NUMBER 10 — MARCH 8, 1999

RSA Laboratories' Bulletin

News and advice on data security and cryptography

The Factorization of RSA-140

Scott Contini
RSA Laboratories, San Mateo, California

As is well known, the security of the RSA cryptosystem [3] and the difficulty of factoring are closely related. To help track progress in factoring technology and to promote interest in factoring as a research problem, RSA Data Security sponsors the *RSA Factoring Challenge* with financial prizes being awarded to successful factorers.

On February 2, 1999, the factorization of RSA-140 was completed using the general number field sieve factoring algorithm (GNFS). RSA-140 is a 140-digit number of the form used for RSA moduli and it was the smallest unfactored RSA-number in the factoring challenge. Its factorization is the largest factorization ever reported using a general purpose factoring algorithm. Such algorithms are the most important for attacking cryptosystems based on the difficulty of factoring. The previous record was a 130-digit number known as RSA-130 which was also factored by GNFS.

contribution	factorer
36.8%	Peter L. Montgomery, Stefania Cavallar, Herman J.J. te Riele, Walter M. Lioen
28.8%	Paul C. Leyland
26.6%	Bruce Dodson
5.4%	Paul Zimmerman
2.5%	Arjen K. Lenstra

Scott Contini is a member of the research staff at RSA Laboratories, and can be reached at scontini@rsa.com.

GNFS [1] is the fastest general purpose factorization algorithm known. However prior to this factorization, there were reasons to question its practicality for factoring numbers substantially larger than 130-digits. In particular, the algorithm consists of three parts: (1) a gathering of data stage, (2) a solution of a matrix to find dependencies among the data, and (3) the use of the dependencies to factor the number. The third stage can be accomplished efficiently on a single workstation, and the first stage can be efficiently carried out in parallel on a network of loosely coupled workstations. However, existing techniques to solve the second stage seem to work well only when done on a single machine and, at least in theory, this stage requires a lot of computation. Moreover, the memory requirements to solve such a matrix are huge. Therefore, this stage could potentially become the bottleneck for factoring larger numbers.

When RSA-130 was factored, the matrix had approximately 3.5 million rows and columns. This was much larger than any previous matrices seen in factoring algorithms. Based on this, the expected size of the matrix for a 140-digit number was about seven million rows and columns. However, the matrix for RSA-140 was significantly smaller: it had only a little more than 4.5 million rows and columns. The reason for the smaller than expected size is an improvement of the "polynomial selection" techniques of GNFS, which also had the impact of reducing the expected amount of time for the data gathering stage. This improvement gives new hope in factoring a 512-bit (155-digit) number in the near future, which is important since at one time (long before the discovery of GNFS), a 512-bit RSA modulus was considered to be secure.

RSA Laboratories
A Division of RSA Data Security

Today, RSA Data Security recommends using a 768-bit RSA modulus for personal use, 1024-bits for corporate use, and 2048-bits for protecting extremely valuable data. The chart below demonstrates the difficulty of factoring such moduli in comparison to the factorization of RSA-140. RSA-140 was pessimistically estimated to take 2000 MIPS-years to factor (in other words, a computer that does one million instructions per second would take about 2000 years to factor the number), and required about 800 megabytes of central memory to solve the matrix. The values in the chart are approximations which were obtained by using the heuristic running time formula for GNFS (ignoring the o(1) term). The second columns tells how much more time the data gathering and matrix stages are expected to take, and the third column tells how much more memory the matrix should require. It is worth noting that the time and memory to solve the matrix can be reduced at the cost of spending more time on the data gathering stage.

number	month	MIPS-years	algorithm
RSA-100	April 1991	7	quadratic sieve
RSA-110	April 1992	75	quadratic sieve
RSA-120	June 1993	830	quadratic sieve
RSA-129	April 1994	5000	quadratic sieve
RSA-130	April 1996	1000†	generalized number field sieve
RSA-140	February 1999	2000	generalized number field sieve

† *The original report sent to the RSA Factoring Challenge administrator cited 500 MIPS-years of computation. However, other postings by the factorers of RSA-130 suggest that 1000 MIPS-years more accurately reflects the work effort expended. Both GNFS factorizations could have been done faster had more memory been available.*

modulus size (bits)	number of times harder to factor than RSA-140	number of times more memory required than RSA-140
512	6.5	2.5
768	40000	200
1024	49000000	7000

We conclude that it is likely that we will see a 512-bit factorization within the next couple years. However, GNFS in its present form is not good enough to factor numbers of the sizes recommended by RSA Data Security. There would have to be major assymptotic improvements to the algorithm, or the discovery of an entirely new way of factoring for such moduli to be considered insecure.

The reader interested in more information about possible factoring trends is referred to Andrew Odlyzko's article *The Future of Integer Factorization* [2]. More information on the RSA Factoring Challenge can be obtained by sending e-mail to *challenge-info@rsa.com*.

References

[1] J.P. Buhler, H.W. Lenstra, and C. Pomerance. The development of the number field sieve. Volume 1554 of *Lecture Notes in Computer Science*, Springer-Verlag, 1994.

[2] A.M. Odlyzko. The future of integer factorization. *CryptoBytes*, 1(2): 5-12, 1995.

[3] R.L. Rivest, A. Shamir, and L.M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2): 120-126, February 1978.

For more information on this and other recent security developments, contact RSA Laboratories at one of the addresses below.

RSA Laboratories
20 Crosby Drive
Bedford, MA 01730 USA
781/687-7000
781/687-7213 (fax)
rsa-labs@rsa.com
http://www.rsa.com/rsalabs/

Copyright © 1999 RSA Laboratories, a division of RSA Data Security, Inc., a Security Dynamics Company. All rights reserved.