# Quadratic Sieve

Pick a number **a** at random from [1,..,(**m**-1)/2]

Case 1: **a** has a factor in common with **m** (i.e. gcd(**a**, **m**)>1) then use **a** to factor **m** by finding the gcd.

Case 2: **a** has no factor in common with **m** (i.e. gcd(**a**, **m**)=1) then find $a^2$ (mod **m**) and compare the answer to all the other squares already found. If there is another number b such that

$$a^2 \equiv b^2 \pmod{m}$$

then

$$(a+b)(a-b) \equiv a^2 - b^2 \equiv 0 \pmod{m}$$

This means that

$$(a+b)(a-b) = km \text{ for some } k$$

but since a and b are ≤ (**m**-1)/2 then we know that **a** + **b** < **m** and **a** - **b** < **m**
So **m** doesn't divide **a** + **b** or **a** - **b** but it does divide the product. ∴ some factors of **m** are in **a** + **b** and the others are in **a** - **b**. So **m** factors into gcd(**a** + **b**, **m**) and gcd(**a** - **b**, **m**).

Example: **m** = 91

$1^2 \equiv 1 \quad 6^2 \equiv 36 \quad 9^2 \equiv 81 \quad 12^2 \equiv 144 \equiv 53 \quad 20^2 \equiv 400 \equiv 36$

$20^2 - 6^2 \equiv (20+6)(20-6) \equiv 0$

gcd(91, 20+6) = 13 and gcd(91, 20-6) = 7

It is not unusual for RSA keys to have close to 1000 digits. Using this method of factoring, numbers on the order of 100 digits are vulnerable.

**Factoring Googols**
***Computers on three continents factor an elusive number***

Networking through more than 400 computers in the U.S., the Netherlands and Australia, a team of computer scientists has shattered all previous records by finding the two large, prime factors for a 100-digit number. The accomplishment, which was one of the largest parallel-computing projects ever undertaken, has begun to threaten the security of some cryptographic codes used by governments, banks and industries.

To factor the 100-digit number the project organizers, Mark S. Manasse of the Digital Equipment Corporation (DEC) in Palo Alto and Arjen K. Lenstra of the University of Chicago, implemented a method devised by Carl Pomerance of the University of Georgia. This method, known as the quadratic sieve, discovers factors by finding two numbers that when squared and divided by the original number have the same remainder. To find the factors of 15, for instance, the method would reveal that 8 and 2, when squared and divided by 15, both leave a remainder of 4. Once the two numbers are found, the factors can be computed. In this case 2 is subtracted from 8, leaving 6. If 6 is then subtracted from 15 as many times as possible without producing a negative number, the final result is 3, which is indeed one of the prime factors of 15.

It may take more than subtracting 6 from 15 until the smallest positive number is found. In general you should take the gcd of 6 & 15

Although factoring small numbers by the quadratic-sieve method is a slow process, this method factors large numbers faster than any other method yet devised.

Another advantage of the quadratic sieve is that many different computers can share the task of finding factors. A computer at DEC handled the bulk of the task of factoring the 100-digit number while computer centers in the U.S., the Netherlands and Australia shared the rest of the calculation. On the 26th day of the project Manasse and Lenstra had accumulated enough data to factor the 100-digit number, which is equal to $11^{104}+1$ divided by $11^{8}+1$, into prime factors 41 and 60 digits long.

The ability to factor numbers that large may enable decipherers to break some codes from a widely used cryptographic system created by Ronald L. Rivest, Adi Shamir and Leonard Adelman of the Massachusetts Institute of Technology. The Rivest-Shamir-Adelman (RSA) system is based on the fact that, although large prime numbers can be computed easily, factoring the product of two such numbers has been infeasible. Every user of the RSA system chooses two large prime numbers and publishes the product. A message is converted into a string of numbers by some conventional method and is then encoded by a mathematical operation based on the published number. A message can be decoded only by a second operation based on the original prime numbers. If the published number can be factored, however, the message can be deciphered. To keep a system secure, users must choose prime numbers sufficiently large to ensure that the published number cannot be factored.

Following Manasse and Lenstra's project, many organizations may reconsider the security of their codes and choose larger numbers. In 1977 Rivest calculated that a 125-digit code that consisted of two 63-digit primes would be secure. The time required for the fastest computers of that year to break a 125-digit code would have been 40 quadrillion years. A system similar to the one employed by Manasse and Lenstra, the workers say, could break such a code in one year. —*Russell Ruthen*

The setup:
Factor n by finding two numbers a≠b, a,b ∈ [1..(n-1)/2] s.t.
$a^2 \equiv b^2 \pmod{n}$
∴ $a^2 - b^2 \equiv (a+b)(a-b) \equiv 0 \pmod{n}$
Then the factors of n are gcd(a+b, n) & gcd(a-b, n)

# The Assault on 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

By GINA KOLATA

Mathematicians say they are close to breaking a cryptographic stronghold that was not expected to fall for many years. The item is a 129-digit number that was first described in 1977 as proof of the security of a new public cryptographic system.

The number is known for short as RSA 129 after the initials of its inventors and its number of digits. The new coding system depended on very large numbers that were multiples of two primes, a prime being a number divisible only by itself and one.

The code could be cracked only by finding the component primes, one of the most mathematically difficult tasks imaginable. The inventors proposed RSA 129 as an example. Only they knew its component primes, and they asserted it would take others at least 40 quadrillion years to factor it, using the best methods and the fastest computers that were then available.

But over the years the number proposed as uncrackable simply became a challenge. Eight months ago, with the power of computers growing, cryptography enthusiasts proposed a cunning scheme to attack it. They would break the problem into millions of tiny pieces and then use volunteers recruited on the Internet, an international electronic mail system, to do the calculations on their computers, at night or in other fallow periods.

RSA 129 has not crumbled yet. But several factoring experts said that so many of the calculations have already been completed that they are confident the solution will emerge in a few weeks.

The inventors of RSA are Dr. Ronald Rivest, of the Massachusetts Institute of Technology, Dr. Adi Shamir of the Weizmann Institute of Science in Rehovoth, Israel, and Dr. Leonard Adelman of the University of Southern California.

The RSA code acts like a lockbox with two keys. One key is a large composite number, which the owner may distribute publicly. Anyone could use that key to open the box and put a message in for the owner. But once the message is put in, the lockbox can only be opened again by the owner, who has the second key, which is the two factors of the composite number. And only the owner knows those numbers, because he has purposely constructed the composite number from two large prime numbers..

Commercial cryptographic chips based on this scheme use numbers that are typically either 135 or 150 digits. But users can choose even larger numbers if they like. Dr. Rivest, who is also chairman of the company that makes the chips, says that even if the 129 digit number is cracked, their security will not be immediately threatened.

Dr. Arjen Lenstra, a factoring expert at Bellcore in Morristown, N.J., said the eventual factoring of RSA 129 was a near certainty. Dr. Andrew Odlysko, a factoring expert at A.T.& T. Bell Laboratories in Murray Hill, N.J., said although it was still possible that the effort to factor RSA 129 would fail, "It is extremely unlikely, probably much smaller than the chances of an asteroid hitting the earth tomorrow."

Dr. Odlysko said that putting together the pieces of the problem to yield the factors of RSA 129 was like turning over squares on "Wheel of Fortune." Just as, eventually, participants in the game show know that almost enough squares have been turned for the phrase to be guessed, so the mathematicians know that almost enough calculations have been completed so that discovery of the factors of RSA 129 is imminent.

The soon to be realized factoring of RSA 129 will be "a landmark," Dr. Odlysko said. "It shows us how far we can go," he added.

The attack on RSA 129 originated last summer, when Dr. Lenstra got a message from a group of Internet users who wanted help with a factoring challenge. The three computer hobbyists, Dr. Paul Leyland, who is a computer system manager at Oxford University in England, and two graduate students, Derek Atkins at the Massachusetts Institute of Technology and Michael Graff of Iowa State University, wanted to recruit volunteers to factor a large number, thinking of it as a sort of a mathematical game.

## Making Task 'Really Interesting'

"I told them, why don't you do something that's really interesting, like RSA 129," Dr. Lenstra said. They readily agreed.

The three advertised on an Internet bulletin board that is read by people interested in cryptography. So far, said Mr. Atkins, they have had 1,693 requests from volunteers for identification numbers, which are used to keep track of those working on the problem, and for pieces of the problem to work on. And, Mr. Atkins added, "every day more join in."

The Internet volunteers use computer programs supplied by Mr. Graff, Mr. Atkins and Dr. Leyland to do the calculations. Then they send their data to M.I.T., to be checked for accuracy. When all the data are in, Mr. Atkins will send them to Dr. Lenstra. He, in turn, will put them together in one immense calculation to yield the factors of RSA 129.

Factoring a number is one of the oldest and most difficult mathematical problems. It requires finding every prime number that divides into the number with no remainder. Factoring is simple for smallish numbers. The factors of 33, for example, are 3 and 11. The factors of 935 are 5, 11, and 17 because 5×11×17 gives 935. But as numbers grow large, the task of testing every lesser prime to see if it is a factor quickly becomes very daunting.

For example, Dr. Lenstra said, to mount this kind of attack on RSA 129 would require testing 10 to the 50th, or more than one hundred thousand quadrillion quadrillion quadrillion primes. Using the conventional approach, this task could take up to a quadrillion quadrillion years. But, the code's designers said at the time, mathematical shortcuts might bring that down to 40 quadrillion years.

## Basis on Factoring Scheme

No one has found a way to factor very large numbers with little effort, but mathematicians have taken nibbles at the problem. The method being used by the Internet volunteers is based on a factoring scheme invented in 1981 by Dr. Carl Pomerance of the University of Georgia, known as the quadratic sieve.

It allows a large and complex problem like factoring to be parceled out as millions of small pieces that, put together at the end, can yield a solution. Most of the pieces of data turn out to be useless to the final solution, but mathematical tricks allow the good data to be separated from the bad, like a sieve sifting gold nuggets from sand.

Even with the quadratic sieve, the factoring of RSA 129 will end up taking more than 10 to the 17th calculations. This is within a factor of a million of experts' best estimate of the total number of calculations ever done in the history of humanity, Dr. Adelman said. What made the effort work was the fact that computers have gotten so fast and that so many computers could be brought to bear on the problem.

RSA was a sensation when it appeared because it was entirely different from conventional cryptographic schemes, which use mathematical formulas to scramble data. Because there is no way to prove that their method is unbreakable, the cryptographers can only say that they asked experts to try to break it and none succeeded.

With RSA, in contrast, the only way to break the code is to factor a very

NYTimes March 22, 1994

NY Times
March 22.
1994

# Code was believed unbreakable a decade ago, but not anymore

SD Tribune Tues May 16, 1994
Computer Link Section

Continued From Page B5

# Assault on Big Number Said to Be Near Success

large number that was used to scramble data. So the inventors could say that breaking the code was provably hard — it was as hard as factoring a particular large number.

In theory, owners could use numbers as large as they want for encoding. But the larger the number, the longer it takes to encode data, so users have to balance their need for security with their need for speed. Dr. Rivest said the code is widely used by companies, and that more than three million copies of its software have been sold.

Dr. Adelman said he was happy to see the attack on RSA 129. "I congratulate them," he said. "It's a stimulating thing." Dr. Adelman himself contributed to the effort, joining the Internet volunteers.

Dr. Rivest said the effort to crack RSA 129 was "a demonstration of the difficulty of the problem." After all, Dr. Rivest said, RSA 129 "has been around for 17 years and it has taken this long to get up the stage where you can attack it."

Dr. Adelman said the attack posed little threat to the RSA scheme in general because making the number to be factored just slightly bigger added immensely to the difficulty of factoring. "Improvements in computer technology always favor the cryptographer over the cryptanalyst," he said.

Dr. Odlysko said he agreed with Dr. Adelman, but he added that the attack on RSA 129 did reveal something about the security of the code. "The real significance of the factoring of RSA 129," he said, "is that the foreseeable future 17 years ago did not envision being able to factor a number of this size."

No one predicted that individual computers would be so fast, that thousands of computers would be hooked up on Internet or that such significant technical advances would be made in the mathematics of factoring.

By RORY J. O'CONNOR
*Knight-Ridder News Service*

An international team of 600 volunteers, armed mostly with inexpensive computers, has demonstrated that a popular scheme for protecting sensitive computer data is more vulnerable than many of its users might believe.

The team broke a coded message that just 10 years ago was considered too difficult for even the most powerful computers in the world to decipher. The chief of the codebreaking effort is warning users that they should employ far more complex versions of the scheme, called RSA, because the growing power of interconnected personal computers and workstations could eventually allow determined hackers to break their codes.

Led by Bellcore, the research arm of the seven Baby Bell telephone companies, the team read a message encoded 17 years ago in RSA-129, a version of RSA invented by three mathematicians at MIT. The trio — Ronald Rivest, Adi Shamir and Leonard Adleman — were so confident of the code's security that they offered a $100 reward to anybody who could break it.

## NUMERICAL LOCKS.

The RSA code secures information with the help of lengthy numbers that act as electronic locks and keys.

The keys, which are kept secret, are a pair of "prime" numbers — numbers divisible only by themselves and by the number 1. The lock is a much larger number obtained by multiplying the two secret prime numbers together. It can be made public and used to scramble a message — one that can be unscrambled only with the secret keys.

The system is considered secure because it is impractical to calculate the secret numbers from the public one — if the public number is large enough. But the task is not impossible. The Bellcore project, whose results were announced late last month, showed that the 129-digit public number used in the 1977 challenge is no longer adequate.

It is not yet a direct threat to most commercial installations, which use far more digits in their public numbers. Software that includes RSA encryption as part of a larger package — such as Lotus Development Corp.'s Notes and Apple Computer's System 7 Pro operating system — use 150 digits.

Such a number is around 100 times more difficult to factor than the RSA-129 code, said project leader Arjen Lenstra.

Indeed, the MIT researchers rescinded the award in 1985, when they thought computers had become powerful enough to challenge the 129-digit key. And in the past four years, Lenstra and others have broken RSA schemes with 100, 110 and 120 digits.

## VULNERABILITY TEST

Bellcore organized the project to see how vulnerable RSA users might be to those bent on reading their messages or misdirecting electronic financial transactions. While many organizations fear hackers might break their codes, the needed computing power is within easier reach of large corporations or foreign governments engaged in industrial espionage, or spy agencies like the computer-studded National Security Agency.

The commercial distributor of RSA technology, RSA Data Security of Redwood City, Calif., said the time it took to break the 129-digit code means the 150-digit code will remain uncrackable for some time.

"It took all those computers running all that long to break that key," said RSA Data chief James Bidzos. "Every three digits you add to the size of the key doubles the difficulty of factoring it."

The effort to break the 129-digit code underscores, though, how networks of cheap computers can perform the tasks once reserved for the most powerful supercomputers. Of the 1,600 computers used in the project, about 80 percent were the same kind of personal computers and workstations commonly found in offices and universities.

The message itself made little sense. It read: "The magic words are squeamish ossifrage." And the MIT mathematicians awarded the $100 prize anyway.