Cryptography: On the Brink of a Revolution?

Computers are increasingly a central part of cheap and efficient communication systems, but a number of experts warn that computer-controlled communications networks are coming into use before problems of ensuring privacy and security have been solved. This issue is coming to the fore as these communications networks play an ever larger role in technological societies.

One way to provide security is to encode computer messages. New developments in cryptography promise to change the age-old methodology of secret coding by the seemingly contradictory proposal to keep codes secret by making them public. This proposal may be arriving just in time to overcome the massive logistical problems that exchanging codes will pose if computerization of communications continues as expected.

Many technological systems already involve computers that "talk" to each other. For example, electric power companies often use computer messages to control their systems. Floodgates at major dams are controlled by computer messages. Airlines use computer networks to make passenger reservations. Many long-distance telephone calls are transmitted in digital form—for example, strings of 0's and 1's. Electronic fund-transfer systems are becoming commonplace in the banking industry, and electronic mail systems are now being tested by some businesses and corporations. Electronic mail is also being tested in a town outside Tokyo, where 3000 households are sending and receiving messages by means of a closed-circuit television system.

This growing use of computers in communication networks gives rise to a number of questions. How can a bank be assured that a computerized request to transfer funds to a particular account is legitimate? How can terrorists be prevented from tapping into computer lines used by a power system and inserting messages that cause blackouts? How can two people at different branches of a corporation who communicate by means of electronic mail be sure that a competitor does not tap their lines and intercept their messages?

Some of these problems can be solved if sensitive or private computer data is cast in secret codes to be deciphered only by authorized persons. But current cryptographic systems do not allow for authentication of computer messages (so-called digital signatures) and are not easily used in large communications networks of the kind now under development.

Current cryptographic devices make use of special-purpose computers to encode and decode messages. A message, which may consist of an English sentence, a chart, a phone conversation, or even a picture, is represented in a computer as a set of numbers. The special-purpose computer encodes a message by transforming it into a different set of numbers. The rules that determine how the numbers are to be transformed constitute the coding scheme. These rules are generally members of a collection of nonlinear mathematical functions. The computer decrypts a message by reversing the encryption procedure—that is, by acting on the coded message with the mathematical inverses of the encryption functions.

Each group of users of a particular encryption procedure has its own coding function. With the encryption schemes currently available, knowledge of the coding function allows a person to encode computer messages and to decode them as well, but even a person who designed the scheme cannot decipher a group of users' messages without knowing their coding function.

A Problem with Current Systems

One problem with these cryptographic systems is that a key, or information specifying the coding function, must be sent out to all users before messages can be exchanged. The military often uses private couriers for this purpose. But sending a key involves a time delay that may not always be practical and raises the possibility that the key may fall into unauthorized hands. Sending keys may be completely infeasible in large communications networks, such as those being envisioned for electronic mail.

Recently, Whitfield Diffie and Martin Hellman of Stanford University devised an ingenious way to send and receive messages without the need for secret coding functions. Their solution also leads to a way to generate digital signatures. Already, patent applications have been filed for cryptographic devices based on these new ideas and a number of large corporations are interested.

The Stanford investigators' solution is to make use of enciphering functions whose inverses, which are used for deciphering, are impossible to deduce, but which are known to the users of a particular system. (In current schemes, deciphering functions are easily determined from knowledge of enciphering functions.) Each user places its enciphering key in a public file and keeps its deciphering key secret. It is then easy to send a coded message to a particular recipient by using the recipient's public enciphering key, but only the intended recipient can decode the message. Hellman and Diffie call their new schemes public key cryptosystems.

In the future, they believe, businessmen may make use of public key cryptosystems to exchange messages by electronic mail. A businessman in Atlanta, say, would sit at his computer terminal and call an information number to obtain the public encryption key of another businessman in New York. Then he would type a letter on his computer terminal. As he typed it, the computer would automatically encode it with the New York businessman's coding function. The encoded message would be transmitted to the man in New York, whose computer would automatically decode it. Only the New Yorker could decipher the message since only his computer would contain his secret decoding key.

The man in Atlanta could also use his computer to "sign" an order for goods that he wishes to buy from the man in New York. He first types the order for the goods into his computer and instructs the computer to encode the message with his secret deciphering key. This is his "signature." (A deciphering key, like an enciphering key, is a rule for transforming computer messages. Thus it may be used to encode as well as decode.) He then has the computer act on the message a second time, encoding it with the New York man's public enciphering key. This double-coded message is sent to New York.

The New York businessman uses his secret deciphering key to reverse the second coding of the message. He then uses the Atlanta man's public enciphering key to reverse the first coding and extract the original message. This procedure works because encoding and decoding rules can be applied in either forward or reverse order. The message must have been "signed" by the Atlanta businessman since only he knows his secret deciphering key. Only the New York man could understand the message since the New York man's deciphering key is known only to him.

Development of public key cryptosystems was previously impeded because investigators found it impossible to de-

rive suitable coding functions that could not be inverted. The success of the newly proposed system depends on specially developed mathematical functions known as "trapdoor one-way functions." These are functions that are easy to compute but whose inverses are impossible to derive from descriptions of the functions unless some special information is known about how the functions were constructed. (The special information is the "trapdoor.") The idea is for a user to construct such a one-way function and, in so doing, also construct the function's inverse. Although the function would be made public, no one who sees only the function would be able to construct its inverse.

Ronald Rivest, Adi Shamir, and Len Adleman of the Massachusetts Institute of Technology and, independently, Michael Rabin, of the Hebrew University in Jerusalem, recently developed a class of one-way functions that could serve as the basis of a public key cryptosystem. According to Rivest, the MIT group is now planning to implement their scheme on special-purpose integrated-circuit chips and to make it commercially available.

The researchers made use of well-known results in number theory to design their one-way functions. A person, A, employing this system would publish two numbers, r and s, as his key. Anyone wishing to send A an encoded message would raise the numbers that constitute the message to the sth power, divide that number by r, and determine the remainder. The remainder is the coded message. To decode the message, A would make use of a number t, whose identity would be kept secret. Recipient A would raise the encoded message to the tth power, divide it by r, and determine the remainder, which would be the decoded message.

This encoding and decoding scheme hinges on the relations between r, s, and t. The number r is the product of two very large prime numbers, and r is constructed by finding two large primes and multiplying them together. The numbers s and t are also constructed from these two large primes, and t can be determined only if the identities of the large primes are known.

To break this code, it is necessary to find t. But no way is known to find t without first factoring r into its constituent primes. This task is not easily accomplished. For example, the MIT investigators estimate that it is technically impossible to factor a 125-digit number into primes, even if the fastest computers and the most efficient factoring algorithms are used. They quote other experts on the subject who say, "In general, nothing but frustration can be expected to come from an attack on a number of 50 or more digits, even with the speeds available with modern computers."

Although it is computationally infeasible to factor a very large number into primes, it is entirely feasible to find very large primes with a computer. A number of efficient algorithms to do so have recently been developed, including a probabilistic one devised by Rabin, which is based on the same number theory results as the encryption scheme of Rabin and the MIT investigators (*Science*, 4 June 1976, p. 989). Because of this, Rivest says it should be possible to use a computer chip incorporating the encryption and decryption algorithms to find large primes. This may make the system easier to implement since only one chip may be necessary to encode, decode, find an encoding key (r and s) and its corresponding decoding key (t). Security should also be tighter since the code would be generated in the same computer that uses it. Thus the secret deciphering function need never be taken out of the computer.

An Alternative Solution

An alternative group of one-way functions is proposed by Ralph Merkle of Stanford University and Hellman. Their cryptographic scheme is based on the fact that it is easy to select arbitrarily and to add up a subset of numbers from a large collection of numbers. But it is very difficult to reverse this procedure—that is, to decide which subset of the collection adds up to a particular sum.

In Merkle and Hellman's scheme, a user's public encryption key is a large collection of numbers, chosen in a specific way, which is being kept secret as part of their patent application. (The particular way in which it is chosen provides a "trapdoor.") A person sends a message by adding up a particular subset of those numbers and transmitting the sum. Because the recipient has knowledge of the trapdoor, he can easily decide which subset of numbers was added up and can extract the original message from the enciphered one. According to Merkle and Hellman, an eavesdropper would essentially have to try out all possible ways to add up subsets of the large collection of numbers to find a subset that adds up to a particular sum. This task is computationally infeasible for large collections of numbers. For example, Ronald Graham of Bell Laboratories in Murray Hill, New Jersey, says that all the computing power in the world would not suffice to find which subset of 200 randomly chosen 20 digit numbers adds up to a particular 22 digit number.

Merkle and Hellman's encryption scheme is based on a problem, known as the knapsack problem, whose solution becomes computationally infeasible as the problem grows in size. The knapsack problem is one of a class of problems known as NP-complete (*Science*, 8 November 1974, p. 520). These problems are equivalent in that, if an efficient way to solve one were found, all could be solved efficiently. But computer scientists strongly suspect that there is no easy way to solve any of these problems. General solutions to NP-complete problems involve trying out all possible solutions until the correct one is hit upon.

Although computer scientists have been continually frustrated in their search for efficient solutions to NP-complete problems, this failure may be an asset to cryptographers. Hellman, for one, believes that the NP-complete problems may provide a rich lode of one-way functions. The functions would be designed in such a way that it would be necessary to solve an NP-complete problem to discover the inverse of an encryption algorithm. In addition, NP-complete problems could serve as the basis of provably "unbreakable" public key cryptosystems.

The development of provably unbreakable systems would represent a new milestone in cryptography. Before this century, cryptographers "proved" their systems were unbreakable by enumerating all the steps necessary to break them. But clever spies would continually find ways to circumvent most of those steps. During this century, systems have been tested by assigning cryptanalysts the task of breaking them. If the cryptanalysts failed, the systems were said to be secure. The use of NP-complete problems or other provably hard mathematical problems to design cryptographic systems, however, will result in systems whose security does not depend on this sort of experimental certification.

Although public key cryptosystems and digital signatures are not yet in use, a need for them has arisen, and, many believe, current designs for them are feasible. As societies begin to rely on computer-controlled communication networks, cryptography becomes essential to ensure privacy. Cryptography has left the exclusive domain of the military and the National Security Agency and, in the eyes of Hellman and Diffie, now stands "on the brink of a revolution."

—GINA BARI KOLATA