PRODUCT REVIEWS

December 9, 1996 (Vol. 18, Issue 50)

Encryption software

CrypEdit leaves an insecure feeling
By Joe Peschel

As the need for data security grows, more vendors are creating file-encryption products. Yet not all of them are effective. One example is CrypEdit 5.0D, from Genio USA, which calls itself the "industry leader in encryption and data security software for Windows." Despite this lofty assertion, I can't recommend this product.

CrypEdit is easy to use, includes a nice text editor, lets you encrypt and decrypt any file, and optionally offers clues about your password in case you forget it. In addition, you can use CrypEdit's proprietary key-set files to share encrypted files with other users. The utility can also compress, UUencode, and securely delete files. Even though the encryption scheme has changed in Version 5.0D, I don't think it's any stronger than in previous versions.

It's difficult for a typical user to gauge the strength of cryptographic software. For example, a user might look at the output of a simple substitution cipher and be satisfied that a file encrypted in such an elementary manner is secure. Unfortunately, it's not. What's worse is that not only could your ciphertext be read by an attacker, but someone also could reverse-engineer the algorithm and then post a "cracker" on the Internet that renders the encryption scheme useless.

Any proprietary encryption algorithm whose security depends on the algorithm's remaining a secret is called a restricted algorithm and is a weak method. If the algorithm is revealed, encrypted files can be cracked. Strong algorithms have been subjected to review by other cryptographers and mathematicians. The algorithm behind CrypEdit is proprietary, and the vendor will not reveal it.

However, with strong cryptography, such as Pretty Good Privacy (PGP), it doesn't matter if the algorithm is revealed or even published. The encrypted files still can't be decrypted without the key. The compelling argument for PGP is that it still hasn't been broken. A strong implementation of PGP is ViaCrypt's PGP Business Edition, Version 4.0. (See Product Reviews, April 15, page 121.)

On top of the secrecy shrouding a proprietary, restricted algorithm, you'll come across claims about the algorithm's unbreakability and superiority to proven encryption schemes,

such as RSA, PGP, DES, and Blowfish. But proprietary algorithms can be vulnerable to elementary cryptanalytic attacks.

To confirm my opinion, I consulted two outside resources; neither could recommend CrypEdit. To judge CrypEdit's strength, I sent Randall Williams, an independent computer consultant, plaintext and ciphertext pairs from CrypEdit 5.0B and 5.0C. I encrypted the plaintext files with one password in top-secret mode.

Although Genio won't reveal the algorithm, Williams determined that it's likely a stream cipher with a lot of problems, making CrypEdit a weak product. He also noted that the algorithm displayed evidence that Genio is attempting a block cipher.

Williams launched several typical attacks that cryptanalysts use -- known plaintext, chosen plaintext, and chosen key -- against CrypEdit. His known plaintext attack revealed that if you have one or more known plaintext and ciphertext pairs, you can decrypt any other file encrypted with the same key. Further, according to Williams, it's a simple matter to write a program that will grab the key stream and test it on other files.

The chosen plaintext attack revealed that a great deal of information and patterns show up in the key stream, which is bad for maintaining security. Most notable is the all-zero file, which gives you the key stream for any given key.

Williams' chosen key attacks showed that some keys generate a stream where about 50 percent of the key stream is the same as other key streams. Other keys generate key streams that are similar enough that cryptanalysis could restore the text.

Williams concludes by saying CrypEdit is a typical beginner cipher that is based on transparent modular addition and subtraction of a key stream. He sees no evidence that this program would stand up to more advanced cryptanalysis. It is clearly breakable.

I also asked AccessData (http://www.accessdata.com), an encryption-testing company that I've called on before, to look at CrypEdit. The company concluded that the program was very simple and provided "virtually no security."

"It took one of our cryptographers less than 2 hours to analyze the output generated by CrypEdit and determine a very successful method of attack," said Eric Thompson, president of AccessData and one of the top cryptanalysts in the country.

Joe Peschel, a free-lance computer journalist, covers security programs and other utilities. He can be reached at jpeschel@aol.com.

Decrypting the jargon

0-file - A file that contains nothing but 00h or null values. In this case, if you encrypt a 0-file and another file with the same key, you can decrypt the file using the key stream from the 0-file, which must be longer than the other file.

Block cipher - Ciphers that operate on groups of bits simultaneously.

Chosen key attacks - Attacks that discover relationships between the ways different keys encrypt the same data.

Chosen plaintext attacks - Attacks that find information about the key when you have known-plaintext and ciphertext pairs; also, you can encrypt whatever plaintext you choose.

Ciphertext - An encrypted file.

Key stream - The stream or sequence of data generated by a key.

Known plaintext attacks - Attacks that deduce the encryption key by looking at the plaintext and the corresponding ciphertext; these are plaintext and ciphertext pairs.

Modular addition/subtraction - A branch of number theory. Think of it as clock arithmetic where modulo 12 is used: If it's 9 p.m. and you sleep for 13 hours, you wake up at 10 a.m.

Plaintext - Any file that is not encrypted.

Proprietary and restricted algorithms - Algorithms that are kept secret to keep the encryption from being cracked.

Stream cipher - Ciphers that perform encryption operations on one bit or byte at a time.

Substitution cipher - Ciphers that substitute "D" for "A," "J" for "G," and "T" for "Q," for example.

THE BOTTOM LINE: POOR

CrypEdit 5.0D

This product will likely protect sensitive documents from novices; however, those who want real security should use a proven algorithm such as triple DES or Blowfish.

Pros: Nice text editor.

Cons: Weak encryption.

Genio USA, Northbend, Wash.; (800) 918-9850, (206) 831-5591; fax: (206) 831-5591; geniousa@geniousa.com; http://www.geniousa.com/genio/

Price: $70

Platforms: Windows 3.1x, Windows 95, Windows NT 3.51 or later.