Enigma Version 2.0, released 7/4/93

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 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 because US law does not allow export of the complete algorithm. Stupid as it sounds, DES is considered a "munition" by the US government. Exportation 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.)

What's new in version 2.0

Version 2.0 is a substantial improvement over 1.2. The most important are:

- 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. Vaults allow you to keep your encrypted files better organized and also provide extra security because the individual file names and lengths of vault files are protected by encryption. Note: the freeware version allows a capacity of only 5 files in a vault; registered users will have room for 128 files in their vaults.
- The annoying startup delay in Enigma 1.2 has been eliminated. This wasn't a bug, certain tables were computed at program startup. These tables are now stored in the program and read from disk at startup. Storing these tables on disk instead of calculating them has no impact on the security of the encryption process.

- 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.

Because of all these new features, Enigma 2.0 requires System 7.0 or later. Sorry people, it's time to upgrade. 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 2.0. Enigma 1.2 is compatible with all Macintosh's with at least 512K of RAM and the 128K ROM (there aren't any 128K Macs out there anymore are there?).

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 plaintext 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 just can't realistically use more than about 75 characters for a key. If no packing were done someone searching for a key would only need to examine those 75 characters for each 8 bits 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.

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 2.0 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 brute force a Mac LC-II can break into a file protected by the free version of Enigma in about 16 days of non-stop computing. It would take that same Mac two million centuries to break into the same file protected by the full DES version. Equivalent numbers for a single Cray supercomputer (estimate somewhat rougher) would be less than two hours versus 700,000 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 2.0 contains a single option entitled "Encryption Options...". Selecting this menu item will bring up a dialog box containing the four encryption options available. Selection of an option is indicated by a check in the box adjacent to the option. Below each option is described in detail.

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 deselect the *Remember Key* option.

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.

Destroy Clear-text After Encryption:
This option does exactly what it says it does. After a successful 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. Don't try 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 typed wrong. 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.

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

New for version 2.0 (and why it's version 2.0 instead of 1.3) are 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 if you quit the program.

Vaults should be very intuitive to use. There are obviously lots more features to be added to make the interface even better. Just wait till version 2.1. 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...". This option is not implemented in version 2.0. However, 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. The Compact option when implemented will remove these gaps and keep vaults at minimum size. You can accomplish the same thing manually for now by extracting files from one vault and adding them to a new vault.

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. What you have to do in this case is manually 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.

Both of the above restrictions will be addressed with the next release.

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.

I love the program, but can't you do something about those ugly icons? I'm a software artist not a graphics artist. A few people have sent me icons already, but I'm still looking for the perfect set of Enigma icons (hint: I really like the ? motif). Send me your icons. If I use your icons I will send you a registered copy of Enigma and put your name in the credits if you desire it.

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.

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. The source code to Enigma 1.2 (not 2.0) 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 5. The encryption engine is machine independent and isolated from the rest of Enigma.

Updates

Registered users of any previous version of Enigma may receive an upgrade to Enigma 2.0 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 attempt to notify registered users via email or postcard. If you did not receive a notice you probably moved. 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 a product of Next Wave Software (not yet ™).

Payments and questions can be mailed to:
(Note: the below address is a permanent address, allow about a week for mail forwarding).

Mike Watson
11955 S.W. Clifford
Beaverton, OR 97005

I don't mind email. If you have questions, bug reports, icons, or ideas feel free to email me at the following addresses:
America OnLine : MikeW03
Internet: mdw@cns.cscns.com <-- change