

PRODUCT REVIEWS

July 7, 1997 (Vol. 19, Issue 27)

WebHub develops innovative Web applications;

'scrambled' doesn't mean secure with Crypt-o-Text

Windows encryption utility

Crypt-o-Text 1.24

By Joe Peschel, Review Board

E-mail security seems to be on everyone's minds these days, and there are plenty of both weak and strong encryption products from which to choose. Crypt-o-Text 1.24, from Savard Software, is a Windows-based encryptor that's easy to use on small text files and has a nice built-in text editor. Unfortunately, Crypt-o-Text proved a weak e-mail encryption solution.

According to the company, Crypt-o-Text uses a "complex proprietary encryption algorithm"; the vendor says "there is absolutely no way to determine what password was used by examining the encrypted text."

If you're looking for an encryption program and see the phrase

"proprietary algorithm" used on the box or in the documentation, I suggest looking elsewhere.

Crypt-o-Text encrypts data based on a password you enter. This password doesn't need to be case-sensitive, which makes Crypt-o-Text more vulnerable to brute-force attacks.

Unfortunately, brute force isn't required to recover a Crypt-o-Text password and read the file. A cracker is available that breaks a Crypt-o-Text message (Version 1.21 through 1.24) in a couple of seconds. (The cracker is available at <http://members.aol.com/jpeschel/index.htm>.) The author of the cracker, known as Casimir, traced the encryption

algorithm using a system-level debugger and then reversed the algorithm.

Savard Software, wisely, plans to replace Crypt-o-Text with another product that uses Blowfish, a secure algorithm. Unfortunately, the company plans to implement Blowfish in Electronic Code Book mode, which is the weakest mode available and vulnerable to a known plain-text attack.

Crypt-o-Text doesn't cost much. But good encryption products don't necessarily cost much, such as Briggs SoftWorks' Puffer, and some are free, such as PGP. In any case, I suggest using a product other than Crypt-o-Text.

- Savard Software, Kennewick, Wash.; (509) 736-6342;
<http://www.owt.com/users/rsavard/software>; \$15; Windows 95, Windows NT 3.51 or 4.0,
Windows 3.1.

Copyright (c) InfoWorld Publishing Company 1997