Enigma Version 1.0, released 9/26/92

About Enigma

Enigma, named after the famous German encryption system of world war II, implements a partial version of the NSA developed Data Encryption Standard which is the standard for commercial, unclassified, data protection. Theoretically DES is secure against any computer that can not do more than about a thousand billion encryptions a second. Massively parallel computers however bring DES within the capability of government organizations to break. Short of that kind of computing power DES is completely secure when used properly. There have been no known compromises of DES since it was developed in 1977 [IEEE Spectrum Aug '92].

Restrictions

Because this program is distributed over an international network this program can not implement the full DES standard because US law does not allow export of the complete algorithm. The program you have downloaded implements a crippled 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. Despite these changes the protection provided is still very high against almost all attacks.

A Note About Keys

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. It is because even in the best cases, people simply can not choose from more than about 75 characters for their 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.

How to achieve maximum protection

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 hard disk. Use an application which overwrites deleted files with null data. Several such programs are available commercially. Alternatively use a disk sector editor to write zeros over where your data was written (do this carefully). In a future version I plan to add this capability directly to enigma. Even if you don't follow this step the data will eventually be overwritten by other data. And only an extremely sophisticated user can retrieve data after deletion.

Finally, take reasonable care in choosing your keys. They should be more than a few characters long (13 at least for maximum security). Do not choose obvious things like people, place or pet names. The more unconnected a key is from you and your life the harder it will be to guess.

How to get the full DES version of this program

A full DES version is available for $10 US. The source code 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. With the full version of enigma I will include a utility to zero out files so that no trace of an encrypted document remains on your disk. If you do not or can not pay the shareware fee rest assured, files encrypted with this program are still quite secure.

Notes:

This program can only encrypt data files (files can not contain resources). I plan to add the ability to encrypt applications in the future. You will only get the data fork of a file if you decrypt a file originally containing resources. The program will warn you if you encounter this condition.

This program is compatible with ANY macintosh running any version of the system up to 7.1.1. If you encounter compatibility problems please let me know. It will run on an original Mac 128K and it will run on a Quadra (it's a little faster on the Quadra though).

Updates

Congratulations, you have the very first release of enigma in your possession. I have many plans for more sophisticated versions. If you buy the full DES version you will receive future updates for a nominal cost.

Standard Disclaimer

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

You are free to use and distribute this program 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.

Payments and questions can be mailed to:

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