KEEPING SECRETS SECRET

PUBLIC RESEARCH IN CRYPTOLOGY CONFLICTS WITH GOVERNMENTAL CONCERNS ABOUT NATIONAL SECURITY

BY IVARS PETERSON

Imagine a network of filing cabinets, connected by subterranean tunnels through which agents can crawl freely. The agents can copy or alter anything they want from any of the files without leaving signs of their intrusion. An analogous situation is developing as tens of thousands of computers connect businesses, corporations and banks in giant webs. Magnetic memories and the invisible flow of electrons are rapidly replacing paper and ink.

It is possible to wiretap a data transmission line with only $1,000 worth of equipment bought at a computer store. By examining the signals he picks up, a wiretapper often can break the simple code that tells a receiving bank, for example, that the message is authentic. Then he can program his personal computer to mix fraudulent messages with legitimate fund transfers.

The growing use of computers in communications networks has raised questions of ensuring privacy and security. How can a bank know that a computerized fund-transfer request is legitimate? How can a utility prevent terrorists from tapping into computer lines that control electrical power systems and from causing blackouts? How can two people communicating by electronic mail be sure no one is intercepting their messages? How is it possible to protect the vast quantities of private information, such as credit records and medical histories, now stored in computer data banks?

The solution to some of these problems lies in the use of sufficiently strong codes so that only authorized persons can decipher them. This idea has attracted first-rate mathematicians and computer scientists to cryptology, the study of the enciphering and deciphering of secret messages.

In the past, cryptology was a government monopoly. Now the monopoly is crumbling in the face of a broad, economically motivated interest in cryptology outside government. The low cost of electronic equipment, the growing scientific and technical expertise and the increased need for coding have combined to produce a strong market for encryption devices and "unbreakable" codes.

The guardian of governmental and military interests in cryptology is the National Security Agency (NSA), one of the most secret of federal agencies. The NSA's job is to preserve the security of U. S. communications by devising the codes that protect the country's secrets while gathering intelligence by monitoring the communications of foreign governments. The NSA has probably the world's largest reservoir of expertise in codes and communications security.

In January 1979, Vice Admiral Bobby R. Inman, NSA director at the time, expressed NSA's concern about nongovernmental research in cryptology. He said, "I believe that there are serious dangers to our broad national interests associated with uncontrolled dissemination of cryptologic information within the United States."

The NSA has two fears: First, published research results may reveal to certain countries that their codes are insecure and lead them to change their codes to ones the NSA can't break; second, scholars may publish instructions enabling anyone to make unbreakable codes, which would greatly inhibit the NSA's intelligence-gathering function.

In the last few years, the NSA has made several attempts to control and restrict nongovernmental research in cryptology. This is where the conflict between public and national interest arises most directly.

The NSA's and the government's efforts to control information raises vexing questions concerning individual freedom and governmental controls. Most of the legal and constitutional issues are still unresolved.

Businesses and the public are interested in a secure, private computer communications network. Scientists want the freedom to do research and publish their results. The government must protect the national interest and maintain national security. This web of conflicting interests pits First Amendment rights against national security needs. Even examining the question raises the paradox of seeking a public resolution of a matter that deals with secrets.

When the National Bureau of Standards and IBM developed a "data encryption standard," a coding system for civilian and commercial use, the NSA — as adviser on the project — persuaded the NBS to weaken part of the system. Critics claim this cipher was made just strong enough to withstand commercial attempts to break it, but weak enough to yield to NSA computers.

The thumbnail-size cipher machine, itself a tiny computer, became the official Data Encryption Standard (DES) in 1977.

(continued on page 254)

Science Service, Inc. is collaborating with JSTOR to digitize, preserve, and extend access to *Science News.* www.jstor.org

KEEPING SECRETS

(continued from page 252)

Federal agencies are required by law to use the DES for enciphering nonclassified computer data such as Internal Revenue Service records. Manufacturers of the equipment see a market for the device among banks, insurance companies and other commercial concerns.

Each DES user has a key, a string of 56 zeroes and ones, which enables the user to encipher data, and anyone who has that particular key to decipher the information. The difficulty, as several computer scientists pointed out, was that the key was too small. A sufficiently large computer could find the key in a reasonable time by trying all the possible combinations of zeroes and ones. But only a government agency like the NSA would be likely to have such a computer.

Meanwhile, Stanford University computer scientist Martin Hellman and several others were working on a new kind of code, one in which knowledge of how to encode did not necessarily reveal how to decode a message. Their system was more secure than the DES and made unforgeable electronic signatures possible. It appeared to be the "unbreakable" code.

One problem with the DES is that the key must be sent to all users before messages can be exchanged. However, sending a key involves a time delay and raises the possibility the key may fall into unauthorized hands. The new, "public-key" cryptography proposed by Hellman avoids this problem. There are two related keys, one for the sender and one for the receiver, but given only one key, it is impossible to deduce the other. Thus, one key can be made public and anyone can send a coded message, but only the receiver with the second, complementary key could unlock the message.

In 1977, an NSA employee pointed out that academic scientists could be prosecuted if they discussed their cryptologic research at a scientific meeting open to foreign scientists. The basis of the threat was the Arms Export Control Act and the International Traffic in Arms Regulations, which restrict the export of "technical data" that endanger U. S. national security or adversely affect foreign policy. The Justice Department thinks the rules may be unconstitutional, but they have never been tested in court.

In 1978, at NSA's request, two applicants for unclassified patents on cryptologic devices suddenly received secrecy orders, classifying the inventions. The government action stunned officials at the University of Wisconsin at Milwaukee, where one of the inventors worked. They protested the ruling as a serious intrusion into academic freedom. After considerable publicity, both orders were lifted.

For the first time, beginning in late 1978, the director of the "Never Say Anything" agency (NSA) gave interviews to the press and made a public speech. Inman spoke out on the need for restraint in the area of cryptology. He visited leading nongovernmental cryptologists in universities and research laboratories or invited them to visit NSA.

Inman's search for contacts led the NSA and the academic community to establish a forum to determine where and how the line between government needs and those of basic research might be drawn. This forum, the Public Cryptography Study Group, on Feb. 7, 1981, voted to recommend a voluntary system of prior restraints on the publication of cryptology research.

The dissenting opinion came from George I. Davida, representing the Computer Society of the Institute of Electrical and Electronics Engineers. It had been one of Davida's inventions that had received a secrecy order a few years before. He wrote, "The effects of withholding basic or applied research results relating to cryptography would handicap researchers, not only in data security, but in computer science and engineering and allied areas. The restraints would remove from the public domain the most interesting and intellectually stimulating results. The long-term consequences would no doubt be harmful to the Nation."

Other scientists are also concerned that such voluntary self-regulation would lead eventually to demands for a similar approach to research ranging from lasers to integrated circuits.

Jim Hudec, NSA legislative counsel, says, "We're still working on the definition [of what aspects of cryptology should be covered] in conjunction with the various groups that participated in the study. There are a great many people who have views on what that definition should be, and I think it will take some time to work that out."

"Apart from that, in effect, the system has started, and it seems to be working well," says Hudec. "I think anyone who has sent a paper in has found we've been very responsive in reviewing the paper and giving them answers." So far, the NSA has not raised objections to any of the papers.

Notice of the formation of a five-person Advisory Committee to oversee the process has appeared in the Federal Register. The President's science adviser has asked the president of the National Academy of Sciences for nominees to fill three of the positions. The NSA director will appoint the other two.

Recently, the National Science Foundation's Mathematical and Computer Sciences Advisory Committee studied the role of the NSF in the funding of cryptology research. Beginning with the premise that protecting information is exceedingly important, the report stated, "It is clear that our government must be able to keep secrets from other governments and that businesses must be able to hide information from foreign and domestic competitors."

However, the advisory committee stated that it does not support the voluntary system of prepublication review proposed by the Study Group and that it did not believe the proposal reflected a consensus within the research community. It also expressed concern that the controversy over cryptology research was "just the tip of the iceberg." There were potential threats to basic research in many other areas.

The advisory committee urged the NSF to "insulate its role as a funding agency for basic research from the problem of trying to protect the interests of the country by restricting either research or the distribution of results."

The NSA has offered to fund certain cryptology research projects that would be expected to be unclassified.

Over the last year, the NSA made two grants, one to a group headed by Hellman at Stanford. Hellman says he accepted the grant to test the system. He chose a topic at the periphery of cryptology, a study of the possibility of solving hard problems more rapidly and cheaply when a cryptanalyst deals with many instances of the same type of complicated problem. Hellman also has NSF support for research in an area closer to the core of cryptology. However, some other scientists are reluctant to take NSA money because they fear their research could be classified. □

SUBSCRIBER SERVICE

Please include a SCIENCE NEWS address label to ensure prompt service whenever you write us about your subscription.

mail to: SCIENCE NEWS, Subscription Office, 231 W. Center St., Marion, Ohio 43305.

change of address: If you're moving please let us know four to six weeks before changing your address.

ATTACH LABEL HERE

to subscribe, mail this form to the address shown above.

subscription rates:

□ 1 year $22.50 □ 2 years $39.00
□ 3 years $55.00
□ Payment enclosed □ Bill me later

name (please print)

address

city state zip code

D421-0B