

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

ABOUT THIS SITE

About *MathWorld*
 About the Author
 Terms of Use

DESTINATIONS

What's New
 Headline News (RSS)
 Random Entry
 Animations
 Live 3D Graphics

CONTACT

Email Comments
 Contribute!
 Sign the Guestbook

MATHWORLD - IN PRINT

Order book from Amazon

MathWorld Headline News

RSA-576 Factored

By Eric W. Weisstein

December 5, 2003--On December 3, the day after the announcement of the discovery of the largest known prime by the Great Internet Mersenne Prime Search on December 2 (*MathWorld* headline news, [December 2, 2003](#)), a team at the German Federal Agency for Information Technology Security (BIS) announced the factorization of the 174-digit number

1881 9881292060 7963838697 2394616504 3980716356 3379417382
 7007633564 2298885971 5234665485 3190606065 0474304531
 7388011303 3967161996 9232120573 4031879550 6569962213
 0516875930 7650257059

known as RSA-576.

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-576 is a *much* smaller number than the 6,320,430-digit monster [Mersenne prime](#) announced earlier this week, its factorization is significant because of the curious property of numbers 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-576 has 576 binary digits, which translates to 174 digits in decimal.

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-155, and RSA-160 were also subsequently factored between 1996 and April of this year. (Amusingly, RSA-150 apparently remains unfactored following its withdrawal from the RSA Challenge list. [However, see postscript.]

On December 2, Jens Franke circulated an email announcing factorization of the smallest prize number RSA-576. The factorization was accomplished using a [prime factorization algorithm](#) known as the general number field sieve. The two 87-digit factors found using this sieve are

```

3980750 8642406493 7397125500 5503864911 9906436234 2526708406
3851895759 4638895726 1768583317
x
4727721 4610743530 2536223071 9730482246 3291469530 2097116459
8521711305 2071125636 3590397527

```

and can easily be multiplied to verify that they do indeed give the original number.

Franke's note detailed the factorization process in which "lattice" sieving was 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; and "line" sieving was done by P. Montgomery and H. te Riele at CWI, F. Bahr and his family, and NFSNET (which at that time consisted of D. Leclair, P. Leyland, and R. Wackerbarth). Post-processing of this data to construct the actual factors was then done with the support of the BSI.

For their efforts, the team will receive a cash prize of \$10,000 from RSA Security. However, award seekers need not be deterred. As the following table shows, RSA-640 to RSA-2048 remain open, carrying awards from \$20,000 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	withdrawn?	open [see postscript]
RSA-155	155		Aug. 22, 1999
RSA-160	160		Apr. 1, 2003
RSA-576	174	\$10,000	Dec. 3, 2003
RSA-640	193	\$20,000	open
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

Postscript added August 24, 2004:

RSA-150 was factored into two 75-digit primes by Aoki *et al.* in a [preprint](#) dated April 16, 2004.

References

Franke, J. "RSA576." Privately circulated email reposted to [primenumbers Yahoo! Group](#).

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`.