Enigma Version 2.2, released 1/94

About Enigma

Enigma, named after the famous German encryption system of world war II, implements a limited version of the NSA developed Data Encryption Standard (DES) which is the standard for commercial, unclassified, data protection. A version with full DES capability is available as well (see below for ordering information.) Theoretically DES is secure against any computer that can't do more than about a thousand billion encryptions a second. It is likely that the NSA (and probably no other agency on earth) has the raw computing power to break DES if they make an all out effort, but I would say that if you have attracted the attention of that particular organization this program will not help you. Short of that kind of computing power Enigma provides complete security when used properly. There have been no known compromises of DES since it was developed in 1977 [IEEE Spectrum Aug '92].

Restrictions

Because Enigma is distributed over an international network it can not implement the full DES standard since US law does not allow export of the complete algorithm. Stupid as it sounds, DES is considered a "munition" by the US government. Export of DES outside of the United States and Canada is a rather severe felony if the Justice Department should decide to prosecute. The program you have downloaded implements a limited version which is almost as secure, but does not violate US law. For those interested in the technical details: The key size is only 32 bits (instead of 64) and part of the f-module has been removed. The level of protection provided by the free version of enigma is more than adequate against casual attacks from co-workers or nosy neighbors. It is not adequate protection against highly motivated people with access to powerful computers. If you are concerned about serious attempts to access your data from skilled professionals you should order the full DES version.

Please write your congressmen and let them know you oppose the FBI's proposed Digital Telephony Bill which would make this program and all other encryption programs that do not provide a back door for the US Government illegal. Also 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 blatant back doors, and has survived the test of time.)

Enigma 2.2 Requirements

Enigma 2.2 requires System 7.0 or later.   Sorry people, it's time to upgrade. It requires about 512K of memory (remember when 64K was a lot of memory?), and about 200K of disk space. I know of no hardware or init conflicts if you meet the above requirements. For users with older machines or users who won't upgrade to system 7, you can get a copy of Enigma 1.2 from me by writing to the same address as those registering Enigma 2.2. Enigma 1.2 is compatible with all Macintosh's with at least 512K of RAM and the 128K ROM. Enigma 1.2 contains all the encryption capability of Enigma 2.2 but does not support vaults.

What's new in version 2.2

-	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

Change History

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 accidently 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 startup 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 AppleTalk 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

Maximum Security

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.

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. An application that does this is included with the Enigma software distribution (it is called Burn-It and is documented separately). Further, Enigma allows you to specify that it destroy a plain-text file after encryption (See the section on Options, below.)

The introductory discussion on how secure Enigma is assumes that your key can not be guessed. I can not over-emphasize the criticality 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 ignored. 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 at least 13 characters.

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 cyphertext 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 in

developing the vault code. Enigma 1.2 source code remains available and can be used to verify the integrity of the encryption because Enigma 1.2 and Enigma 2.2 will produce identical results when encrypting a file.

How Secure is the free version of Enigma?

For comparison I have done some rough (but conservative) calculations. Using <u>brute force</u> a Mac LC-II can break into a file protected by the free version of Enigma in about 1 day of non-stop computing. It would take that same Mac almost a million years to break into the same file protected by the full DES version. Equivalent numbers for a single Cray supercomputer (estimate somewhat rougher) would be about 10 minutes versus 3,000 years. Brute force is defined as trying one half of all possible combinations of 32 or 64 bit keys, and the assumption you could detect success in the first eight bytes of a file. If your curious as to the details of this calculation feel free to send me mail.

How to Encrypt or Decrypt an Individual File

To encrypt or decrypt a file simply drag the desired files to the Enigma icon and release the mouse button. You will be prompted for a key. From that point on if you have the *Remember Key* and *Use Default Names* options selected the files will be automatically encrypted and/or decrypted depending on their type. Enigma assumes files of type 'crp1' and 'crp2' (full DES) are encrypted and you are requesting their decryption. All other files are assumed to need encryption. If *Remember Key* is off this may be overridden on a file by file basis (this would be useful only if a file had been encrypted twice.) If the *Use Default Names* option is off you will be prompted to enter the name of the output file each time another file is processed.

Enigma will automatically erase any key in memory and exit after all files in a drag-and-drop operation have been processed. This will assure you don't accidently leave Enigma running with your key possibly exposed.

You may also run the program and select files for encryption and decryption using the "Open File..." command under the File menu. When used in this way, the program will stay resident until you select "Quit" from the File menu.

The Options Menu

The options menu of Enigma version 2.2 contains three options, the first entitled "General Options...". Selecting this menu item will bring up a dialog box containing the seven encryption options available. Selection of an option is indicated by a check in the box adjacent to the option. Each option is described in detail below.

The first two options: *Remember Key*, and *Use Default Names* 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.

Remember Key:
Selecting the *Remember Key* option will use the first key entered by the user for the entire session. The key will be "forgotten" as soon as the application exits. If you wish to enter a new key during a session select the *clear key* option under the options menu. If you accidently open a file with a different key from the "remembered" one, you will get an error message saying the key entered was invalid.

Use Default Names:

Selecting the *Use Default Names* keeps Enigma from prompting you for an output name. If a file is being encrypted the output name will be the input 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 Clear-text After Encryption:
This option does exactly what it says it does. After a <u>successful</u> encryption the original clear-text file is destroyed using the same algorithm used by Burn-It, the included file destroying utility. 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. Read through the cautions in the Burn-It documentation because they apply equally to selecting this option.

Hide Key While Entering:
If this option is selected your key will be displayed with ?'s 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.

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.

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 (name must be exact) "Enigma Sound" 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.

The second options dialog available from the options menu is entitled, "Vault Options...". Currently there is only a single option available entitled "Verify Vault Deletes...".

Verify Vault Deletes:
Selecting this option will allow you to confirm deleting a file from a vault.

The final menu selection from the Options menu allows you to manually clear the last key entered if the Remember Key option is selected. This allows a quick way to reset the key if you accidently typed in an incorrect key or switch to a different file which has a different key.

Once you are satisfied with your option selections select the save button. The options will be saved in a preferences file in the system folder. If no preferences file is present the options will all be reset to unchecked. You can also select the cancel button if you are not satisfied with your changes to the option selections.

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. If you don't have the key you can't get in the file cabinet. 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 100 files in the vault.

Several commands under the File Menu allow you to open and manipulate vaults. After selecting "Create Vault..." or "Open Vault..." you will be prompted for a file name and a key. The key you enter applies to the vault and all files in the vault. The program will then bring up a window with a list of files currently in the vault. At the bottom of this window are four buttons: "Add", "Extract", "Rename", and "Delete". Select files from the vault list and press the buttons to perform the actions you want (Aren't Macintosh's great?). You may shift-click on more then one file in a vault to apply an operation to multiple files. Adding or extracting a file does not require entering a key, the key you entered when opening the vault is used. Click the close box on the window or select "Close Vault..." from the File Menu when done. The vault will also be closed automatically if you quit the program.

You will notice a slight pause when opening or creating a vault. This is because the program must decrypt the vault's directory map each time it is opened. Let me emphasize that vaults are completely protected by encryption. No clear-text data about the vault or its contents exists.

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 the following effect should be noted (I'm not calling it a problem because I don't have to). 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.

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 normal Enigma documents.

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.

Sound

Enigma will optionally beep when encryuption or decryption operations are complete. Further, Enigma will examine the system file (not folder) for a sound with the name "Enigma Sound" (case is important). If this sound is found it will be played instead of the standard beep sound when encryption or decryption is complete.

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 seen published for other applications.

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]
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.

Frequently Asked Questions

I am often asked the following questions, so I'll save time and answer them now:

Is there a DOS/Window's version available? Not yet. I do not own a PC Compatible, and am not likely too unless lots more people register. However I'm working with a friend to try and get a port done. He's learning Windows at the same time, and also can't devote a lot of time to the project. In the meantime I can only say be patient, and consider buying a Macintosh.

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. The author

of that program has much bigger cojonés then I have. PGP is available (last I heard) from uunet. Enigma is more suited, by the nature of its interface, to protecting files on a hard disk.   The new self-extracting vault feature enhances Enigma's email usefulness. Keep in mind though to keep within the law you can not send a full DES self-extracting vault outside the US and Canada. The limited DES version is not a problem.

Things that look like bugs but aren't really

Some virus checking (and probably some disk checking) programs will report that Enigma 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.

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.

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 independant of your key and in no way affect the security of the algorithm, only its speed.

Things that need improvement
If you decide to cancel an encryption or decryption operation before it is finished, the destination file will be removed (even if there used to be a different file with the same name). Use the *confirm overwrites* options if this is a concern.

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, very rarely 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.

Vaults can only be opened by the same version of Enigma as that which created them. This means that a full DES version of enigma can not open a limited DES vault or vice-versa. If you attempt to do this you will get a "Password not recognized" message.

User Support

As my registered users know I provide full support for Enigma. 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 $15 US for non-commercial users [see site license fee below if you are purchasing Enigma for a business with more than three Macs]. The source code to Enigma 1.2 (not 2.2) 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.

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 is written in Think C version 6. 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 public domain and available from any on-line service]. I can only do this for internet users, commercial online services such as AOL 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).

Site License Fee

If you are purchasing Enigma for a business please include a site license fee of $5 per CPU (3 CPU minimum). For very large sites, I request a maximum site license fee of $500 (100 CPUs) no matter how many CPUs you really have. 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 2.2 with full DES capabilities by sending a disk and a SASE (or $2 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.

Standard Disclaimer

I am not responsible for any loss or damage due to any failure of this program regardless of the cause.

Enigma is © 1993 by Michael Watson.

Enigma is a product of Next Wave Software (not yet ™).

This program is not in the public domain. I reserve all rights to this program.

You are free to distribute 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 and questions can be mailed to:

Mike Watson
4830 Nightingale Drive #E302
Colorado Springs, CO 80918

I don't mind email. If you have questions, bug reports, or ideas feel free to email me at the following addresses (even if your not registered):
Internet: mdw@cns.cscns.com   <-- preferred
America OnLine : MikeW03
Compuserve: 72510,3427   <-- guaranteed slowest response