New Codes Coming into Use

Their unique properties make them ideal for tamper-proof security systems

A few years ago, academic mathematicians and computer scientists began working on a new kind of code that had the potential, they thought, to revolutionize the ancient science of cryptography. Now these codes are beginning to come into practical use and close observers say that this is only the beginning of what will likely be a vast market for them.

The codes were suggested in 1976 by Martin Hellman of Stanford University and Whitfield Diffie of BNR, Inc., in Palo Alto, and they are being developed by numerous researchers. They differ from traditional codes in that knowledge of how to encode does not necessarily reveal how to decode. It is this difference that is being exploited.

In all coding systems, encryption and decryption are reverse mathematical procedures. In traditional systems, it is simple to calculate how to decode once you know how to encode and vice versa. The new systems, however, are based on mathematical procedures that are easy to compute but nearly impossible to reverse, unless you have some secret information about how the particular code was constructed. A user could designate the easily computed procedure as his encryption "key" and could make that key public. But he could keep secret the information on how to reverse the procedure, and thus only he would know the decryption key. In that way, anyone could send him a message, but only he could decode messages addressed to him. Alternatively, the encryption key would be kept secret and the decryption key made public.

One of the first places the codes are being applied is at the Zero Power Plutonium Reactor in Idaho Falls, Idaho, a research facility used to study designs of reactor cores. In experiments on the nuclear physics of the cores, fissionable materials are brought almost to the critical point. Because the nuclear fuels include uranium and plutonium, it is important that only authorized persons be allowed in the facility. Ordinarily in such cases, guards identify those who seek admission. But this is not an ideal system—guards can be bribed or can be inattentive.

Robert Lederer of Sandia Laboratories in Albuquerque recently made use of the new codes to design an automated system for controlling access to the Idaho Falls facility. Each person who is authorized to enter is given a magnetic card containing encoded information on the dimensions of his hand. The person provides a password and his identification number to a computer. Then he inserts his magnetic card in the computer and puts his hand in a device that measures it. If his hand dimensions match those encoded on the card, he is allowed entry.

According to Gustavus J. Simmons of Sandia Laboratories, this access device is secure because the new codes are used to encrypt information on the magnetic cards. The people who work at the facility could obtain the decoding instructions, since the computer that reads these instructions is not secure. With a traditional code, where encoding instructions are easy to deduce from decoding instructions, it would then be possible to forge magnetic cards containing properly encoded dimensions of the hands of unauthorized persons. But with the new codes this is impossible.

Paul Amundson of the Zero Power Plutonium Reactor says the hand-reading system has been in operation for several months and is working well. His facility is testing the device for the Department of Energy (DOE), which may put it in widespread use.

The codes also may be useful in keeping track of nuclear fuel—ensuring that it is not enriched into weapons-grade material and that stored fuel is not stolen. The enrichment application is particularly promising because thus far there has been no effective way to make sure that countries do not turn their fuel enrichment plants into plants for making fissionable products for bombs.

A system to keep tract of enrichment will be tested in June at a uranium enrichment plant in Oak Ridge. A monitor, developed by Lederer, will read gamma radiation emitted from the fuel and will convert the amount of radiation to the degree of enrichment of the fuel. Reactor-grade fuel is enriched 3 or 4 percent; weapons-grade fuel is enriched 20 to 90 percent. The enrichment information will be automatically encoded with one of the new codes. Anyone can decode the information, since the decoding instructions will be made public, but no one can forge information because the encoding instructions will remain sealed in a container with the radiation monitor.

After the demonstration project at Oak Ridge, the enrichment monitoring system may be used at a plant under construction at Portsmith, Ohio. The plan is for this facility to be used to set an international precedent for keeping tabs on fuel enrichment.

The codes also are being considered by DOE to encrypt information necessary for remote monitoring of spent nuclear fuel. This monitoring is a concern of the International Atomic Energy Agency (IAEA), which verifies that spent fuel is not diverted to other uses. According to Thomas Sellers of Sandia Laboratories, it is relatively easy to keep track of these fuels. For example, cameras can be trained on the fuel, or fiber optic seals can be placed on it so that to move the fuel one would have to break the seal. The problem, however, is to be sure that no false information is transmitted about fuel movements.

One way around this problem is to use the new codes to encrypt information about fuel movements and to make the decryption key public. In that way the host country and the IAEA could easily decrypt the signals but no one could forge information.

The Mitre Corporation in Bedford, Massachusetts, and the Digital Communications Corporation in Gaithersburg, Maryland, are testing systems using the new codes to protect the privacy of electronic mail. Theoretically, the codes would be perfect for the application. The user could make public his encryption key so that anyone could send him a coded message, but keep secret his decryption key so that only he could decode his mail. But it takes too long to en-

0036-8075/80/0516-0694$00.50/0

crypt and decrypt with the new codes for this sort of application to be practical. In electronic mail, long messages must be very rapidly transmitted. Brian Schanning of Mitre and Thomas McPherson of Digital Communications, however, explain that their firms are experimenting with a hybrid system that incorporates the best features of a new and more traditional code.

The more traditional code being used is the Data Encryption Standard (DES), a sophisticated system developed by the National Bureau of Standards. Although encryption is fast with the DES, the problem with using the DES alone for electronic mail is that each recipient of a message must be sent a decoding key in advance. The key must be sent through secure channels such as registered mail or a private courier. The sending of the key, then, can be cumbersome, time-consuming, and infeasible for any large-scale mail system.

At Mitre and at Digital Communications, the idea has been to encode DES keys with one of the new codes and then transmit the keys electronically. A user could make public his encryption key but keep his decryption key secret. Then anyone could send him an encoded DES key in advance of a DES-encoded message but only he could decrypt the key and thus the message.

The relatively low speed of encryption with the new codes is a consequence in part of their very novelty. At present, computers, such as microprocessors, must be used to encrypt, rather than special-purpose microelectronic chips, which would be much faster. Ronald Rivest of the Massachusetts Institute of Technology explains that, with a microprocessor, only a few hundred bits of information per second can be encrypted. The DES, which is available commercially as a single chip, can encrypt more than 10^6 bits per second. Rivest and his associates are now putting a new code that they designed on a single chip. A prototype of the chip should be available in June or July, Rivest says, and it should encode more than 10^3 bits per second. And it should be possible to make chips that encode 10^4 bits per second. Rivest speculates that when the new codes are available on single chips, they will be much more widely implemented. Quite a few companies have been asking him when the chips will be available.

Simmons points out, however, that there is another reason people have been slow to use the new codes. They are waiting for some sort of seal of approval from the National Security Agency (NSA), which has already certified that the DES is secure.

The American National Standards Committee has convened a subcommittee to try to decide on a secure version of one of the new codes. This version would then be submitted to the NSA so that it could be officially deemed "not insecure."

For now, implementation of the new codes is still proceeding slowly. But in the future, Amundson predicts, "The applications will only be limited by the needs of the users."

—GINA BARI KOLATA

Quake Prediction by Animals Gaining Respect

The popular idea that animals can sense coming earthquakes is getting a boost from some of the first U.S. studies

> Some instances noted at this time [before the earthquake] were of snakes being found frozen on the road, . . . geese flying, chickens refusing to enter their coop, pigs rooting at their fence, cows breaking their halters and escaping, and goats as well as cows being unusually restless. Rats appeared to behave as though drunk. Three well-trained police dogs howled, refused to obey commands, and kept their noses close to the ground as though sniffing.—HAICHENG EARTHQUAKE STUDY DELEGATION*

Although rarely more than anecdotes, the sheer volume of reports of unusual animal behavior preceding Chinese earthquakes has had a considerable impact in the United States. Reports in the daily press of apparently anomalous animal behavior before an earthquake can upstage the earthquake itself. Even the highly skeptical U.S. scientific community has had to concede that there might be something to it after all. Now, preliminary results from modest U.S. studies suggest that some animals may indeed sense phenomena related to a coming earthquake, but only sometimes. In many cases, it appears that the connection between unusual animal behavior and the subsequent earthquake is only in the mind of the human observer. Unlike Chinese specialists, American researchers are anxious to identify any geophysical link between earthquakes and animals, an interesting prospect being low-frequency sound generated by foreshocks too small to be recognized by standard seismic networks.

Disappointingly, the highly publicized accounts of strange animal behavior, such as those reported from Marine World/Africa USA after the Coyote Lake, California, quake of last summer, have added little acceptable support for the hypothesis that animals can predict earthquakes. "If it's true, it doesn't smack you in the face," says Leon Otis of SRI International in Menlo Park. Otis and William Kautz of SRI run a network of observers that includes people who work in the animal park. The network's 1200 volunteer observers, who are spread over several earthquake-prone areas of California, are instructed to report immediately on a toll-free line any unusual animal behavior.

The trouble, Otis explains, was that most people called after rather than before the magnitude 5.7 Coyote Lake earthquake (*Science*, 2 November 1979, p. 542), which fell on the fringe of the network and 70 kilometers from Marine World/Africa USA. There was no significant increase in calls before the quake, but "as soon as it happened, we got a whole flock of calls," Otis recalls. Most were what the researchers term "I goofed" calls—the observer immediately apologizes for not reporting it when it happened, but their dog or horse or cat certainly was acting strangely soon before the earthquake. Such calls, even those reporting numerous cases of unusual behavior as at Marine World/Africa USA, are dropped from consideration in the study as invalid. The problem may simply be one of training, Otis says, or perhaps people tend to attach special significance to unusual behavior that coincidentally preceeds an earthquake.

*C. B. Raleigh *et al.*, *Eos* **58** (No. 5), 236 (1977).

0036-8075/80/0516-0695$00.50/0