The new encryption password which you wish to use from now on.

Your existing encryption password.

Select this option if you want the password to be scrubbed from memory immediately after the selected files have been encrypted or decrypted.

Select this option if you want the password to be retained in memory until the PC is shutdown. This option is not available on Windows 95.

Select this option if you want the password to be retained in memory for a specific length of time.

The number of minutes the password will be retained in memory.

Use this button to change the encryption password. Make sure you decrypt all encrypted files before changing the password, as you will not be able to successfully decrypt a file which has been encrypted with the previous password.

#Unless this box is checked, Cryptext will not encrypt any executable (.EXE, .DLL, etc) files

Notes

DISCLAIMER OF WARRANTY

THIS SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES AS TO PERFORMANCE OF MERCHANTABILITY OR ANY OTHER WARRANTIES WHETHER EXPRESSED OR IMPLIED. BECAUSE OF THE VARIOUS HARDWARE AND SOFTWARE ENVIRONMENTS INTO WHICH THIS PROGRAM MAY BE PUT, NO WARRANTY OF FITNESS FOR PARTICULAR PURPOSE IS OFFERED. GOOD DATA PROCESSING PROCEDURE DICTATES THAT ANY PROGRAM BE THOROUGHLY TESTED WITH NON-CRITICAL DATA BEFORE RELYING ON IT. THE USER MUST ASSUME THE ENTIRE RISK OF USING THE PROGRAM.

Any product or brand names mentioned in this document are trademarks or registered trademarks of their respective owners.

Cryptext is a freeware Windows 95 / NT4 shell extension that performs strong file encryption. It uses a combination of SHA and RC4 to encrypt files using a 160-bit key. The current version of Cryptext can be found on my home page at http://www.pcug.org.au/~njpayne

Cryptext may be used in any way, for any purpose, at no cost. It may be distributed by any means, provided that the original files as supplied by the author remain intact and that no charge is made other than for reasonable distribution costs. Note that Cryptext contains strong cryptographic routines upon which some countries place distribution and/or use restrictions. Verify that you are allowed to use/distribute Cryptext before doing so.

To install Cryptext

1. If you have a previous version of Cryptext installed and you have files encrypted with the old version, decrypt the files
2. Unzip the contents of CRYPTEXT.ZIP into a directory
3. In Explorer, right-click on CRYPTEXT.INF and select Install from the popup context menu

To install this shell extension on Windows NT you must be logged in as administrator or a user who is a member of the Administrators group. This is because installing a shell extension on NT requires update rights to a part of the registry to which a normal user cannot write.

To uninstall Cryptext

1. From the Start menu, select Settings, then Control Panel, then Add/Remove Programs
2. If you are running on Windows 95, select the "Cryptext (Windows 95) (Remove only)" entry. If you are running on Windows NT, select the "Cryptext (Windows NT) (Remove only)" entry.
3. Click on the Add/Remove button

How does it work

1. When you install Cryptext it adds "Encrypt" and "Decrypt" items to the context menu you get when right-clicking on files or directories in Explorer.
2. When you encrypt a file, Cryptext takes your password and uses the SHA-1 one-way hash function to generate a 160-bit key.
3. For each file selected, it then cancatenates the key generated in step 2 with (a) the number of 100-nanosecond intervals since January 1, 1601, and (b) a 32-bit random number, and hashes this concatenation with SHA-1 to produce the key which is used for the encryption. This step is taken to ensure that no two files are encrypted with the same keystream.
4. The time and random number values used in step 3 are stored in plaintext with the encrypted file, so that the file can be successfully decrypted when the correct passphrase is supplied. There is no requirement that these values be kept secret, only that they be unique for each file.
5. In order to verify your password on second and subsequent executions, Cryptext takes the 160-bit key generated in step 2, adds it to the end of your password, and applies the SHA function to the concatenation of the password and key. The resultant hash is saved so that subsequent passwords can be checked for validity by being put through the same two-step hash and compared with the stored value.

For decryption, Cryptext first reads from the encrypted file the values saved in step 4, and concatenates them with your hashed passphrase to obtain the decryption key.

Running Cryptext

1. In Explorer, select the files and directories to encrypt. Click the right mouse button and select “Encrypt”.
2. If you are running on Windows NT 4 then you have the option to retain the encryption password in memory for the duration of your NT session. If you are running on Windows 95 you must enter the password for each encryption or decryption.
3. After the initial execution of Cryptext, you cannot change your encryption password unless you know the existing password. If you forget the password, you have to uninstall and reinstall Cryptext. If you have files you have encrypted and you have forgotten the password then those files are not recoverable.
4. Cryptext allows a password to be up to 255 characters long. As a file encryption password is generally in use for much longer

than a login password, you should use more care selecting it. For more information on good password selection, use one of the www search engines to search on the words "password", "selection", and "good".

5. Cryptext assumes that the file system on which it is running supports long filenames. When it encrypts a file it adds the extension ".$#!" to the filename. This name change will fail if the existing filename already exceeds 252 characters or if the file system does not support long filenames (such as a NetWare server volume which does not have long namespace support loaded). The resulting file is still encrypted but it does not have the extension which Cryptext recognises, and when you decrypt it you will be queried whether the file is actually encrypted.

Information on cryptography

If you are interested in finding out more about encryption and cryptography:

1. RSA's web site at www.rsa.com has a good cryptography FAQ available both online and as a downloadable PDF file.
2. You can find cryptographic source code at
   idea.sec.dsi.unimi.it/pub/security/crypt/code
   which is where I found the source for both "RC4" and SHA.
3. Bruce Schneier's book "Applied Cryptography" has a comprehensive coverage of both protocols and algorithms.
4. An encryption library that provides an easy-to-use and consistent interface to many encryption algorithms is available from http://www.cs.auckland.ac.nz/~pgut001/cryptlib.html

Nick Payne
njpayne@pcug.org.au