



## ... 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

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 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 — Jeffry 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.

206

SCIENCE NEWS, VOL. 120

