

Alice and Bob, who live in New York and Los Angeles, respectively, want to decide in which city to meet. They agree to toss a coin, but they can communicate only by telephone. Somehow, they must find a way of tossing the coin without suspecting each other of cheating.

Manuel Blum of the University of California at Berkeley says he has a solution not only to the dilemma facing Alice and Bob, but also to potential problems of cheating in the high-technology world of telephone-linked computers. Blum, a computer scientist, works on "transaction protection protocols," methods of exchanging secrets or signing contracts using telephone-linked computers. The basis of his schemes is a mathematical equivalent of tossing a coin that Blum says eliminates practically all possibilities of lying or cheating to gain an advantage over a rival.

The coin-toss algorithm is an ingenious blend of the capabilities of modern, high-speed computers and ancient Euclidean mathematics. It is based on an algorithm invented recently by Michael O. Rabin of Harvard University's computer science department. Rabin's algorithm, which he named the "oblivious transfer," provides a powerful solution for protecting both parties' interests in telephone transactions.

What excites computer scientists is the possibility that they can adapt the oblivious transfer method to ensure the fairness of a variety of business transactions. "This is not a question of secrecy of messages," says Rabin. "What people are seeking is protection from each other." Rabin and Blum look for methods or protocols that ensure people behave as they promise.

The oblivious transfer depends on two important principles. First, computer scientists have shown that it is possible to determine quickly whether a 60-digit number is a prime number; that is, divisible only by the number one and itself. A programed personal home computer can do this in about half a minute.

Second, computer scientists believe that it is almost impossible to factor a 120-digit or larger number. This has not been proved, but mathematicians have strong evidence that supports this idea, and Rabin says, "The security of a system is provably equivalent to the difficulty of factorization."

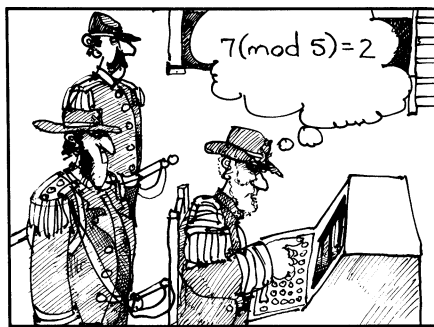
As in many computer security and encryption systems, modular arithmetic plays an important role. Given two integers, a and n , the remainder of a divided by n is $a(\text{mod } n)$. For example, $7(\text{mod } 5)$ is 2; $13(\text{mod } 5)$ is 3. In this system of arithmetic, a negative number, $-a$, is treated in the same way as $(n-a)(\text{mod } n)$. Thus, $-2(\text{mod } 5)$ is the same as $(5-2)(\text{mod } 5)$ or $3(\text{mod } 5)$. The answer is 3.

Here's how the oblivious transfer would work in the case of a coin toss.

WHOM DO YOU TRUST?

Computer scientists are applying ingenious mathematical methods to keep computer users from cheating each other

BY IVARS PETERSON



Alice and Bob use their linked personal computers to perform the coin toss. Normally, the computers would deal with 60- and 120-digit numbers and go through the procedure in less time than it takes someone to read this example. However, to make the example easier to follow, Alice selects much smaller numbers than those a computer would handle.

Alice, in New York, starts the coin toss by selecting two prime numbers, 7 and 13. She multiplies the numbers together and sends the product, 91, to Bob. She keeps the numbers 7 and 13 secret. Bob wins the toss if he can factor 91; that is, find 7 and 13.

Suppose that Bob, in Los Angeles, cannot factor 91. First, he can check whether Alice is cheating. For example, she could have sent a number that can't be factored. The number shouldn't be even, and Bob's computer has efficient tests to show whether the number is a prime or a power of a prime.

Once he finishes checking, Bob randomly selects an integer, say 11, between 1 and 91. The integer may, by chance, turn out to be a factor of 91, and therefore he wins the toss immediately. However, the chances of this happening with a 120-digit number are incredibly small.

Bob squares 11 to get 121, then divides by 91 and finds that the remainder from the division is 30. He sends this remainder to Alice. He keeps the number 11 secret.

Alice looks for numbers that will give a remainder of 30. In this case, she can do it

by trial and error, but there are other methods available. She finds two pairs: ± 11 and ± 24 . She can send either 11 or 24 to Bob. One of the numbers is Bob's number, but Alice does not know which one of the two is his.

If Bob receives 11 from Alice, he has no new information and loses the toss because he can't factor 91. If he receives 24, then he adds his own number, 11, to 24 and gets 35. The lowest common divisor of 35 and 91 is 7. This will automatically be a factor of 91, according to a Euclidean algorithm, and Bob wins the toss.

Blum particularly delights in this last step because it utilizes what he says is "the first algorithm in all history."

Rabin originally developed the oblivious transfer in April in answer to a problem suggested by Richard A. DeMillo of the Georgia Institute of Technology. Is it possible for two people to exchange secrets without the help of a trusted third party? This looks impossible because if one person reveals his secret first, then the other person can refuse to divulge his secret in return. However, Rabin solved the problem in a few days, in the process applying randomization algorithms he developed six years earlier and inventing the oblivious transfer. He was able to make the probability of cheating as small as he wished.

Rabin was intrigued by the result. "What is provably impossible by classical methods becomes practically possible through randomization," he says.

In July, Rabin visited Berkeley and heard that Blum and a student, Sylvia Micali, were working on the coin-toss problem and had come up with a complicated solution. Rabin saw within minutes that his oblivious transfer method provided a better, simple and strong solution for the coin-toss problem. Soon after, Blum applied the oblivious transfer to create a protocol for certified mail (mail sent in exchange for a receipt) that could be used with computers and reduced the chances of cheating considerably.

One complaint of some businessmen who use certified mail is that although they get a record that the message has been received, they do not get confirmation of the content of the message. This allows the possibility of deliberate or accidental misunderstanding of the intent of the message.

Blum developed a protocol that he thinks allows certified mail, such as contracts, to be sent directly from one computer to another without the need of an intermediary. In his system, the sender automatically gets a receipt that also confirms the nature of the message.

Blum's certified mail protocol uses the oblivious transfer in the same way it was used in the coin-toss example. The difference is that the sender, Alice, encodes her message as a string of digits in 10 numbers

Just Released!
Contains everything
needed including
ready-to-use
forms.

**HOW TO
INCORPORATE
IN TAX FREE
NEVADA
FOR ONLY \$50**
by
John L. Hayden

**Highlights of this revealing
book include how to . . .**

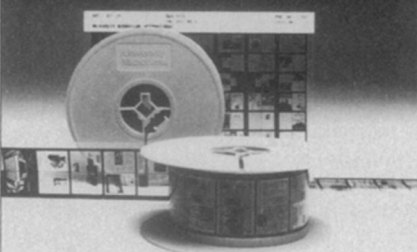
- Incorporate without a lawyer
- Gain more privacy and benefits than Delaware corporations
- Pay no state income tax, less federal tax
- Be a one-man corporation
- Incorporate within 48 hours
- Start with zero capital
- Limit personal liability
- Eliminate franchise tax
- Transfer stock freely
- Raise capital by selling shares of stock

SATISFACTION GUARANTEED

To: **Newport Marketing Corp.**
P.O. Box 8320, Newport Beach, CA 92660
Please send _____ copies at \$14.95 each.
 Payment of \$ _____ enclosed. We pay P&H.
 Please send more free information.
California residents add 6% sales tax.

Name _____
Address _____
City _____ State _____ Zip _____ SN-8

This publication
is available
in microform.



**University Microfilms
International**

300 North Zeeb Road
Dept. P.R.
Ann Arbor, Mi. 48106
U.S.A.

30-32 Mortimer Street
Dept. P.R.
London W1N 7RA
England

. . . Whom Do You Trust?

she sends to Bob for factoring. The numbers are constructed so that Bob must factor all ten in order to find the message.

As in the coin-toss example, Bob picks a number at random and runs through the oblivious transfer. Depending on Alice's response, he may or may not be able to factor the first number. Then he goes on to the second number, runs through the algorithm, and so on until he has tried all ten. After completing this first stage, Bob is likely to be able to factor some, but probably not all, of the numbers. Bob then repeats the procedure, again running through all of Alice's numbers in the same order as before but with new random numbers. He continues through these stages until he has enough information to find the factors of all 10 numbers. On the average, this takes three or four stages of running through all 10 numbers that Alice sent.

Eventually, Bob has the information to find and decode Alice's message, and Alice has a record of Bob's efforts. The collection of Bob's requests constitutes her receipt. If there were a dispute over the receipt of the message, a judge could determine from the record of the transaction that Alice provided enough information for Bob to factor the numbers, and that Bob must have received the message she sent.

This method, with some modifications and additional safeguards, can also ensure contracts are signed simultaneously in different parts of the world. Traditionally, businessmen or diplomats have gathered in one place to sign a document according to a prescribed ritual so that no person gains an advantage over anyone else. If the parties to a contract are in different locations, then, without a protocol, one party can delay signing a contract and possibly gain an advantage.

Blum suggests this problem can be avoided if participants use a form of computer certified mail, but in a two-way rather than a one-way sense. The contract would include a clause that states that the contract is valid only if both participants have both contract copies and receipts. Each of the parties sends a contract and receives a receipt, which can be interpreted as a signature. Only if the transaction is completed by both sides will the contract be valid.

So far, the oblivious transfer algorithm, together with randomization techniques to reduce the probability of cheating, has proved applicable to a variety of human problems associated with using computers. Rabin does not expect his results to be applied extensively until electronic mail becomes more common and businesses begin to conduct more transactions through computers rather than with paper and ink. However, within a decade, he predicts, the ideas he, Blum and others are working on will be important to many people. □

BOOKS

BOOKS is an editorial service for readers' information. To order any book listed or any U.S. book in print please remit retail price, plus 50¢ handling charge for each book to **Book Order Service**, Science News, 1719 N Street, N.W., Washington, D.C. 20036. All books sent postpaid. Domestic orders only.

A COMPLETE MANUAL OF AMATEUR ASTRONOMY: Tools and Techniques for Astronomical Observations—P. Clay Sherrod with Thomas L. Koed, foreword by Leif Robinson. By many it is assumed that the era of amateur contributions to astronomy is over. The foreword states, "This is far from the truth," as recent work by amateur astronomers has shown. This book presents many of the research projects suitable and useful to the nonprofessional astronomer. P-H, 1981, 319 p., illus., \$24.95.

GENESIS AND DEVELOPMENT OF A SCIENTIFIC FACT—Ludwik Fleck, edited by Thaddeus J. Trenn and Robert K. Merton, translated by Fred Bradley and Thaddeus J. Trenn, foreword by Thomas S. Kuhn. The author has selected an established medical fact—that the so-called Wassermann reaction is related to syphilis—and then asks the question: How, then, did this empirical fact originate and of what does it consist? Originally published in hardback in 1979. U of Chicago Pr, 1981, 203 p., illus., paper \$6.95.

SCIENCE ANXIETY: Fear of Science and How to Overcome It—Jeffrey V. Mallow, foreword by Sheila Tobias. In our technological, complex society science avoidance is disastrous both for those individuals attempting to move ahead vocationally and for those who need to have an understanding of science in order to make policy. This book outlines the steps that parents, teachers, victims and psychologists can use in dealing with science anxiety. Thomond Pr (Van Nos Reinhold), 1981, 232 p., illus., \$9.95.

SHALLOW WATERS: A Year on Cape Cod's Pleasant Bay—William Sargent. An account of the seasons' changes in the estuarine world of Cape Cod's Pleasant Bay through the trained eye of a naturalist. Beautiful photographs enhance the text. HM, 1981, 138 p., color/b&w illus., \$17.95.

A SIERRA CLUB NATURALIST'S GUIDE TO THE NORTH WOODS: Of Michigan, Wisconsin, and Minnesota—Glenda Daniel and Jerry Sullivan. The North Woods, a transitional zone where northern boreal forests of evergreen conifers mingle with eastern deciduous growth, contains natural communities unlike those found anywhere else in the country. This field guide describes the North Woods region from the underlying soils and rocks to the plants and wildlife they sustain. Sierra (Scribner), 1981, 408 p., illus., \$24.95, paper, \$10.95.

THESE ARE THE ENDANGERED—Charles Cadieux. Shows why various species have been so greatly reduced in numbers, gives their potential for recovery and tells what steps are being taken to assist the battle for survival. Stone Wall Pr (Greene), 1981, 221 p., illus., \$15.

WHALES—W. Nigel Bonner. Describes the natural history of whales, dolphins and porpoises. Focuses on the basic facts and theories of those features of whales that distinguish them from the rest of the mammals and fit them for life in the sea. Discusses the history of man's relationship with the whale. Blandford (Sterling), 1980, 278 p., color/b&w illus., \$24.95.

WIND-CATCHERS: American Windmills of Yesterday and Tomorrow—Volta Torrey. The history of the use of wind power and its prospects for the future. Originally published in hardback in 1976. Greene, 1981, 226 p., illus., paper, \$9.95.