The Science of Secrets ...
MATHEMATICAL CRYPTOLOGY
is yours for only $1.00

as your introduction to the
Library of Computer and Information Sciences

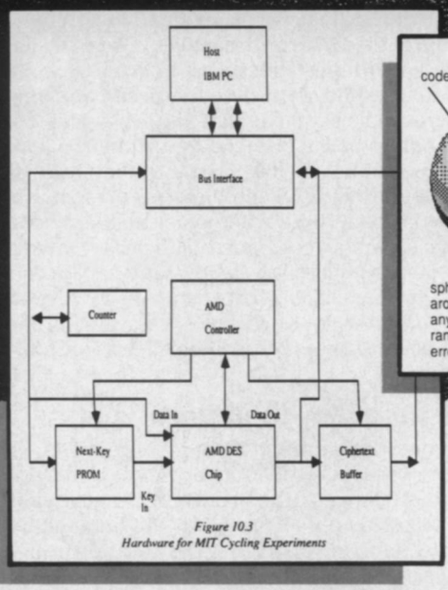
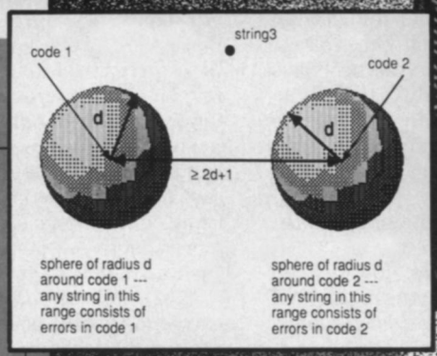
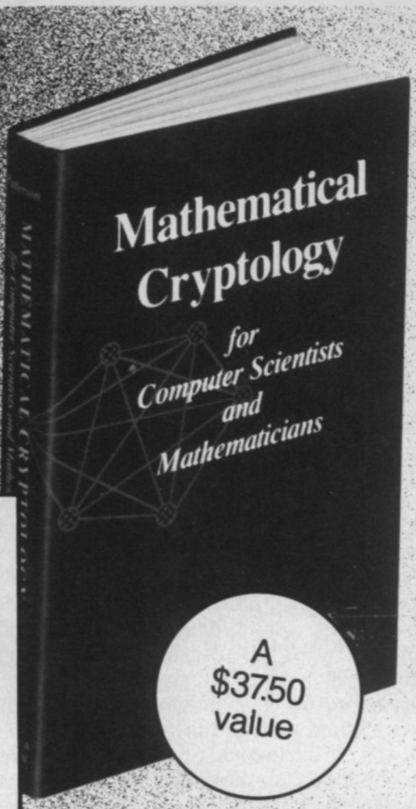


Figure 10.3
Hardware for MIT Cycling Experiments





A $37.50 value

You simply agree to buy three more books—at handsome discounts—within the next 12 months.

- **Why are some cryptosystems effective and others not?**
- **Can a system verify that a message actually comes from the sender and not an impostor?**
- **Why is the current standard, for all practical purposes, obsolete?**

Understand and apply some of the latest techniques in what has quickly become a most critical area in computer science: confidentially transferring computer information.

Covering the Data Encryption Standard (DES) and public-key cryptosystems (PKCs), MATHEMATICAL CRYPTOLOGY starts with basic concepts, and takes you step-by-step through to state-of-the-art applications.

The author explores flaws in the DES, and how the newer PKCs overcome these problems. You'll find details on the original Merkle-Hellmann (or knapsack) PKC as well as the popular Rivest-Shamir-Adelman (RSA) algorithm, including a demonstration of how some knapsack PKCs can be broken. You'll explore recent models for PKCs including a new, unbroken knapsack method using Galois fields.

MATHEMATICAL CRYPTOLOGY considers solutions to puzzles of authentication, "oblivious transfer," and one-way encryption. It details verification protocols, multiple-key encryption, playing "mental poker," and much more.

Complete with 70 pages of Pascal programs that execute algorithms described in the book, MATHEMATICAL CRYPTOLOGY gives you a practical and complete overview of this fascinating topic ... for only $1.00. You save $36.50!

To get your copy for only $1.00, just complete and return the coupon today.

The Library of Computer and Information Sciences 7-EU2
Riverside, NJ 08075

Please accept my application for trial membership and send me Mathematical Cryptology for Computer Scientists and Mathematicians (61000) billing me only $1.00, plus shipping and handling. I agree to purchase at least three additional Selections or Alternates over the next 12 months. Savings range up to 30% and occasionally even more. My membership is cancelable any time after I buy these three additional books. A shipping and handling charge is added to all shipments.

No-Risk Guarantee: If I am not satisfied—for any reason—I may return Mathematical Cryptology for Computer Scientists and Mathematicians within 10 days. My membership will be canceled, and I will owe nothing.

Name_____

Name of Firm_____
(If you want subscription sent to your office)

Address_____ Apt._____

City_____ State_____ Zip_____

(Books purchased for professional purposes may be a tax-deductible expense. Offer good in Continental U.S. and Canada only. Prices slightly higher in Canada.)
Science News 7/23/88

The Library of Computer and Information Sciences is the oldest, largest book club especially designed for computer professionals. In the incredibly fast-moving world of data processing, where up-to-the-moment knowledge is essential, we make it easy to keep totally informed on all areas of the information sciences. What's more, our selections offer you discounts of up to 30% off publishers' prices.

4 Good Reasons to Join

1. The Finest Books. Of the hundreds of books submitted to us each year, only the very finest are selected and offered. Moreover, our books are always of equal quality to publishers' editions, *never* economy editions.
2. Big Savings. In addition to getting Mathematical Cryptology for Computer Scientists and Mathematicians for only $1.00 when you join, you keep saving substantially, up to 30% and occasionally even more. (For example, your total savings as a trial member—including this introductory offer—can easily be over 50%. That's like getting every other book free!)
3. Bonus Books. Also, you will immediately become eligible to participate in our Bonus Book Plan, with savings of 65% off the publishers' prices.
4. Convenient Service. At 3-4 week intervals (16 times per year), you will receive the Library of Computer and Information Sciences News, describing the Main Selection and Alternate Selections, together with a dated reply card. If you want the Main Selection, do nothing, and it will be sent to you automatically. If you prefer another selection, or no book at all, simply indicate your choice on the card and return it by the date specified. You will have at least 10 days to decide. If, because of late mail delivery of the News, you should receive a book you do not want, we guarantee return postage.