A mighty number falls

May 21 2007

Mathematicians and number buffs have their records. And today, an international team has broken a long-standing one in an impressive feat of calculation.

On March 6, computer clusters from three institutions – the EPFL, the University of Bonn and NTT in Japan -- reached the end of eleven months of strenuous calculation, churning out the prime factors of a well-known, hard-to-factor number that is a whopping 307 digits long.

"This is the largest 'special' hard-to-factor number factored to date," explains EPFL cryptology professor Arjen Lenstra. (The number is 'special' because it has a special mathematical form -- it is close to a power of two.) The news of this feat will grab the attention of information security experts and may eventually lead to changes in encryption techniques.

Although it is relatively easy to identify huge prime numbers, factoring, or breaking a number down into its prime components, is extremely difficult. RSA encryption, named for the three individuals who devised the technique (Ronald Rivest, Adi Shamir and Leonard Adleman), takes advantage of this. Using the RSA method, information is encrypted using a large composite number, usually 1024 bits in size, created by multiplying together two 150-or-so digit prime numbers. Only someone who knows those two numbers, the "keys", can read the message. Because there is a vast supply of large prime numbers, it's easy to come up with unique keys. Information encrypted this way is secure, because no one has ever been able to factor these huge numbers. At least not yet.

The most recent factoring record is RSA200, a 200-digit 'non-special' number whose two prime factors were identified in 2005 after 18 months of calculations that took over a half century of computer time.

The international team factored the current 307-digit behemoth using the "special number field sieve," a method devised in the late 1980s by Lenstra (then at Bellcore), his brother Hendrik, then a professor at UC Berkeley, English mathematician John Pollard and Mark Manasse from DEC. The 11-month job took a century of computer time.

A feat like this would have been unthinkable back in 1990 when Lenstra started applying number theory and distributed computing to the task of breaking factoring records. Increased computer power and refined computational techniques have raised the bar, and will continue to do so. "We have more powerful computers, we have come up with better ways to map the algorithm onto the architecture, and we take better advantage of cache behavior," Lenstra explains.

Is the writing on the wall for 1024-bit encryption" "The answer to that question is an unqualified yes," says Lenstra. For the moment the standard is still secure, because it is much more difficult to factor a number made up of two huge prime numbers, such as an RSA number, than it is to factor a number like this one that has a special mathematical form. But the clock is definitely ticking. "Last time, it took nine years for us to generalize from a special to a non-special hard-to factor number (155 digits). I won't make predictions, but let's just say it might be a good idea to stay tuned."

Source: Ecole Polytechnique Fédérale de Lausanne

https://phys.org/news/2007-05-mighty-falls.html