Faster Factoring for Cracking Computer Security

For years, mathematicians have known that the number $11^{64}+1$ is really the product of at least two smaller numbers multiplied together, but this 67-digit number until recently withstood their repeated attempts at finding its factors. Last month, mathematicians at Sandia National Laboratories in Albuquerque, N.M., made it the longest "hard" number ever to be factored by a general-purpose factoring routine. That record is likely to fall within the next few weeks when the Sandia group, using their specially designed method for factoring on a Cray computer, expects to crack a 71-digit number. Only eight years ago, the best anyone could do, using a day of computer time, was to factor a difficult 40-digit number.

While factoring was once the pursuit of a few eccentric mathematicians, it has now become an important activity for people concerned about computer security (SN: 7/3/82, p. 12). Several important cryptographic methods (SN: 9/26/81, p. 205) depend on the inherent difficulty in factoring compared with finding out whether a number is prime (divisible only by itself or one) (SN: 3/6/82, p. 158). The recent rapid advances in factoring larger and larger numbers are making some computers vulnerable that just a year ago were thought to be adequately protected by cryptographic systems.

Sandia's Gustavus J. Simmons says, "Factoring is one of a whole class of problems that are so difficult that they're at the edge of computational feasibility. You quickly get to numbers that you can't factor." However, during the last year or so, mathematicians have begun to take advantage of the way particular computers handle information internally by matching a mathematical scheme or algorithm for solving a problem to the way the machine operates most efficiently.

At Sandia, James A. Davis and Diane B. Holdridge started with a method for factoring called the "quadratic sieve," originally invented by Carl Pomerance of the University of Georgia in Athens. This method breaks the problem of factoring a big number into an enormous number of smaller problems, each of which provides some information about the original factorization. The answers go into large arrays in the computer's memory. The "sieving" operation requires selecting and manipulating entries at locations that are all the same distance apart. The Cray is designed to do just that. It can hop directly from one regularly spaced array position to another instead of counting off every location along the way. Matching the Pomerance algorithm to the Cray's "architecture" cut the time to factor a 55-digit number from more than 50 hours to less than four hours.

Then, Davis improved the factoring algorithm by finding a way to make the sieving operation more efficient. After this change, a 58-digit number that had required 8.8 hours took only 1.8 hours to factor. The Sandia researchers reached a new limit when they tried a 67-digit number. The million words of high-speed memory within the Cray simply wasn't big enough to hold all the necessary numbers. Holdridge had to steal "bits" from the computer's operating system to fit the computation within the computer. Now, the Sandia group is switching to a larger model of the Cray computer that will allow them to factor even bigger numbers.

To put their factoring method through the toughest possible tests, the Sandia group has been working on numbers of special interest to mathematicians, including those numbers on a "10 most-wanted" list of candidates for factoring. Six numbers from that list have already been done at Sandia. Their current target is $10^{71}-1$. Although that number is divisible by 9, division leaves a string of 71 ones. This "hard part" is known to be factorable, but no one has yet found its factors.

Other groups are also attacking the problem of factoring large numbers. For instance, Samuel Wagstaff at Purdue University in Lafayette, Ind., and Jeffrey Smith and Carl Pomerance at the University of Georgia are building a computer specially designed just to factor numbers. When the machine is ready, they expect to be able to factor a 78-digit number in a day. The consensus at a recent meeting of mathematicians interested in factoring was that it may be possible to factor any 100-digit number by the 1990s.

Simmons says, "Computational feasibility is something that changes all the time." Given Sandia's dependence on cryptographic systems, some of which apply the difficulty of factoring large numbers, for protecting information such as weapons systems data, Simmons says, "It's critically important for us to know just how difficult factoring is." —*I. Peterson*

The pull of El Niño: Sluggish rotation and longer days

For several weeks last year, the earth slowed down, taking a leisurely fifth of a millisecond extra per day to rotate around its polar axis. At the same time, the earth's atmosphere, which rotates around the same axis, picked up speed — a response, researchers believe, to the record-breaking westerly winds fanned by the El Niño (SN: 11/5/83, p. 298).

The change in the length of day was far briefer than the duration of a single human heartbeat, and certainly never justified an extra swat at the snooze alarm. Still, when meteorologists in Cambridge, Mass., scanned logs of the earth's total wind speeds provided by the U.S. National Meteorological Center in Washington, D.C., they saw instantly that the peak in wind speeds, and thus the atmosphere's rate of rotation, was higher than recorded for any several-week period since record-keeping began in 1976. The speed of the atmosphere varies seasonally — faster during the Northern Hemisphere winter, slower in summer — but the observed 1983 winter peak was eight percent higher than the normal increase of several milliseconds per day.

The scientists, Richard D. Rosen and David A. Salstein of Atmospheric and Environmental Research, Inc., were aware that the El Niño, a massive warming in the Pacific Ocean, was near its peak around Jan. 25, 1983, when the greatest change in day length first occurred. "It didn't take long to figure out that there must be a relationship" between the two events, Salstein says.

For several years, the researchers have been monitoring the wind speed, or the total angular momentum of the atmosphere, and linking it to the rotation of the earth. The connection is expressed in a physical principle known as the law of conservation of angular momentum. According to this law, the rotation of the earth and atmosphere are coupled and share a total momentum: when one speeds up, the other must slow down. For many years, the speeds of rotation of the earth and atmosphere have been correlating very well, Salstein says. When the researchers noted last winter's high values for the angular momentum of the atmosphere, they contacted geodesists, scientists whose field of study encompasses the speed of the earth's rotation. "When they checked their records, indeed they found that the earth had slowed down by the same amount that the atmosphere had speeded up," Rosen says. "It's a nice confirmation of the theory."

The atmosphere can have a significant effect on the length of day over periods of up to four years. Over longer terms, the rotation of the solid earth is more influenced by geophysical effects such as tides, earthquakes and the coupling between the earth's core and mantle. —*C. Simon*