Key Escrow Done Right

With most encryption systems today, if you forget your key, you're out of luck. PGP author Phil Zimmermann admits he receives panicky e-mails about lost keys all the time. His response? Be more careful.

But now Zimmermann's archrival, RSA Data Security, has a much better answer.

The company's new program, RSA Secure, uses a technique called "secret splitting," which lets you make multiple copies of your key and give them out to friends for safekeeping. This works a bit like the key escrow system used in the US government's Clipper chip, but with one crucial twist: you control how the key should be split up, how many parts need to be reassembled to unlock your computer, and, most importantly, who holds the keys.

RSA Secure encrypts data using a powerful and proprietary RC4 stream-encryption algorithm with an 80-bit key. Files automatically encrypt when you shut down your computer and decrypt when you start back up - provided you type the correct key, of course.

Forget your only PGP key? RSA Secure has a better way to lock up.

RSA Secure is ideal for laptop owners who want to carry around confidential information without worrying about it falling into the wrong hands. Thieves might swipe your laptop, but if the files are encrypted, they can't nab your data.

What makes RSA Secure better than its rival programs - such as Fischer International's SafeBoot and Scrambler Technologies' Scrambler for Windows - is the ability to generate multiple keys. With RSA Secure, you can split the key into four parts and give a specially made "key diskette" to your company's chief information officer, treasurer, auditor, and director of human resources. Now, if Sam in Finance gets hit by a truck, you can still access your accounts.

Is RSA Secure really secure? The company claims that cracking a single 80-bit RC4 key would take more than 70 trillion years of MIPS computer time. It's certainly fast: the RC4 algorithm cranks through 850,000 bits per second on a 33-MHz 486 PC. - *Simson Garfinkel*

RSA Secure: US$129. RSA Data Security Inc.: (800) 782 5453, +1 (415) 595 8782, fax +1 (415) 595 1873, on the Web at *http://www.rsa.com*.