MATHEMATICS

Small Army of Code-Breakers Conquers a 129-Digit Giant

Look at it as a mathematical game—with national security at stake. Cryptographers create codes that are extraordinarily difficult to break, and then code-breakers set out to break them, both sides exploiting exponential improvements in technology. In the latest move, Arjen Lenstra of Bellcore in Redbank, New Jersey, and his colleagues announced last week that after 8 months of work they had factored a 129-digit number, notorious in the cryptography trade as RSA-129, into two mammoth primes. The feat may have been the largest computation ever, but the team had lots of help: 600 computer-wielding volunteers recruited over the Internet.

BELLCORE

Number crunchers. Lenstra and Leyland *(left and center)*, along with Rivest, who helped set the challenge.

The computational tour de force, say its leaders, sets a benchmark for the security technologies that protect sensitive data in government and industry. That's because the difficulty of factoring such enormous numbers underlies many of the computer high-security codes in use these days. The achievement also demonstrates the potential for using the Internet to recruit hundreds of geographically disparate computers for a single scientific task. It's a strategy, says Ravi Ganesan of Bell Atlantic, that could "move science forward to achieve things we can't even imagine today."

The challenge these researchers took up was laid down 17 years ago in a column in *Scientific American*. It was based on the then-new idea of public-key encryption—a coding scheme that relies on two keys. One key is published freely, for use by anyone who wants to encode a message. Only the intended recipient holds the other, private key, needed to decipher the message. Conversely, the private key can serve for encoding messages, which any holder of the public key can decipher—but no one can forge.

In 1977, three Massachusetts Institute of Technology cryptographers, Ronald Rivest, Adi Shamir, and Leonard Adleman, developed what is now the dominant public-key system, called RSA. RSA is based on the fact that it is easy to find large prime numbers but extraordinarily difficult to factor the product of two large primes. "We based the security of our cryptosystem on that difficulty," says Rivest. "You use the product of two large prime numbers as the public key, and the two primes themselves as part of the private key." That same year, *Scientific American*'s Martin Gardner asked Rivest, Adleman, and Shamir for a challenge to put in his "Mathematical Games" column, and RSA-129 was born.

For Gardner's column, Rivest estimated the time needed to factor RSA-129 with the best computers and algorithms of the day at 40 quadrillion years. He now says that prediction was in error even at the time. Other papers he published with Adleman and Shamir made forecasts much more in line with the time it actually took Lenstra and his colleagues, Paul Leyland of Oxford University, Michael Graff of Iowa State, and Derek Atkins of MIT, to unknot the problem.

The work began last year when Leyland, Graff, and Atkins, all active members of an Internet mailing list devoted to cryptography and computer security, decided to see just how vulnerable a large-prime product might be to new technologies and factoring algorithms. Lenstra suggested that they tackle RSA-129 and provided the factoring algorithm, and Leyland adapted it to a software package for distribution on the Internet. He then "cast it adrift around the world for people to join in," he says. Six hundred volunteers from 25 countries, representing some 1600 computers, took part in this first stage of the factoring, which entails building a large database of mathematical clues (see box).

"They [had] everything from personal computers," says Leyland, "to workstations of every kind, a Cray supercomputer, and several parallel supercomputers." Graff coordinated the volunteers, and Atkins handled queries from the volunteers and collected their results. Lenstra then fed the data into

How to Make a Prime Cut

Exactly what 1600 computers did day in and day out for 8 months to factor a 129-digit number into a pair of primes isn't easy to grasp, says Arjen Lenstra of Bellcore in Redbank, New Jersey. But after some coaxing he provided *Science* with a much-simplified version of the factoring algorithm that broke the back of RSA-129. Here it is:

The goal is to find two numbers, x and y, such that $x^2 - y^2$ is equal to a multiple of n, the number to be factored. Then $x^2 = y^2$ + (a multiple of n), or, in mathematical notation, $x^2 \equiv y^2 \bmod n$. If you then take the greatest common divisor of n and $x - y$, says Lenstra, "there's a big chance that you'll get a prime factor" of n.

For example, say you want the factors of $n = 143$. As Lenstra explains, there's little chance of guessing an x that also gives you a y right away. "You'll usually find an x that only satisfies a much weaker property, from which you can build up a database that you can eventually squeeze into a factorization."

For 143, your first guess might be $x = 17$. Since $x^2 = 289$, or $3 + 2 \times 143$, $x^2 \equiv 3 \bmod 143$. Although 3 is not a square, so it doesn't satisfy the condition $x^2 \equiv y^2 \bmod n$, it is a small prime. That, says Lenstra, makes $x = 17$ qualify for entry into the database.

Next guess: $x = 18$. $x^2 = 324 = 38 + 2 \times 143 \equiv 2 \times 19 \bmod 143$. "We don't get a nice small [number like] 3," says Lenstra. "We get 2×19, so we say this is a bad choice and throw it out."

Third guess: $x = 19$. $x^2 = 361 = 75 + 2 \times 143 \equiv 3 \times 5^2 \bmod 143$. Because 3 and 5 are small primes, this too goes into the database.

The two database entries, $17^2 \equiv 3 \bmod 143$ and $19^2 \equiv 3 \times 5^2 \bmod 143$, turn out to be enough to factor 143. First, multiply the two entries to get $17^2 \times 19^2 \equiv 3 \times 3 \times 5^2 \bmod 143$.

That can be written $(17 \times 19)^2 \equiv (3 \times 5)^2 \bmod 143$ and satisfies the condition $x^2 \equiv y^2 \bmod n$.

So $x = 17 \times 19 = 323$, and $y = 3 \times 5 = 15$.

Now the final step: Find the greatest common divisor of n and $x - y$, where $n = 143$ and $x - y = 323 - 15 = 308$. It turns out to be 11. That's one prime factor; dividing 143 by 11 gives 13, which is the other prime factor of 143.

"What the Internet volunteers do," says Lenstra, "is something similar to this method, using tricks that are more complicated. And they do it by guessing billions of numbers at a time, all starting at different places."

–G.T.

RSA-129 and Its Factors

1143816257578888676692357799761466120102182967212423625625618429357 \
0693524573389783059712356395870505898907514759929002687954354 1

=

3490529510847650949147849619903898133417764638493387843990820577

X

3276913299326670954996198819083446141317764296799294253979828853 3

Bellcore's MasPar supercomputer to arrive at the factors: two primes of 65 and 64 digits.

In explaining the significance of the Bellcore feat, Rivest says that "assessing the difficulty of factoring these large numbers has become very important for the security of the national information infrastructure." Or as Lenstra puts it, "If we can do it, someone else can do it." The factoring of RSA-129 does not, however, mean the RSA code is obsolete. Even now, Rivest says, few users rely on numbers as small as RSA-129. "They're using numbers which are considerably larger, and this accomplishment will encourage them to use numbers larger yet." Numbers as long as 200 digits are predicted to be 7000 times more difficult to factor, and a 400-digit number may be 300 billion times more difficult.

But as in an arms race, no escalation is likely to go unmatched for long. At the same press conference where Lenstra and company announced the defeat of RSA-129, he promised a "surprise" for the next factoring feat. He hinted at a new, faster algorithm—and perhaps a test involving a number with quite a few more digits than 129.

–Gary Taubes

NUCLEAR RESEARCH

Physicists Find a Double Dose of Magic

DARMSTADT—Magic seems to abound at Germany's heavy-ion accelerator laboratory, GSI. Researchers there are the acknowledged masters of the black art of creating new heavy elements by smashing smaller nuclei together—they are credited with discovering the three heaviest elements currently known—and they also bring a magic touch to other regions of the periodic table. So much was evident last week, when GSI scientists announced that they had created the isotope tin-100, a so-called "doubly magic" nucleus that had been predicted by theories of nuclear structure but never before found.

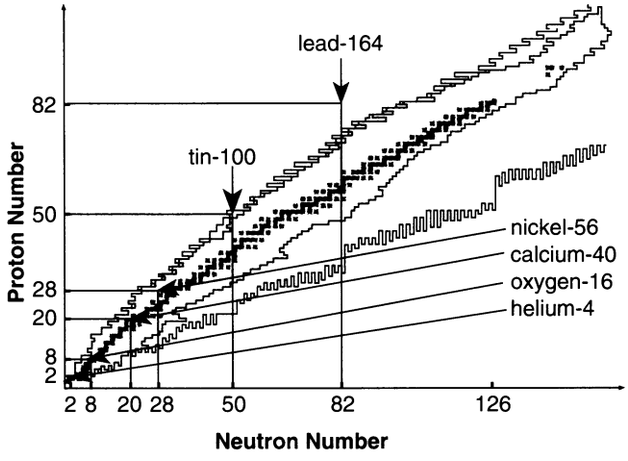
Nuclear physicists are acclaiming the achievement, which other laboratories had also been pursuing. "There was talk 15 years ago about trying to make tin-100 nuclei, but at that time many people thought it would be impossible to do," says Brad Sherrill of the National Superconducting Cyclotron Laboratory at Michigan State University (MSU). Tin-100, which has equal numbers of protons and neutrons, lies far from the range of stable elements; in stable nuclei of this size, a large majority of neutrons ordinarily counteracts the electromagnetic repulsion of the charged protons, which would otherwise break the nucleus apart. But physicists eager to test nuclear theories had a strong incentive to try to make tin-100. According to current theories, the isotope's complement of protons and neutrons constitute "magic numbers," which should make it—relatively speaking—far more stable than nuclei with slightly different numbers. By making and studying the isotope, physicists could test the theories' predictions.

Indeed, the GSI team, led by Jörg Friese from Munich's Technical University and Gottfried Münzenberg from GSI, now estimates that compared to nearby isotopes, which have lifetimes in the range of less than a millisecond, tin-100 is a virtual Methuselah, surviving for several seconds. More detailed studies of the new isotope, says Sherrill, should help researchers test fine points of the current nuclear theory, which holds that protons and neutrons occupy a series of spherical "shells." When a nucleus contains full shells of protons or neutrons (2, 8, 20, 28, 50, or 82 of them, for example), it gains extra stability and is said to have a magic number. Doubly magic nuclei have magic numbers of both protons and neutrons.

Doubly magic nuclei serve as prime testing grounds for this picture because of their simplicity. As soon as a nucleus has more than a few protons and neutrons, the equations governing its structure ordinarily become impossibly complicated, and it becomes very difficult for theorists to predict its properties accurately. Full shells of protons and neutrons simplify the equations. Tin-100, however, has an added advantage: equal numbers of protons and neutrons, a symmetry that improves the situation even further. "A doubly magic nucleus like tin-100 is a nice simple system," says Sherrill. So far, physicists have studied four other doubly magic nuclei with equal numbers of protons and neutrons, but all are smaller than tin-100. The new member of this select group will help researchers prove the validity of the theory for larger nuclei.

But such studies will have to wait until the GSI group can scale up production of the isotope. The team made tin-100 by smashing xenon-124 ions against a target of beryllium, then analyzing the charge and mass of the debris in search of the isotope. Despite the relatively long half-life of tin-100 nuclei, they are very hard to make because of the delicate balance of forces: After such a violent collision, the chance that the nuclear debris will settle into neat spherical shells before electromagnetic repulsion breaks it apart is slim. In fact, the GSI team had to bombard the target with 1.7×10^{13} xenon ions to produce just seven tin-100 nuclei.

The other groups also pursuing the isotope are further behind. The disappointment may be particularly sharp for a group at the French heavy-ion accelerator GANIL at Caen. They have produced various tin isotopes including tin-101, and they finished another run on the very day the Darmstadt team announced its findings. Says group leader Marek Lewitowicz: "From the data we gathered, we have a 90% chance of also identifying tin-100 at GANIL."



Isotope table. Doubly magic nuclei with equal protons and neutrons.

The race that has just ended at Darmstadt may be the last of its kind. The next doubly magic nucleus with equal protons and neutrons would be lead-164, which is so far outside the range of stable nuclei that even a double dose of magic will not preserve it. "No one suspects that that nucleus will be possible," says Sherrill.

–Michael Simm and Daniel Clery

Michael Simm is a science writer in Bonn.