead, its more suitable for that kind of thing than Enigma is. Enigma is more suited, by the nature of its interface, to protecting files on a hard disk although the new clipboard encryption and binhex options enhance Enigma's email usefulness.

I live outside the US and Canada but would like to be able to have large vaults, what can I do?

I can not intentionally export any version of Enigma outside of the United States. Hopefully US law in this area will change in the near future.

I forgot my key, can you recover my files?

Absolutely NO. There is no Enigma cracking program, no backdoor, no key stashed away somewhere. If you forget your key there is no hope. If I could get to your file Enigma would be worthless. This fact, by the way, is an excellent reason to avoid some of the commercial encryption programs which deliberately place back doors or use a master key type system to allow system administrators and tech support types to get to files.

Things that look like bugs but aren't really

Some virus checking and disk checking programs will report that encrypted files contain a corrupted resource fork. This is because the resource fork is encrypted by Enigma, rendering it unreadable even by the Apple system software. This isn't a bug, encrypted applications aren't supposed to be readable. Do NOT attempt to "repair" an encrypted file. Vaults do not have this problem, only encrypted files. This situation does occasionally create problems for programs which try to read the resource fork for any reason. For instance I wouldn’t recommend trying to opening an encrypted file [containing a resource fork] using Resedit.

The *Remember Key* option can be tricky sometimes if you have files with different keys. Remember that with this option is selected, once a key has been entered it will be used for the ENTIRE session. If you later open a file or vault encrypted with a different key then you will get a message saying an invalid key was entered. To change keys, click on the "Clear Key" command under the options menu and open the file again. This is also a problem if you work with a mixture of limited and full DES files. Even if you type in the same key for both limited and full DES, they are actually different as far as Enigma is concerned.

You will notice a pause while launching a self-extracting vault application. This pause (of up to 30 seconds on slower CPUs) is due to Enigma calculating

some internal tables which substantially speed up decryption during extraction. In order to keep the size of the self-extracting vaults as small as possible these tables are not stored on disk (as they are in the main Enigma application) so they must be recalculated each time the application is launched. These tables (stored on disk or not) are independent of your key and in no way affect the security of the algorithm, only its speed.

Enigma can temporarily require large amounts of disk space. There must be free disk space available equal to the size of the file being operated on for the operation to be successful. Vault compaction temporarily requires an amount of disk space equal to the size of the vault being compacted. If you are low on disk space Enigma will warn you, there is no risk of losing data.

Because of the way the limited DES version reduces the key size to 32 bits the last couple of characters of your key might not be significant. You should always choose a long key when you use the limited DES version.

Enigma can temporarily require very large amounts of RAM when it is processing folders with either many files or many levels of nesting. If you encounter a problem trying to either add or extract a very large folder try increasing Enigma's memory partition (Usually you will get an error -108). The default memory partition of approximately one megabyte is adequate for all but extreme situations.

Compatibility with Earlier Versions of Enigma

There are some compatibility issues with different versions of Enigma that you should be aware of:

- Vaults larger than 200 files can not be opened by versions of Enigma prior to 2.5.
- The limited DES version of Enigma is not capable of opening any files or vaults created by any version of the full DES Enigma application.
- The full DES version can not open vaults created by the limited DES version of Enigma although it can open files.
- Vaults created by versions of Enigma prior to 2.3 do not have a Folder capability, and only a limited "Info" capability.
- Self Extracting vaults created by a version of Enigma prior to Enigma 2.3 can not be opened by later versions (They are still fully functional applications, you just can't modify them).
- Dates on files extracted by Enigma are not correct if the file or vault was originally created with a version earlier than 2.3.

You can't hurt anything if you have an incompatibility. The worst that will happen is you will get an appropriate error message.

Things that need improvement

If you enter an incorrect key while trying to decrypt an individual file (not a vault) the program will usually tell you by reporting an error that says "Invalid Key Entered". However, occasionally the decryption process will generate a valid (though meaningless) filename which Enigma will blindly use. This causes no harm except the output will be total garbage (which should be deleted by the user). Just repeat the process with the correct key and your file will be decrypted properly. This happens because Enigma uses the validity of the filename generated for the output file to determine if you entered an incorrect key. Vaults use a different mechanism and don't have this problem.

User Support

As registered users know full support for Enigma is provided. Don't hesitate to send mail with questions, bug reports or suggestions (even if you're not registered). I want this program to be the best there is, and I want you to be a satisfied user.

How to get the full DES version of this program

First of all let me repeat that the limited DES version is free, it is not shareware, you don't need to feel guilty about not registering. But if you want or need the maximum protection full DES provides or need larger vaults they are available for $20 US for non-commercial users [see site license fee below if you are purchasing Enigma for more than one Mac]. The source code to Enigma 1.2 (not 2.5) including the complete DES algorithm is available for an additional $10. In either case I can only ship to a US or Canadian address. When requesting the full version you must include a statement that you agree not to upload the program on any network and that you will not export the program outside of the United States or Canada. A registration form is included with the standard Enigma distribution.

If you would like the source code you must agree that you will not use the name "Enigma" in any program using my source code. You may use Enigma source code royalty free. Source to version 1.2 is written in Think C version 5.0.3. The encryption engine is machine independent and isolated from the rest of Enigma.

If you include an Internet address I will send the full release via email the day I receive your request. To take advantage of this you will need to be able to download text from the Internet to your Macintosh, and have the binhex and Stuffit applications available [both are free and available from any on-line service]. I can only do this for Internet and Delphi users, most commercial on-line services such as AOL and CompuServe do not easily allow for large email files even though they are nominally on the Internet. If you know you can not take advantage of receiving the program via email please let me know

so I won't waste both our times trying (but still include your email address for upgrade and support).

Be sure when ordering you specify that you want the Macintosh version of Enigma. Even if you can't be bothered to fill out the registration form. If you don't specify which machine you want your order could be delayed.

Site License Fee

If you are purchasing Enigma for a business please include a site license fee of $20 per CPU for the first ten CPUs, and $15 per CPU after that up to a maximum of $500 for a site license that covers all people within a 100 mile radius. Purchase of the site license gives you full upgrade privileges as a private user ($2 total cost), as well as allowing unlimited growth of your network (i.e. no additional costs for new CPUs). I will provide my normal (high) level of support via email. Please count all machines connected to a file server with Enigma installed as CPUs when calculating the cost.

Updates

Registered users of any previous version of Enigma may receive an upgrade to Enigma 2.8 with full DES capabilities by sending a disk and a SASE (or $5 and no disk) to the regular address and specify that you would like the upgrade. I will attempt to notify registered users of upgrades via email. For those users without an email account I will send a postcard roughly every other version or so if you upgraded last time I contacted you. If possible, include your email address with your update request. It will facilitate notification of new upgrades and my ability to provide support.

Acknowledgments

Many people have contributed to the success of Enigma. First of all, let me thank everyone who has ever sent me a message saying "Wouldn't it be great if Enigma did...". I keep track of every such comment and implement all those which are feasible and possible. For instance, I had never thought of self extracting vaults until a user suggested them.

Dr. William MacGregor wrote me a letter shortly after Enigma 1.1 was released and said, basically, here's how to make DES super fast. The result was that Enigma 1.2 was twelve times faster than Enigma 1.1.

Gabriel Schuyler and JayKW helped out a lot with the icon designs.

And special thanks to my beta testers. Encryption is tricky stuff so Enigma must be completely reliable. Over the last year I have asked several people who have demonstrated a great ability to search out the deepest corners of Enigma to help me test each release. They are: Brian Clark, Jerry Goldstein, Harry Mueller, Gabriel Schuyler, and Neil Van Ess. Each one a person you want on your side if you have a significant software application to develop. And if you don't do a good job I promise they will let you know! :)

Standard Disclaimer

Neither Next Wave Software, Inc. nor Michael Watson are responsible for any loss or damage due to any failure of this program regardless of the cause.

Enigma is a product of Next Wave Software, Inc.

You are free to distribute the limited DES version of this program to other users provided this documentation is enclosed. The program can not be offered for sale without my permission. Enclosure as part of a user group shareware collection is allowed so long as the collection is sold only to recover distribution costs.

Any party desiring to include this program as part of a shareware collection that is sold on a for profit basis must receive written permission from the author.

Payments (make checks out to Next Wave Software, Inc.) and questions can be mailed to:

Next Wave Software, Inc.
3140 S. Peoria St. #247
Aurora CO 80014

I don't mind email. If you have questions (about Enigma), bug reports, or ideas feel free to email me at the following addresses (even if your not registered):

service@thenextwave.com <-- preferred

Next Wave Software is on the web, check out our site at
http://www.thenextwave.com/ for the latest information.

Appendix A: Change History

What's new in version 2.7?

- Fixed a crashing bug in drag-and-drop that occurs with Mac OS 8.
- Revised contact information for Next Wave Software, Inc.

What's new in version 2.6.2?

- Fixed a problem in 2.6.1 that made it difficult to select folders and multiple files in vaults.
- Added reveal-invisible menu command for finding those invisible vaults.
- Fixed a problem that prevented using Self-extracting vaults in version 2.6.
- Fixed drag-manager crash with old (version 7.1 or older) system software.
- Fixed minor window position problem with two monitors

Version 2.6.1 (never in widespread release)

- See whats new in version 2.6.2.

Version 2.6 (released 8/96)?

- True Drag and Drop between open vaults and the Finder.
- Web page support for all Next Wave Software products. Visit us at http://www.thenextwave.com/
- New mail address for Next Wave Software.

Version 2.5 (released 9/94)

- Folders can now be directly added to vaults.
- Folder hierarchies maintained both while adding folders to vaults and extracting folders from vaults.
- Registered users can create vaults containing up to 800 files, unregistered users continue to be able to create vaults with up to five files.
- Clipboard encryption in a manner suitable for use in email.
- Encrypted files can be saved as binhex.

- A new status line across the top of the vault window shows number of files in vault, total size of vault, and amount of space that can be saved by compacting.
- A new interface makes it much easier to add many files and folders at once to a vault.
- Files and folders can be added to an open vault by dragging to the Enigma Application.
- The user interface continues to improve: more use of color, more consistent interface, many little touches to make the whole application easier to use.

Version 2.4 (released 7/94)

- Enigma now runs in native mode on the Power Macintosh encrypting at speeds well above 100K/second.
- Changes have been made to make Enigma more compatible with Enigma for Windows 1.0 which was released simultaneously with version 2.4 for the Macintosh.
- Incorrect keys are now handled much more gracefully (again).
- A bug that occasionally resulted in items showing up in the trash as "rescued items" has been fixed.
- Fixed a crash when more than 255 files extracted from vaults in a single session.

Version 2.3 (released 4/94)

- Vaults are now hierarchical. Organize your vaults using folders. Folders can be extracted from a vault.
- Stronger encryption. Full DES versions of the program now use CBC mode for newly encrypted vaults and files. (See the section describing DES for what this means).
- Full DES vaults can now contain 200 files.
- A new dialog box makes it much easier to add multiple files at once to a vault.
- Vault windows are now fully resizeable. Size and position of a vault is remembered for the next time the vault is opened.
- A Get Info function for files in a vault gives detailed information about the file and allows a comment to be entered. The comment is saved in encrypted form.

- If cancel is selected during an encryption or decryption operation, any file that was being overwritten is restored.
- Finder flags, creation date, last modified date and custom icons are now preserved during encryption and restored during decryption.
- A large number of user interface improvements such as a moveable encryption status dialog.
- The file erase application Burn has been improved: User selectable erase pattern, user selectable number of erase passes, and the ability to erase free space on a disk (in case you accidentally deleted a file that should have been burned).

Version 2.2 (released 01/94)

- You can now create Self-extracting vaults so you can send files to your friend protected by encryption, even if they don't have the enigma application.
- Vault windows can now be resized along the vertical axis.
- If an incorrect key is entered, the key is cleared so key must be reentered by the user.
- Added new command key equivalents to open and close vault menu functions.
- New menu available when vaults are open, allowing command key equivalents for vault functions such as add, extract, rename, and delete.
- Encryption done sound can be turned on or off from options dialog.
- Enigma will now play the sound called "Enigma Sound" if it exists.
- Files will now have the correct type immediately. Previously Enigma would sometimes create files which appeared to have the wrong type until the window was closed and opened or the system rebooted.
- You can no longer perform cut/copy/paste operations in hidden key entry dialogs (it never worked properly anyway)
- Fixed problem making it impossible to extract files from a vault which had been renamed to a length greater than 31 characters. Filenames in vaults are now firmly limited to 31 characters (same as the Macintosh Operating System).
- Stationary documents now handled properly (stationary encrypted not a copy).
- Fixed crash when "About..." selected with a vault open

Version 2.1 (released 10/93)

- The annoying crash caused when an incorrect password is entered has been fixed.
- Vaults can now be compacted which will save space when files are frequently added to and deleted from a vault.
- Within vaults, the sizes of individual files are displayed.
- You can now double click on a file in a vault to extract it.
- New options have been added to make it less likely you will accidentally overwrite a file you didn't want to.
- Upon completion of an encryption or decryption operation the program will beep.
- Better (and color) icons!
- The file being processed is now displayed in the status window.

Version 2.0 (released 7/93)

- Enigma now supports vaults. A vault is a collection of files encrypted together. Individual files within a vault may be extracted, renamed or deleted and new files can be added to the vault at any time.
- The annoying start up delay in Enigma 1.2 has been eliminated.
- There was a bug in Enigma 1.2 which resulted in files being a few bytes longer than they should have been. This has been fixed, decrypted files will now be exactly the same length as the original file.
- Enigma 2.0 now uses a preferences file stored in the system folder. This will make the program more compatible with network usage.
- The string ".???" which Enigma 1.2 appended to encrypted files can be edited by the user to a string of his or her choice.

Version 1.2 (released 3/93)

- Encryptions and decryptions are now 12 times faster!
- Plain-text files can optionally be destroyed (overwritten) after encryption.
- Running Enigma over an Apple Talk network is about 100 times faster.
- The key you type in can optionally be hidden.
- The program will now quit after completing a drag-and-drop event.

- The key is now cleared from memory as soon as possible to be sure that a memory dump will not expose your key.
- For those interested in upgrading, you can now choose between the limited and full DES encryption on a file by file basis.

Version 1.1 (released 10/92)

- Several bugs in the user interface have been squashed
- The program is now System 7 aware but remains compatible with any Mac.
- Improved support for encryption and decryption of multiple files.
- Encryption of applications and documents with resource forks is now supported.

Version 1.0 (released 9/92)

- Initial capability

Appendix B: Bibliography

The following references are outstanding sources of information on the DES algorithm and encryption in general.

Schneier, Bruce. *Applied Cryptography*. New York, NY: John Wiley & Sons, 1994. ISBN 0-471-59756-2.

Dewdney, A. K. "Computer Recreations: On Making and Breaking Codes." *Scientific American*, November 1988, pp. 142-145.