

PRODUCT REVIEWS

April 15, 1996 (Vol. 18, Issue 16)

Windows e-mail encryption software

ViaCrypt key to easy security

By Joe Peschel

To its fans, freeware PGP is the only encryption software for e-mail. Likewise for them, its author, Phil Zimmermann, has become a crypto-folk hero. Because I'm a fan of PGP and Zimmermann, I was happy to see that ViaCrypt PGP Business Edition, Version 4.0, (and Personal Edition, too) has taken strides nearly as large as the prime numbers the program generates in bringing pretty good privacy to those who've never used it or to folks who found the freeware unfriendly.

Public, single key cryptography

For e-mail, ViaCrypt PGP (VPGP) (and freeware PGP) employs public key cryptography. In a public key cryptosystem, a public key and a private key

are created. PGP uses a secret key algorithm, International Data Encryption Algorithm (IDEA), for encrypting the body of a message, and RSA for encrypting the message key.

After creating the key, I send my public key to my correspondent, Dave, and he encrypts his message to me with it. I decrypt the message with my private key. Likewise, Dave sends me his public key. I encrypt my message to him with it and he decrypts it with his private key.

With VPGP (and PGP) either of us can sign a message with our private key. For instance, after I encrypt a message to Dave using his public key, I can sign the message with my private key so that he knows it's from me.

VPGP also performs hard disk encryption using only IDEA, a single secret-key system whose key length is 128 bits. You may think this minuscule when you consider created key sizes of 1,024 bits and 2,048 bits, but cryptographer Bruce Schneier (author of Applied Cryptology, <http://www.wiley.com/compbooks/z6.html>) estimates that such a key is as hard to crack as a 2,304-bit public key is hard to factor.

And when cryptographers say "hard" they often mean computing with thousands of systems and getting an answer in months, years, or sometime after the end of the universe. Public key and single key systems are not trivial encryption schemes in which the encryption is secure only if the algorithms remain secret. Instead, the

algorithms' source code has been published and subjected to review by other cryptographers.

Despite that, PGP has never been cracked. Moreover, ViaCrypt says that even when taking into account the increases in computing power and the progress in the mathematics of factoring, if something is encrypted at your birth today with a 2,048-bit key, it will still be secure when you die.

Encryption shouldn't be cryptic

In a DOS environment, key creation, use, and management with freeware PGP means entering a lot of command-line parameters. Consequently, new and even seasoned users may find themselves executing `pgp -h(elp)` more often than they care to. In Version 2.7, ViaCrypt eliminated the need to memorize the parameters but still dropped to a DOS environment to generate its key pairs.

I tested Version 4.0 of VPGP under Windows 95 and never once

dropped to a DOS environment. Creating the recommended 1,024-bit key took only a few minutes, but creating a second 2,048-bit key took about a half-hour.

ViaCrypt estimates that the time to generate the larger key is about eight times the time required to generate the 1,024-bit key. Still, the extra time required to generate a pair of even larger primes is worth the extra security, especially if you are paranoid about future breakthroughs in factoring large numbers. The larger key size, ViaCrypt says, also slows decryption and signature creation.

VPGP has all the features I'd expect of a Windows PGP interface; anything you can do with PGP you can do easier with VPGP. It includes backward PGP compatibility; single-click encryption and signature attachment, options that let you certify and revoke keys; and original plaintext file deletion after encryption.

Nice, also, are features that allow encryption or decryption to the screen only. You can also vary

what VPGP expects as minimum pass phrase. The default of eight characters, for instance, can be changed to 12, and you can specify a minimum number of special characters.

Other features, though, set VPGP Business Edition 4.0 apart from its predecessor. With the new Enclyptor you can encrypt and sign files or decrypt files and verify signatures after the plaintext is copied to the Clipboard. The Enclyptor makes it easy to send encrypted e-mail, but you may want to peek at the contents of the Windows Clipboard Viewer before you encrypt your message. ViaCrypt has also added a key that only encrypts and decrypts, and another that will only sign and verify.

VPGP also lets you configure which of its many functions you want your employees to use. Configuration isn't as simple as point and click, but with some planning, it isn't that difficult, either.

You, as an administrator or security officer, can disable an employee's

ability to change VPGP's settings. You can also create corporate access and corporate certification keys. The access key lets you decrypt any files encrypted by your corporation's VPGP Business Edition users. The certification key forces VPGP to display

only those keys it certifies.

ViaCrypt, for a fee, can hard code VPGP's options and corporate access and certification keys. Soon ViaCrypt will release a Corporate Security Officer's Guide with training materials and sample e-mail security policies.

By the way, you can now temporarily transport strong encryption overseas without paperwork; so, you don't have to uninstall to take your laptop with you overseas.

Joe Peschel is a free-lance computer journalist. He can be reached at jpeschel@aol.com.

War strategies of the hacker

Using cryptography doesn't mean you're necessarily safe. Attackers can use a number of methods to uncover encrypted information or passwords; cryptographic methods tend to be much more difficult than tried-and-true breaking and entering.

Noncryptoanalytic attacks

- Keystroke loggers Stealth utilities capture keystrokes.
- Passwords from other programs Users may be using the same password as on less secure applications such as screen savers.
- Brute force attack on short passwords Short passwords, especially real words, are susceptible to word list and dictionary attacks.
- Plaintext left in the clear An attacker with access to a system may find copies of the unencrypted plaintext in backups or undeleted temporary files.
- Hex editor An attacker may attempt to recover plaintext, backup, or temporary files with a Hex editor.
- Electromagnetic radiation monitoring Sophisticated equipment measures a system's radiation output.
- Outright theft of the system The attacker has plenty of time to search for and recover the victim's plaintext.

Cryptoanalytic attacks

- Factoring algorithms Small keys may be factored using various mathematical algorithms: Number Field Sieve, Multiple Polynomial Quadratic Sieve, Quadratic Sieve, Trial division.

- Paul Kocher's Timing Attack A theoretical attack attempts to time several encryptions to derive the private key. It assumes access to the victim's system and sophisticated monitoring equipment. It has not been successfully implemented.

THE BOTTOM LINE: VERY GOOD

ViaCrypt PGP Business Edition, Version 4.0

ViaCrypt PGP (VPGP) offers the easiest interface for the most popular encryption program around.

Pros: Enclyptor makes pasting encrypted text a breeze; anything you can do with free PGP's command line you can do with mouse clicks with VPGP; lets you create corporate access and certification keys; security officer can configure so that features are disabled, or for an extra fee ViaCrypt will hard-code.

Cons: Doesn't handle long file names.

ViaCrypt, Phoenix; (800) 536-2664, (602) 944-0773; fax: (602) 943-2601;
info@viacrypt.com; <http://www.viacrypt.com>.

Price: \$149; corporate bundles of 50 start at \$60 per user; personal edition costs \$129.

Platforms: Windows 3.x, Windows 95, Windows NT, Macintosh, and various Unix flavors.

Copyright (c) InfoWorld Publishing Company 1996