The New Unbreakable

Will They Put NSA Out of Business?

By Deborah Shapley

Post 7/9/78

IT COULD put the government out of the business of eavesdropping on other nations' messages. It could protect business trade secrets from computer crimes — or guarantee organized crime that its records could never be read by investigators. It could ultimately assure citizens that no government or private agency could tap their phones.

These are a few of the far-reaching consequences which could flow from some new notions about numbers being developed by a group of young university scientists. These mathematicians may be on their way to fulfilling one of man's oldest dreams — break-proof codes — and leaving the world a more private place in the process.

It probably will be 5 to 10 years before these ideas become consumer reality, and the scientists caution that more work is needed to prove out the break-proof codes. Nonetheless, the progress made so far promises to become the basis of an entire new field of "public cryptography," which has excited several major corporations and apparently has put the government's supersecret code agency, the National Security Agency, on edge.

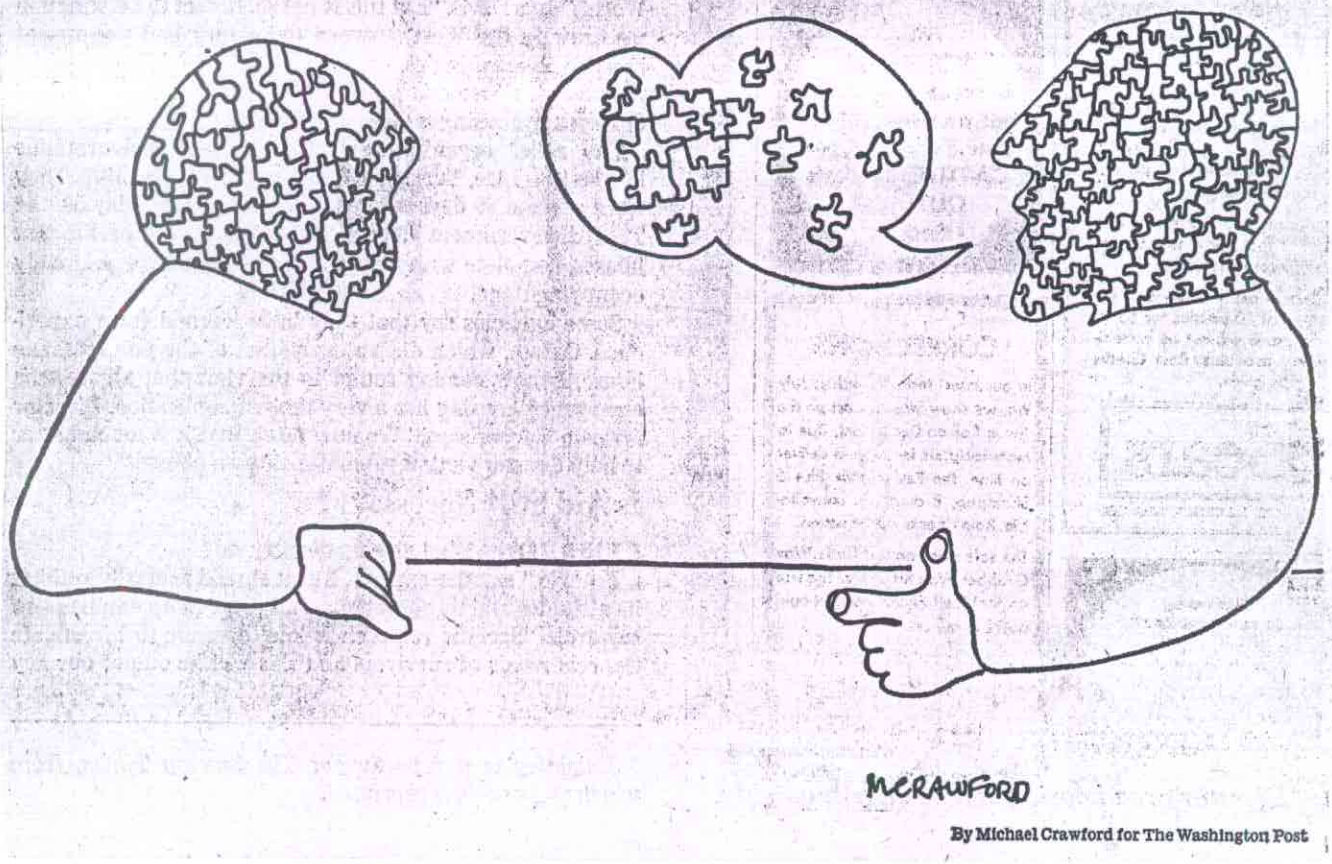
Throughout most of history, codes have been the near-exclusive province of governments and their military and intelligence organizations. In part this is because transmitting coded messages on a large scale has required money and organization, including the ability to run private couriers among the communicators to distribute the code keys.

This is necessary because, in conventional codes, the process of turning letters into numbers is the exact reverse of decoding the message. Experts say that today's encryption is done with a pocket-sized cipher machine, into which the user plugs an IBM card or computer chip that programs the machine to perform the code operations. Since knowledge of the encoding key is tantamount to knowing how to break the code, the security of such codes obviously depends on the security of the keys.

Shapley is a staff writer for Science magazine.

See CODES, Page B3

Codes



By Michael Crawford for The Washington Post

CODES, From Page B1

If a fleet of battleships uses the same code, for instance, the system can be compromised by enemy ransack of a captured ship or rifling through the clothes of a dead sailor washed ashore. And nations have sometimes engaged in chess-like gamesmanship to prevent the other side from knowing its code has been broken. In the North Africa campaign of World War II, for example, when the British captured a houseboat on the Nile that proved to be a German military command station, complete with codebook and radio set, they continued relaying and encoding the Germans' messages to make them think nothing had happened.

But in the new class of "public" codes, the decode key is not the exact reverse of the encode key. Thus the enciphering keys can be widely distributed without fear of compromising the code. This makes possible a wide range of cheaper, large-scale, commercial transactions.

The "Trap Door"

WHY IS THIS possible? Encryption is basically mathematics. To encode a message, letters, punctuation marks and spaces are transformed into numbers by simple substitutions, such as A=01, B=02. Then a mathematical operation turns these into another string of numbers, which is then transmitted — and would appear sheer garble to anyone intercepting the message.

The experts say that in modern military and diplomatic codes, the encoding process is usually some form of algebra: The encoding key turns x into y and the decoding key performs the simple reverse, turning y back into x.

But public key cryptosystems are based on a unique branch of mathematical problems which the availability of high-speed computing equipment is only now making it possible to study. In these problems, while it is easy to turn x into y, it is very difficult to go backwards from y and calculate x. These are called "trap door" problems because only those who know the decoding formula can reverse the original process.

Thus a key that encodes a message, based on the first simple calculation, can be freely distributed without fear that the code will be understood. Only the person with the secret decoding key could ever learn the message's content.

All this was suggested in a paper published in 1975 by two Stanford scientists, Whitfield Diffie and Martin Hellman. Later, a young professor of computer science at MIT, Ronald Rivest, extended these ideas into a specific code scheme, for which he is seeking a patent.

Rivest's scheme, which appears highly secure, is based on the fact that in advanced mathematics, it is easy to find large, 100-digit prime numbers and multiply them together into an even longer, 200-digit numbers. But even with the most advanced computers, it is extremely difficult — knowing only the very long product of two such numbers — to go backwards and find the two prime numbers themselves. According to Rivest, computer trial-and-error attempts to discover the two prime factors of a 200-digit number would require 3.8 billion years of computer time.

Rivest proposed that a public code system could enable an entire network of people to communicate with each other securely. In a network, each user would have a secret decoding key, corresponding to a public encoding key that would be distributed to all the other users and perhaps published in a directory. Each user would have all the others' public keys and therefore be able to send messages to each of them. But only the individual recipient could decipher a message.

Moreover, he suggested a way of double-coding each message so the recipient could be certain who sent it. In this elaboration, the sender would first encode the message with

his unique, secret key, and then code it a second time with the listed public key of the person the message is being sent to.

The recipient would first apply his secret decoding key to the message, and then decode it again with the public key of the person who sent it. The message that pops out then could only have come from the person with the exclusive decode key.

One clear advantage of this "signature" system is that the loss of a single decode key would compromise only one link in the network and not the entire system, as can happen in conventional cryptography.

In a technical memorandum, Rivest also envisioned putting these capabilities into small-scale devices that could be added to data or communications systems. He wrote, "An electronic checking system could be based on a signature system such as the above. It is easy to imagine an encryption device in your home terminal allowing you to sign checks that got sent by electronic mail to the payee . . .

"Another possibility arises if encryption devices can be made fast enough; it will be possible to have a telephone conversation in which every word spoken is signed by the encryption device before transmission," he wrote. In other words, since the telephone system already turns voices into signals, an added device could code and decode these signals at the press of a button, making the conversation secure.

Not only academic scientists feel there will be a need for these new systems. Says Fred Weingarten, a National Science Foundation official who helps fund the scientists, "There is certainly going to be a lot of civilian cryptography. When we start doing our banking electronically and have electronic mail and firms are shipping data over wires. I would think it is going to be routine that all data communication will be encrypted in a few years. It's a natural development of the use of computers."

N. Bruce Hannay, vice president for research and patents of Bell Laboratories, which has pioneered in many other communications revolutions, adds, "People are getting more sophisticated in electronics. Look at today's students, who know all sorts of electronics technology. Out of that population there will be a small but increasing number who will be willing to use that knowledge in ways that are illegal. Companies in the information business, whether computer companies or communications companies like us, are going to have to be concerned about it." Hannay says several of his scientists, too, are doing research on encryption systems.

A Jittery NSA

PERHAPS THE best evidence of the growing interest in public cryptography is the fact that Rivest's technical memorandum describing his scheme has been a sellout: His office estimates that there have been some 7,000 requests for it. Copies were sent on request to oil companies (Exxon, Mobil, Shell, Atlantic Richfield), information companies (Data General Corp., IBM, Bell laboratories), and foreigners (from Norway, Sweden, West Germany, Brazil and some Asian countries). And when Hellman, Rivest and their coworkers gave talks on the new cryptography at a session sponsored by their professional society, the Institute for Electrical and Electronics Engineers at Cornell University, last fall, the jam-packed room included IEEE members from many American firms and from the Soviet Union, Hungary, and Taiwan.

There is little question that all this interest in public key cryptosystems has made the NSA jittery. It is an open question whether this government agency, which is primarily devoted to listening in on the communications and signals — coded and uncoded — of other civilian and military organizations around the world can peacefully coexist with this growing civilian field.

Typical of an agency that does not even list itself in the Pentagon telephone directory, the NSA declines to comment on public cryptography. But an investigator for the Senate Intelligence Committee who has kept track of these developments and who has talked with NSA officials comments, "They recognize the great commercial value of these developments, and they realize they have neither the ability nor the legal authority to police it and stop it. All they would like is some clear authority, so that if something comes out of the universities that really does threaten national security, they could move in on it."

Like other scientific breakthroughs, public key cryptosystems may prove a two-edged sword. While bringing great benefits to some, it could hinder other activities, including U.S. conduct of foreign policy.

NSA clearly is interested in adapting public key cryptosystems for its own uses. Through a Princeton, N.J., subsidiary at the Institute for Defense Analyses, NSA is sponsoring a technical meeting this summer to which mathematicians from around the country have been invited. One purpose of the meeting, according to these scientists, is to see if the Rivest system is as secure as it is said to be.

Besides national security uses, a question has been raised about whether the NSA has a stake in keeping new, civilian codes less than completely secure so that it can break in on encrypted traffic at will. Stanford's Hellman made such a charge last year. When the National Bureau of Standards sought scientific comments on a conventional encryption system developed by IBM for government unclassified and commercial use, the key of "bits" (Os and 1s) had been shortened by half and one mathematical operation in it, called the "S-Box structure," was kept secret

Hellman and others charged that with the shorter key size, advanced computers could crack the code more easily, and that the S-box structure might have been withheld because it contained a shortcut whereby a knowledgable intruder could break in on the code.

The Senate Intelligence Committee, investigating the incident, confirmed that the NSA had persuaded IBM to shorten the key, but it left unanswered why, and whether this was to make the IBM code less secure. The NSA had become involved in the matter because the government was considering certifying the encryption system for some government and commercial use, which it ultimately did. The NBS asked NSA's expert advice, the committee report explained.

Locking the Barn Door

BUT CAN a revolution in cryptography be stopped or classified now that its main features have been published and 7,000 copies of Rivest's memorandum have been mailed around the country and the world?

At one point last fall, an NSA employe named J.A. Meyer tried single-handedly to prevent it from happening. In advance of the Cornell cryptography symposium, Meyer wrote to the symposium's leaders that publication or discussion of cryptography could violate federal export control laws. He identified himself only as a resident of Bethesda, Md., but several publications later confirmed that he was employed by the NSA.

According to Meyer, export laws require that cryptographic devices — as well as advanced computers, some machine tools and other things — must have a government license to be exported. The regulations also require that licenses be obtained for export of "technical data," a term that usually refers to operating instructions for equipment on the export control list. If the scientists' descriptions of the new code schemes could be construed as "technical data" (which Meyer thinks could happen), the scientists, like any other exporter, would have to submit their papers to the State Department before they could publish them or discuss the work in front of foreigners at a meeting.

Meyer's threat sent the scientists scurrying to their lawyers, but did not stop the symposium or the publication of their papers. According to Arthur A. Smith, the MIT general counsel who advised Rivest that he could distribute his memorandum, the export laws are too murky to clearly prohibit scholars from the conduct of their activities.

"We have a duty to publish and protect the faculty's right to do that," Smith says. "If someone can show us that there is a clear violation if the faculty member publishes, then of course we would respect that. But if we have to sift through a lot of unclear regulations, our doubt would be in favor of going ahead and publishing."

NSA's spokesman at the time, Norman Boardman, denied to the press that NSA had any official role in Meyer's letter. This official disavowal seems borne out by events — or the lack of them: The scientists who went ahead with their seminars and publications were not prosecuted or harassed.

Like other scientific breakthroughs, public key cryptosystems may prove a two-edged sword. While bringing great benefits to some, they could hinder other activities, including U.S. conduct of foreign policy.

As Martin Gardner, the mathematics columnist for Scientific American magazine, who in a sense broke the public cryptography story in the August 1977 issue when he described the Diffie-Hellman "trap door" functions and the Rivest scheme, remarked:

"All over the world there are clever men and women, some of them geniuses, who have devoted their lives to the mastery of modern cryptanalysis. Since World War II even those government and military ciphers . . . have become so difficult that the talents of these experts have gradually become less useful. Now these people are standing on trapdoors that are about to spring open and drop them completely from sight."