

INDEX

Algebra
 Applied Mathematics
 Calculus and Analysis
 Discrete Mathematics
 Foundations of Mathematics
 Geometry
 History and Terminology
 Number Theory
 Probability and Statistics
 Recreational Mathematics
 Topology

Alphabetical Index

DESTINATIONS

About *MathWorld*
 About the Author
 Headline News (RSS)
 New in *MathWorld*
MathWorld Classroom
 Interactive Entries
 Random Entry

CONTACT

Contribute an Entry
 Send a Message to the Team

MATHWORLD - IN PRINT

Order book from Amazon

MathWorld Headline News

RSA-640 Factored

By Eric W. Weisstein

November 8, 2005--A team at the German Federal Agency for Information Technology Security (BSI) recently announced the factorization of the 193-digit number

310 7418240490 0437213507 5003588856 7930037346 0228427275
 4572016194 8823206440 5180815045 5634682967 1723286782
 4379162728 3803341547 1073108501 9195485290 0733772482
 2783525742 3864540146 9173660247 7652346609

known as RSA-640 (Franke 2005). The team responsible for this factorization is the same one that previously factored the 174-digit number known as RSA-576 (*MathWorld* headline news, [December 5, 2003](#)) and the 200-digit number known as RSA-200 (*MathWorld* headline news, [May 10, 2005](#)).

RSA numbers are [composite numbers](#) having exactly two [prime factors](#) (i.e., so-called [semiprimes](#)) that have been listed in the Factoring Challenge of RSA Security[®].

While composite numbers are defined as numbers that can be written as a product of smaller numbers known as [factors](#) (for example, $6 = 2 \times 3$ is composite with factors 2 and 3), [prime numbers](#) have no such decomposition (for example, 7 does not have any factors other than 1 and itself). Prime factors therefore represent a fundamental (and unique) decomposition of a given positive integer. RSA numbers are special types of composite numbers particularly chosen to be difficult to factor, and they are identified by the number of digits they contain.

While RSA-640 is a *much* smaller number than the 7,816,230-digit monster [Mersenne prime](#) known as M_{42} (which is the largest prime number known), its factorization is significant because of the curious property that proving or disproving a number to be prime ("[primality testing](#)") seems to be much easier than actually identifying the factors of a number ("[prime factorization](#)"). Thus, while it is trivial to multiply two large numbers p and q together, it can be extremely difficult to determine the factors if only their product pq is given. With some ingenuity, this property can be used to create practical and efficient encryption systems for electronic data.

RSA Laboratories sponsors the RSA Factoring Challenge to encourage research into computational number theory and the practical difficulty of factoring large integers and also because it can be helpful for users of the [RSA encryption](#) public-key cryptography algorithm for choosing suitable key lengths for an appropriate level of security. A cash prize is awarded to the first person to factor each challenge number.

RSA numbers were originally spaced at intervals of 10 [decimal](#) digits between one and five hundred digits, and prizes were awarded according to a complicated formula. These original numbers were named according to the number of decimal digits, so RSA-100 was a hundred-digit number. As computers and algorithms became faster, the unfactored challenge numbers were removed from the prize list and replaced with a set of numbers with fixed cash prizes. At this point, the naming convention was also changed so that the trailing number indicates the number of digits in the [binary](#) representation of the number. Hence, RSA-640 has 640 binary digits, which translates to 193 digits in decimal.

While RSA-640 has slightly fewer digits than the previously factored RSA-200, its factorization carries the additional benefit of a cash reward of \$20,000 from RSA Laboratories to the team responsible for this feat.

RSA numbers received widespread attention when a 129-digit number known as RSA-129 was used by R. Rivest, A. Shamir, and L. Adleman to publish one of the first public-key

messages together with a \$100 reward for the message's decryption (Gardner 1977). Despite widespread belief at the time that the message encoded by RSA-129 would take millions of years to break, it was factored in 1994 using a distributed computation that harnessed networked computers spread around the globe performing a multiple polynomial [quadratic sieve](#) (Leutwyler 1994). The result of all the concentrated number crunching was decryption of the encoded message to yield the profound plain-text message "The magic words are squeamish ossifrage." (An ossifrage is a rare predatory vulture found in the mountains of Europe.)

Factorization of RSA-129 followed earlier factorizations of RSA-100, RSA-110, and RSA-120. The challenge numbers RSA-130, RSA-140, RSA-150, RSA-155, RSA-160, RSA-200, and RSA-576 were also subsequently factored between 1996 and May of 2005.

The factorization of the latest RSA number to fall involved "lattice" sieving done by J. Franke and T. Kleinjung using hardware at the Scientific Computing Institute and the Pure Mathematics Institute at Bonn University, Max Planck Institute of Mathematics in Bonn, and Experimental Mathematics Institute in Essen. The factorization of RSA-640 was accomplished using a [prime factorization algorithm](#) known as the general number field sieve. Sieving was done on 80 2.2-GHz Opteron CPUs and took 3 months. The matrix step was performed on a cluster of 80 2.2-GHz Opterons connected via a Gigabit network and took about 1.5 months. The two 97-digit factors found using this sieve are

```

1634733 6458092538 4844313388 3865090859 8417836700 3309231218
1110852389 3331001045 0815121211 8167511579
x
1900871 2816648221 1312685157 3935413975 4718967899 6851549366
6638539088 0271038021 0449895719 1261465571

```

These numbers can easily be multiplied to verify that their product is indeed equal to the original number.

As the following table shows, RSA-704 to RSA-2048 remain open, carrying awards from \$30,000 to \$200,000 to whoever is clever and persistent enough to track them down. A list of the open challenge numbers may be [downloaded from RSA](#) or in the form of a *Mathematica* package from the [MathWorld package archive](#).

number	digits	prize	factored
RSA-100	100		Apr. 1991
RSA-110	110		Apr. 1992
RSA-120	120		Jun. 1993
RSA-129	129	\$100	Apr. 1994
RSA-130	130		Apr. 10, 1996
RSA-140	140		Feb. 2, 1999
RSA-150	150		Apr. 16, 2004
RSA-155	155		Aug. 22, 1999
RSA-160	160		Apr. 1, 2003
RSA-200	200		May 9, 2005
RSA-576	174	\$10,000	Dec. 3, 2003
RSA-640	193	\$20,000	Nov. 4, 2005
RSA-704	212	\$30,000	open
RSA-768	232	\$50,000	open
RSA-896	270	\$75,000	open
RSA-1024	309	\$100,000	open
RSA-1536	463	\$150,000	open
RSA-2048	617	\$200,000	open

References

Franke, J. Email sent 4 Nov 2005.
<http://www.crypto-world.com/announcements/rsa640.txt>

Franke, J. Email to NMBRTHRY@LISTSERV.NODAK.EDU. 10 Nov 2005.
<http://listserv.nodak.edu/cgi-bin/wa.exe?A1=ind0511&L=nbrthry>

Gardner, M. "Mathematical Games: A New Kind of Cipher That Would Take Millions of Years to Break." *Sci. Amer.* **237**, 120-124, Aug. 1977.

Leutwyler, K. "Superhack: Forty Quadrillion Years Early, a 129-Digit Code Is Broken." *Sci. Amer.* **271**, 17-20, 1994.

NFSNet: Large-Scale Distributed Factoring.
<http://www.nfsnet.org>

RSA Security [®]. "The New RSA Factoring Challenge."
<http://www.rsasecurity.com/rsalabs/challenges/factoring>

RSA Security [®]. "The RSA Challenge Numbers."
<http://www.rsasecurity.com/rsalabs/challenges/factoring/numbers.html>

Weisstein, E. W. *Mathematica* package `RSANumbers.m`.

Weisstein, E. W. "RSA-576 Factored." *MathWorld* Headline News. Dec. 5, 2003.
<http://mathworld.wolfram.com/news/2003-12-05/rsa>

Weisstein, E. W. "RSA-200 Factored." *MathWorld* Headline News. May 10, 2005.
<http://mathworld.wolfram.com/news/2005-05-10/rsa-200>