Cryptology: A Secret Meeting at IDA?

Many mathematicians and computer scientists believe that a meeting sponsored by the Communications Research Division (CRD) of the Institutes for Defense Analyses (IDA) in Princeton, New Jersey, will focus on studies of the security of a new class of encrypting schemes. These schemes are of more than casual interest since they may be used to solve a sticky problem in enforcing the Comprehensive Nuclear Test Ban Treaty. IDA vigorously denies that it will be studying the schemes, saying that the purpose of the meeting, to be held this summer, is to develop software for their new Cray I computer. Those who believe the meeting is for code-breaking say IDA cannot be completely frank about the purpose of its meeting because its work is highly classified. CRD is said to be funded by and to serve as an analytical arm of the National Security Agency (NSA).

The new encryption schemes were devised last year by mathematicians and computer scientists working independently of NSA and other government establishments (*Science*, 19 August 1977, p. 747). In order to break these codes, it may be necessary to use methods that can require years, or even decades, of computer time—thus making the codes, for all practical purposes, unbreakable. It has not been shown, however, that no shortcuts to breaking the codes exist, so their security is still in question.

IDA is said to be particularly interested in a code devised by Ronald Rivest, Adi Shamir, and Len Adleman of the Massachusetts Institute of Technology and often referred to as "the Rivest scheme." The only known way to break this code is to factor very large numbers into primes. Most mathematicians believe that any algorithm would require an unacceptably long time to factor large numbers. Rivest says that even with the Cray I—the world's fastest computer—it could take 9 months to factor a 100 digit number. It could take 100 years on a slower computer.

As to whether the word about this summer's meeting is true, at least one mathematician states unequivocally that it is. This mathematician, who declined to be named, is a frequent NSA consultant. He told *Science* that several people he knows well were asked to suggest names of researchers to invite to the meeting who would be able to investigate the security of the Rivest scheme. "It is definitely not a general software meeting," he says.

Those invited to the meeting seem particularly qualified to study the Rivest scheme. For example, mathematicians who specialize in finding factoring shortcuts and those who specialize in coding theory have been invited. One factoring expert says, "The fact that I was invited is a strong presumption that the meeting is being held to break the Rivest scheme." He reports that the IDA officials who contacted him were cagey about whether the meeting would involve the Rivest scheme. They told him that if he wants to know, he should attend the meeting and find out.

Inviting factoring and coding experts to the meeting does not necessarily contradict IDA's assertion that the meeting is being held to develop Cray I software. Both factoring and coding experts tend to make extensive use of computers, and both could develop software. Lee Neuwirth, who is head of CRD, says that specialists in areas other than factoring and coding theory are coming to the meeting, but that he is not at liberty to divulge their names or areas of specialization.

One coding specialist, who plans to attend the meeting and who frequently serves as a consultant for IDA and NSA, pooh-poohs the notion that the Rivest scheme will be studied and says that people greatly overestimate the government's interest in the new coding systems. But Gustavus J. Simmons, who is manager of the applied mathematics department at Sandia Laboratories, tells a somewhat different story.

Simmons has spent a great deal of time investigating the Rivest scheme and readily admits that his interest is not purely academic and that the United States is very interested in using the new schemes—if they could be shown to be secure.

Simmons describes two proposed uses for the new coding schemes. One is to provide secure communications for the command and control of nuclear weapons. The other is to solve a major problem that arose in connection with the Comprehensive Nuclear Test Ban Treaty. It is in the latter application that the true potential of the new systems comes into play.

In accordance with the Comprehensive Nuclear Test Ban Treaty, the United States will place seismic devices in the Soviet Union in order to detect underground nuclear explosions. These seismic devices will be sealed in tamperproof boxes and placed at unattended monitoring stations. The United States wants to ensure that the Soviets do not alter the seismic data, substituting innocuous for incriminating data after they have been transmitted from the boxes. One way to prevent this occurrence is to encode all the data before transmission. The Soviets object to this solution, however, because they fear the United States could then transmit unauthorized information as well as seismic data from the monitoring stations.

The compromise worked out so far is for the United States to encode a small amount of seismic data and transmit it along with unencoded seismic data. The coded data would serve as a "fingerprint." If the Soviets substitute false data, the fingerprint would be altered. Every 30 days, the United States would give the Soviets the key for decoding the previous month's fingerprints. Neither side is completely satisfied with this compromise. The United States fears it will be rapidly educating the Soviets in how its crypotographic systems work. The Soviets fear the United States might transmit unauthorized information, disguised as fingerprints, for the 30 days before the code-breaking information is supplied.

An ideal way to satisfy both the United States and the Soviets is to use the new coding schemes. These schemes have the property that knowledge of how to decode a message does not give away the procedure for encoding. Thus, the United States could encode the seismic data before they are transmitted. The Soviets could decode the data to satisfy themselves that only seismic data were being sent out. But the Soviets could not substitute false data unless they could break the coding scheme.

The IDA, then, has reason for wanting to study the Rivest scheme, and it seems to have invited to its meeting appropriate people for studying it. All of its operations, however, are surrounded by secrecy; it eschews publicity and is clearly attempting to keep the contents of its meeting known only to the participants.—GINA BARI KOLATA

0036-8075/78/0414-0184$00.50/0