Team Sieving Cracks a Huge Number

It's easy to multiply two large prime numbers to obtain a larger number as the answer. But the reverse process – factoring a large number to determine its components – presents a formidable challenge. The problem appears so hard that the difficulty of factoring underlies the so-called RSA method of encrypting digital information.

Last week, an international team of computer scientists, mathematicians, and other experts succeeded in finding the factors of a 129-digit number suggested 17 years ago as a test of the security of the RSA cryptographic scheme.

This feat and other work now complicate encoding schemes used for national and commercial security.

The effort required the use of more than 600 computers scattered throughout the world. Partial results were sent electronically to graduate student Derek Atkins at the Massachusetts Institute of Technology, who assembled and passed the calculations on to Arjen K. Lenstra of Bell Communications Research in Morristown, N.J. In the final step, which by itself consumed 45 hours of computer time, Lenstra used these data and a MasPar MP-1 computer with 16,000 processors to compute the factors.

"It was a nice piece of work – a huge computation done over 8 months," says Burton S. Kaliski Jr. of RSA Data Security in Redwood City, Calif.

The magnitude of the effort required to factor a 129-digit number demonstrates the strength of the RSA cryptosystem, which typically involves numbers of 155 or more digits (SN: 9/7/91, p.148). However, steady improvements in factoring methods are likely to force the use of significantly larger numbers in the future to ensure security. More worrisome are the consequences of new research apparently proving that under certain circumstances, factoring may actually be easy.

In 1977, when Ronald L. Rivest of MIT, Adi Shamir of the Weizmann Institute of Science in Rehovot, Israel, and Leonard M. Adleman of the University of Southern California in Los Angeles first proposed the RSA cryptosystem, even 50-digit numbers seemed beyond reach. As a challenge to computer scientists, the inventors used their scheme to encode a message, which could be decoded only if a certain 129-digit number could be broken down into its 64-digit and 65-digit factors.

114, 381, 625, 757, 888, 867, 669, 235, 779, 976, 146, 612, 010, 218, 296, 721, 242, 362, 562, 561, 842, 935, 706, 935, 245, 733, 897, 830, 597, 123, 563, 958, 705, 058, 989, 075, 147, 599, 290, 026, 879, 543, 541 = 3, 490, 529, 510, 847, 650, 949, 147, 849, 619, 903, 898, 133, 417, 764, 638, 493, 387, 843, 990, 820, 577 x 32, 769, 132, 993, 266, 709, 549, 961, 988, 190, 834, 461, 413, 177, 642, 967, 992, 942, 539, 798, 288, 533

The number and its two prime factors.

At that time, Rivest predicted that factoring this number, using the fastest computers and best factoring methods then available, would require considerably more than 40 quadrillion years of computation. However, this prediction didn't take into account improvements in factoring methods. The existence of the RSA scheme prompted extensive work on factoring.

In 1981, Carl Pomerance of the University of Georgia in Athens invented a factoring method called the quadratic sieve. It proved faster than previous methods and lent itself to group efforts. Factoring could be broken down into lots of little tasks, with the resulting information then pieced together to factor the original number.

In 1988, Lenstra and a colleague coordinated an extensive, international effort using this method to factor a large number, successfully cracking a 100-digit behemoth (SN: 10/22/88, p.263). Last year, Paul Leyland, a computer system manager at the University of Oxford in England, Michael Graff of Iowa State University in Ames, and MIT's Atkins provided the software and assembled a team of volunteers to tackle the RSA number. Lenstra worked out the details of how to complete the factorization.

But this isn't the last word in factoring. In 1988, John M. Pollard of Reading, England, invented the "number field sieve" for factoring large numbers. Lenstra and his coworkers used the method in 1990 to factor a special, 155-digit number (SN: 6/23/90, p.389). New research reveals that the number field sieve may work significantly more efficiently than the quadratic sieve.

In a startling theoretical result that could call into question any cryptosystem based on factoring, Peter W. Shor of AT&T Bell Laboratories in Murray Hill, N.J., has just proved that factoring is "easy" when done on a special type of computer operating according to quantum mechanical principles. Although such a quantum computer does not yet exist, this finding has shaken the cryptographic community. *– I. Peterson*

Neurons may take panoramic view of sounds

Scientists usually assume that in the brain, key neurons divvy up responsibility for estimating the location of sounds originating at various points in the environment. But a new study suggests that a widespread population of brain cells acts in concert to track sounds approaching from all directions.

Each of these "panoramic" neurons, through a distinctive sequence of electrical discharges known as a firing pattern, signals the approximate source of sounds, assert John C. Middlebrooks, a neuroscientist at the University of Florida's Brain Institute in Gainesville, and his colleagues.

Panoramic nerve cells alerted to an incoming sound in this way then work cooperatively to pin down its precise location, they propose.

"We've shown that there's a neural firing pattern in response to sound locations that can be recognized by a simple computer network," Middlebrooks contends. "The brain somehow must pick up on the same information."

Middlebrooks and his coworkers measured the electrical responses of 67 auditory neurons in eight anesthetized cats. These cells are located in the brain's outer layer, or cortex. Animals listened to brief noise bursts, presented one at a time, through each of 18 speakers placed around them in a circle.

For each sound location, the researchers noted the average firing pattern and average number of electrical discharges for the 67 individual neurons.

They then programmed a simple computer system to learn to recognize some of the single-neuron firing patterns generated by sounds from different speakers. In a series of tests, the computer received additional firing patterns and identified their associated sound sources with a high level of accuracy, the researchers report in the May 6 SCIENCE.

The computer proved far less adept at tracing sound origins when supplied with the average number of electrical discharges, or spikes, emitted by neurons.

"There's structure in neural firing patterns, but investigators usually just add up spikes," Middlebrooks holds.

Other studies indicate that two brain regions below the cortex contain cells devoted to pinpointing sounds from particular locations. However, neural pathways from the cortex to these structures may transmit collectively gathered data on firing patterns that proves essential for sound location, Middlebrooks theorizes.

His study builds on similar evidence that neuron firing patterns play an important role in processing visual images (SN: 7/23/88, p.58). *– B. Bower*