

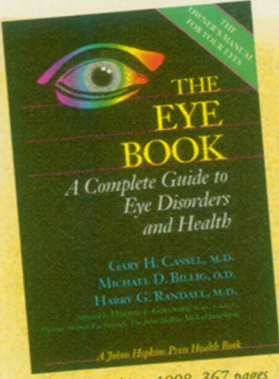
they prefer to study bacteria, such as *Escherichia coli* or *Bacillus subtilis*, that grow quickly and can be genetically manipulated with ease.

"But because of the disease link, I think people are going to be a lot more open to the idea that [nanobacteria] warrant further study," he says.

The medical significance of nanobacteria may eventually extend beyond kidney stones. In a variety of human disorders, including dementias, atherosclerosis, cancers, and arthritis, unexplained calcium precipitation occurs in various tissues of the body, notes Carson in his commentary. And people who get frequent blood transfusions as part of dialysis treatment often develop dangerous calcium deposits, he adds.

Adding to the intrigue, Kajander and Çiftcioglu have conducted a preliminary study of Turkish people who are undergoing dialysis and found that 80 percent displayed evidence of nanobacteria in their blood.

"There is ample cause to investigate thoroughly the part that nanobacteria play not only in renal stone formation but also in the many perplexing diseases associated with pathological extraskeletal calcification," concludes Carson. □




**THE EYE BOOK**  
A Complete Guide to Eye Disorders and Health  
GARY H. CANSEL, M.D.  
MICHAEL D. BELL, O.D.  
HARRY G. RANDALL, M.D.  
A Johns Hopkins Press Health Book  
Johns Hopkins, 1998, 367 pages  
6" x 9", \$18.95

**I**n *The Eye Book*, three eye care specialists present a comprehensive reference to help readers care for their eyes and protect their vision. The authors give special attention to changes and diseases that occur in adults. After detailing how the various parts of the eye work, the authors review everything that can go wrong—from the irritation of itchy eyelids and conjunctivitis to nearsightedness, farsightedness, and astigmatism. Covering emergencies, such as a detached retina, and the major disorders of cataracts, glaucoma, and age-related macular degeneration, the authors explain the signs and symptoms of these problems and their medical and surgical treatments.

—from Johns Hopkins

*Also find out:*

- how to recognize an eye emergency
- all about eyeglasses, including the various kinds of bifocals and trifocals
- how to care for contact lenses and the dangers of improper care
- the unique concerns of people with systemic diseases such as diabetes
- how common medications affect the eyes
- the pros and cons of refractive surgery
- the special problems of people with low vision



A Service of  
Science News Books

**BooksNow**  
The Virtual Bookstore™

*Order by phone for faster service!*  
**1-800-266-5766 ext. 1494**  
Visa, MasterCard, or American Express

*See our web site at [www.sciencenewsbooks.org](http://www.sciencenewsbooks.org)*

There is a postage and handling fee of \$4.95 for the first book and \$2.50 for each additional book.

## Computers

### Quick cracking of secret code

Cryptographers have dramatically reduced the time it takes to decode a message digitally encrypted by a widely used, government-approved method for scrambling sensitive data. Known as the Data Encryption Standard (DES), this method is used routinely by many banks and financial institutions to protect electronic funds transfers and credit-card transactions.

A custom-built computer costing less than \$250,000 needed only 56 hours to identify the required numerical key—a particular sequence of 56 1s and 0s out of 72 quadrillion possibilities. That achievement shattered the previous record of 39 days, set by a network of thousands of computers communicating via the Internet.

"DES can be cracked quickly and inexpensively," says John Gilmore of the Electronic Frontier Foundation (EFF) in San Francisco, which funded the project to counter claims made by U.S. government officials that DES provides adequate protection of sensitive data. EFF announced the feat last month.

"It unambiguously demonstrates that DES is vulnerable, even to attackers with relatively modest resources," comments Matt Blaze of AT&T Labs Research in Florham Park, N.J.

Designed and built by Paul Kocher of Cryptography Research in San Francisco and his coworkers, the new code-cracking computer incorporates more than 1,000 integrated-circuit chips specifically configured for checking the strings of 56 binary digits that comprise DES encryption keys. In its record-breaking run, the computer tried about 25 percent of the possible combinations before finding the correct key to decode a message and win a contest sponsored by RSA Data Security in San Mateo, Calif. The message reads: "It's time for those 128-, 192-, and 256-bit keys."

Some businesses are already using a more robust variant of the DES method, known as Triple DES, which hasn't yet been broken. The U.S. government has also begun a competition to

find a new encryption standard to replace DES. According to requirements established by the National Institute of Standards and Technology (NIST) in Gaithersburg, Md., the new method must allow encryption key sizes of up to 256 bits.

Groups from the United States, Australia, Canada, France, Germany, Japan, and Norway have submitted entries. NIST will announce this month which candidate algorithms meet all the requirements and are eligible for testing and review. —I.P.

### Computers in the house

Survey data prepared for the National Science Foundation (NSF) show a substantial increase in U.S. household computer use in the past decade. According to the just released NSF report "Science and Engineering Indicators 1998," the proportion of households with computers increased from 8 percent in 1983 to 43 percent in 1997. At the end of that period, about 11 percent of the population reported more than one working computer at home, and one-third owned a computer with a modem. Nearly 9 million individuals had two or more e-mail addresses, and 16 percent of the population had access to the World Wide Web.

"Approximately 30 million adults had looked for specific information on the Web during the year preceding the 1997 interview," says Jon D. Miller of the International Center for the Advancement of Scientific Literacy in Chicago, who conducted the computer usage survey. This response indicates that many people are using the Web as a reference library. About a third of those searches involved information about a particular health problem.

The distribution of home computers is strongly related to level of education, the NSF report notes. Where nearly 90 percent of U.S. college graduates used a computer at home or work, only 21 percent of those who did not complete high school worked with computers (SN: 4/18/98, p. 247). —I.P.