The cryptography craze

As commercial use of Net soars, so does interest in debate over encryption / **Simson L. Garfinkel**

SAN FRANCISCO – THE ultra-plush Fairmont Hotel here, which has quartered movie and TV stars, rock musicians, and other celebrities, is this week host to an odd collection of scientists, mathematicians, and software writers all discussing codes and cryptography.

Believe it or not, this meeting of the world's greatest cryptographers – like MIT professor Ron Rivest, who discovered the RSA data encryption algorithm along with Adi Shamir and Len Adelman 20 years ago this summer – has attracted more than 2,400 groupies, uh, attendees. That's up from 1,200 last year and just 600 two years ago.

Data encryption is hot and the third annual RSA Data Security Conference is the place to be if you're turned on by lectures on RSA's new S/MIME toolkit by crypto engineer Rhonda Rasine, and endless debates about whether mechanisms to assure the FBI has access to every file in every computer in the world should be built into computer programs.

The exponential growth of the conference is a direct result of the commercialization of the Internet. Those who have come here know that cryptography, the mathematical science of scrambling information, is the only way to guarantee that financial information sent over the Internet is kept secret and is not modified in transit. This makes all kinds of businesses, from banks to mail-order catalog houses, interested in this once arcane science.

The good news, says AT&T scientist Matt Blaze, is that the engineers now know how to use cryptography for every necessary business transaction. Whether you are signing your name, spending money with your Visa card, or receiving a piece of "locked" software over the Internet, Blaze has an algorithm for you. The technology isn't holding anything back.

The problem, says Blaze, is that to use this technology the Clinton administration wants US companies to adopt a system for "key escrow" or "key recovery," which means there is a copy of every key ever used to encrypt a message on file somewhere, should the US government ever want to decrypt one of those same messages.

Without key recovery, the administration is worried cryptography will be used by terrorists, drug dealers, and child pornographers to hide their evil deeds. But "we have no idea how to do [key escrow] in a secure manner," says Blaze. How do you guarantee that the keys won't be misused?

"Key escrow converts this problem that we know how to solve, establishing secure channels, into a complex problem that we don't know how to solve, and whose solutions are fundamentally expensive and risky," says Blaze. "We in the crypto field had gotten very close to putting ourselves out of business . . . and now the government has handed us a huge set of difficult problems."

One company that stands to make a lot of money off the Clinton administration's policies is Trusted Information Systems, a Maryland-based firm headed by an ex-National Security Council scientist. TIS holds a software patent on the very kind of key-escrow technology that's been advocated by the administration. And TIS is selling a "key recovery toolkit" that lets other firms build these antiprivacy measures into their own products.

Why would companies like IBM and Microsoft want to booby-trap their software so that a file, once encrypted, could be forcibly decrypted by somebody other than the intended recipient or the file's owner?

One reason is exportability. Today there are strict controls that essentially forbid companies to export software that uses strong encryption. Companies that build in back doors for the FBI get those restrictions waived.

A second reason is corporate control. Today US businesses are just waking up to the fact that encrypted information can be trapped if the only person who has the key forgets it, quits, or gets hit by a truck. So some businesses are likely to want some "key recovery" system for their own back-door access to information.

But while there is some support in the computer industry for the TIS solution, you won't find any key-recovery system in the next version of Netscape Navigator that's shipping later this year.

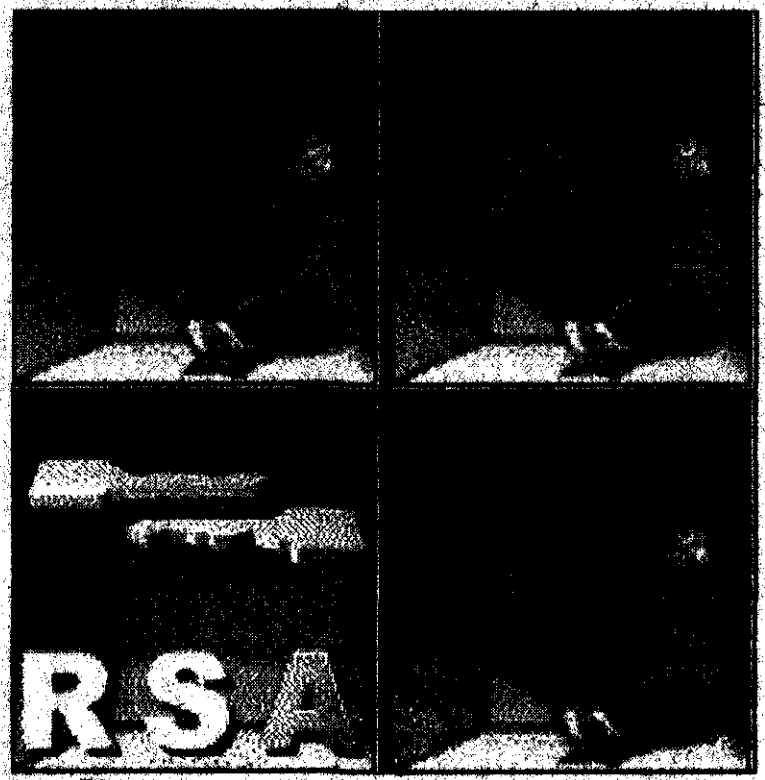
Renamed Netscape Communicator, this new version of the popular Web browser will have the ability to encrypt electronic mail using S/MIME, an extremely strong encryption system. Other programs for encrypting mail with S/MIME can be found on RSA's home page, at http://www.rsa.com. By the end of the year, 50 million people might have the ability to send encrypted mail – all without key recovery of any kind.

Just about the only person at the conference who is fed up with the key-escrow debate is MIT professor Silvio Micali. "I'm also sick and tired about digital signatures and encryption," he said.

Instead of rehashing these old issues, Micali said cryptographers should be looking for fundamentally new things that can be done with cryptography, things that can't be done any other way.

For instance, Micali described a new, as-yet-undiscovered algorithm that could be used during negotiations between a buyer and a seller. The algorithm would see if the buyer's best offer was too low for the seller's bottom line. If there was a gap, the algorithm would report that no deal is possible. Otherwise, it would let the two sides haggle.

Now there's a computer algorithm that could be a threat to national security.



The third annual RSA Data Security Conference is a hotbed of talk about "key recovery" of encrypted material.

Technology writer Simson L. Garfinkel can be reached at plugged-in@simson.net.