The Case against Regulating Encryption Technology

One of the pioneers of computer security says the U.S. government should keep its hands off cryptography

by Ronald L. Rivest

The widespread use of cryptography is a necessary consequence of the information revolution. With the coming of electronic communications on computer networks, people need a way to ensure that conversations and transactions remain confidential. Cryptography provides a solution to this problem, but it has spawned a heated policy debate. U.S. government agencies want to restrict the use of data encryption because they fear that criminals and spies may use the technology to their own advantage.

Before the 1970s, cryptography was too complicated and too expensive for everyday use. Two inventions changed this picture dramatically: public-key cryptography and the microprocessor. The idea of using public and private encryption keys—first proposed in 1976 by electrical engineers and computer scientists Whitfield Diffie, Martin E. Hellman and Ralph C. Merkle—paved the way for the general use of strong cryptography, which scrambles messages so effectively that it would take many years of computer time to break the code. And the growing availability of fast microprocessors gave more and more computer users the ability to make the calculations necessary for this kind of encryption.

As strong cryptography became easily accessible in the late 1980s and early 1990s, two government agencies grew concerned about its widespread deployment. The National Security Agency (NSA), which monitors electronic communications around the globe, worried that it would be unable to decipher the encrypted messages of potential spies and terrorists. Similarly, the Federal Bureau of Investigation feared that criminals in the U.S. would use the encryption software to thwart surveillance of their voice or data communications. Over the past decade these agencies have pushed for government regulation of encryption technology and have favored the continuation of current restrictions on the export of strong encryption software.

The government's concern is that the "bad guys" will benefit from the new cryptographic technology. This is certainly possible—the sun shines on the evil as well as the good. But it is poor policy to clamp down indiscriminately on a technology merely because some criminals might be able to use it to their advantage. For example, any U.S. citizen can freely buy a pair of gloves, even though a burglar might use them to ransack a house without leaving fingerprints.

I rather like the glove analogy; let me expand on it a bit. Cryptography is a data-protection technology just as gloves are a hand-protection technology. Cryptography protects data from hackers, corporate spies and con artists, whereas gloves protect hands from cuts, scrapes, heat, cold and infection. The former can frustrate FBI wiretapping, and the latter can thwart FBI fingerprint analysis. Cryptography and gloves are both dirt-cheap and widely available. In fact, you can download good cryptographic software from the Internet for less than the price of a good pair of gloves.

Should the use of cryptography be restricted to satisfy the concerns of the NSA and the FBI? It is true that these two agencies may find their jobs more difficult as cryptographic technology spreads. But we should also consider cryptography's benefits to society as a whole. Most people use cryptography to prevent crime rather than to hide it, just as most people wear gloves to protect their hands rather than to hide their fingerprints. By ensuring the confidentiality and authenticity of electronic banking and Internet commerce, cryptography prevents theft and credit-card fraud. The vigorous application of cryptography may also improve national security: the encryption of communications, for example, protects U.S. businesses from industrial espionage. Paradoxically, we may create a safer society by promoting a technology that somewhat hampers law enforcement.

Some have hoped for compromise solutions that would allow strong cryptography to be widely used while still enabling the NSA and the FBI to decrypt messages when lawfully authorized to do so. For example, there have been key-escrow proposals that would require users to register their software encryption keys with law-enforcement agencies, and key-recovery proposals that would give government agencies backdoor access to the keys. In a typical key-recovery scheme, an encrypted version of the message encryption key is sent along with each message. An FBI-authorized key-recovery center can use a master backdoor key to decrypt the message key, which is then used to decrypt the message itself.

In my opinion, these systems would satisfy no one. They are very easy to circumvent: spies and criminals could modify the encryption software to disable the key-recovery features, or they could simply download alternative software

from the Internet. Key recovery would be very expensive, too. Someone would have to pay for creating, staffing and maintaining the key-recovery centers. But the most subtle and serious cost in the long run would be the erosion of confidence in the government resulting from an increased sense of "Big Brotherism." To get an idea of the intrusiveness and impracticality of key recovery, imagine that whenever you bought a pair of gloves you were legally required to sew latex copies of your fingerprints onto the gloves' fingertips!

SLIM FILMS

Key-recovery systems would also create substantial security risks. The system's most serious flaw is that the same back doors used by the FBI to decipher encrypted messages would become targets for criminals, hackers, spies and even disgruntled employees of the FBI itself. If criminals or hackers managed to penetrate a key-recovery center and steal a master backdoor encryption key, they would be able to decrypt Internet communications at will. Millions of corporate, personal and government secrets would suddenly become vulnerable to theft and tampering.

In 1993 Congress asked the National Research Council to study U.S. cryptographic policy. The council then convened a blue-ribbon committee of 16 members. Its superb 1996 report, the result of two years' work, offered the following conclusions and recommendations:

- "On balance, the advantages of more widespread use of cryptography outweigh the disadvantages."
- "No law should bar the manufacture, sale or use of any form of encryption within the United States."
- "Export controls on cryptography should be progressively relaxed but not eliminated."

The committee members concluded that a ban on unregulated encryption would be "largely unenforceable." But the FBI and the NSA continue to push for key recovery and to oppose the relaxation of export controls unless key recovery is incorporated into the exported software.

Strong cryptography only gets easier to implement—and harder to regulate—over time. Professional societies are adopting public cryptographic standards that even a high school student can convert into programs. And new techniques such as "chaffing and winnowing"—which does not encrypt a message but achieves confidentiality by hiding pieces of the message in a welter of random data, or chaff—illustrate the enormous technical difficulties involved in trying to control cryptography.

The economic consequences of our current policy are also becoming clearer. A recent study conducted by the Economic Strategy Institute, a think tank in Washington, D.C., concluded that continuing the export controls on cryptographic products will cost the U.S. economy more than $35 billion over the next five years. My personal opinion is that the U.S. risks losing its leadership position in the software industry because of its restrictive export policy.

Finally, the ability to have private conversations is in my view an essential democratic right. Democracy depends on the ability of citizens to share their ideas freely, without fear of monitoring or reprisal; this principle should be upheld as much in cyberspace as it is in the real world. For the U.S. to restrict the right to use cryptography would be a setback for democracy—and a victory for Big Brother. SA

The Author

RONALD L. RIVEST is the co-inventor of RSA encryption, the most widely used public-key cryptosystem. He is Edwin S. Webster Professor of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology and a founder of RSA Data Security (a subsidiary of Security Dynamics Technologies).

Further Reading

CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY. Edited by Kenneth W. Dam and Herbert S. Lin, National Research Council. National Academy Press, 1996. The report can be found at http://www.nap.edu/readingroom/books/crisis on the World Wide Web.

THE ELECTRONIC PRIVACY PAPERS: DOCUMENTS ON THE BATTLE FOR PRIVACY IN THE AGE OF SURVEILLANCE. Bruce Schneier and David Banisar. John Wiley & Sons, 1997.

PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION. Whitfield Diffie and Susan Landau. MIT Press, 1998.