WIKIPEDIA

# RSA Factoring Challenge

The **RSA Factoring Challenge** was a challenge put forward by RSA Laboratories on March 18, 1991 to encourage research into computational number theory and the practical difficulty of factoring large integers and cracking RSA keys used in cryptography. They published a list of semiprimes (numbers with exactly two prime factors) known as the RSA numbers, with a cash prize for the successful factorization of some of them. The smallest of them, a 100 decimal digit number called RSA-100 was factored by April 1, 1991, but many of the bigger numbers have still not been factored and are expected to remain unfactored for quite some time, however advances in quantum computers make this prediction uncertain due to Shor's algorithm.

The RSA challenges ended in 2007.[1] RSA Laboratories stated: "Now that the industry has a considerably more advanced understanding of the cryptanalytic strength of common symmetric-key and public-key algorithms, these challenges are no longer active."[2]

The factoring challenge was intended to track the cutting edge in integer factorization. A primary application is for choosing the key length of the RSA public-key encryption scheme. Progress in this challenge should give an insight into which key sizes are still safe and for how long. As RSA Laboratories is a provider of RSA-based products, the challenge was used by them as an incentive for the academic community to attack the core of their solutions — in order to prove its strength.

The RSA numbers were generated on a computer with no network connection of any kind. The computer's hard drive was subsequently destroyed so that no record would exist, anywhere, of the solution to the factoring challenge.[3]

The first RSA numbers generated, RSA-100 to RSA-500 and RSA-617, were labeled according to their number of decimal digits; the other RSA numbers (beginning with RSA-576) were generated later and labelled according to their number of binary digits. The numbers in the table below are listed in increasing order despite this shift from decimal to binary.

## Contents

## The mathematics

RSA Laboratories states that: for each RSA number *n*, there exists prime numbers *p* and *q* such that

$$n = p \times q.$$

The problem is to find these two primes, given only *n*.

## The prizes and records

The following table gives an overview over all RSA numbers.

> *The challenge numbers in white lines are numbers expressed in base 10, while the challenge numbers in yellow lines are numbers expressed in base 2. The prizes for RSA-576 and RSA-640 have been awarded. The remaining prizes have been retracted since the challenge became inactive in 2007.*

| RSA Number | Decimal digits | Binary digits | Cash prize offered | Factored on | Factored by |
|---|---|---|---|---|---|
| RSA-100 | 100 | 330 | US$1,000[4] | April 1, 1991[5] | Arjen K. Lenstra |
| RSA-110 | 110 | 364 | US$4,429[4] | April 14, 1992[5] | Arjen K. Lenstra and M.S. Manasse |
| RSA-120 | 120 | 397 | $5,898[4] | July 9, 1993[6] | T. Denny et al. |
| RSA-129 [**] | 129 | 426 | $100 USD | April 26, 1994[5] | Arjen K. Lenstra et al. |
| RSA-130 | 130 | 430 | US$14,527[4] | April 10, 1996 | Arjen K. Lenstra et al. |
| RSA-140 | 140 | 463 | US$17,226 | February 2, 1999 | Herman te Riele et al. |
| RSA-150 | 150 | 496 | | April 16, 2004 | Kazumaro Aoki et al. |
| RSA-155 | 155 | 512 | $9,383[4] | August 22, 1999 | Herman te Riele et al. |
| RSA-160 | 160 | 530 | | April 1, 2003 | Jens Franke et al., University of Bonn |
| RSA-170 [*] | 170 | 563 | | December 29, 2009 | D. Bonenberger and M. Krone [***] |
| RSA-576 | 174 | 576 | $10,000 USD | December 3, 2003 | Jens Franke et al., University of Bonn |
| RSA-180 [*] | 180 | 596 | | May 8, 2010 | S. A. Danilov and I. A. Popovyan, Moscow State University[7] |
| RSA-190 [*] | 190 | 629 | | November 8, 2010 | A. Timofeev and I. A. Popovyan |
| RSA-640 | 193 | 640 | $20,000 USD | November 2, 2005 | Jens Franke et al., University of Bonn |
| RSA-200 [*] ? | 200 | 663 | | May 9, 2005 | Jens Franke et al., University of Bonn |
| RSA-210 [*] | 210 | 696 | | September 26, 2013[8] | Ryan Propper |
| RSA-704 [*] | 212 | 704 | $30,000 USD | July 2, 2012 | Shi Bai, Emmanuel Thomé and Paul Zimmermann |
| RSA-220 [*] | 220 | 729 | | May 13, 2016 | S. Bai, P. Gaudry, A. Kruppa, E. Thomé and P. Zimmermann |
| RSA-230 | 230 | 762 | | | |
| RSA-232 | 232 | 768 | | | |
| RSA-768 [*] | 232 | 768 | $50,000 USD | December 12, 2009 | Thorsten Kleinjung et al. |
| RSA-240 | 240 | 795 | | | |
| RSA-250 | 250 | 829 | | | |
| RSA-260 | 260 | 862 | | | |
| RSA-270 | 270 | 895 | | | |
| RSA-896 | 270 | 896 | $75,000 USD | | |
| RSA-280 | 280 | 928 | | | |
| RSA-290 | 290 | 962 | | | |
| RSA-300 | 300 | 995 | | | |

| | | | | |
|---|---|---|---|---|
| RSA-309 | 309 | 1024 | | |
| RSA-1024 | 309 | 1024 | $100,000 USD | |
| RSA-310 | 310 | 1028 | | |
| RSA-320 | 320 | 1061 | | |
| RSA-330 | 330 | 1094 | | |
| RSA-340 | 340 | 1128 | | |
| RSA-350 | 350 | 1161 | | |
| RSA-360 | 360 | 1194 | | |
| RSA-370 | 370 | 1227 | | |
| RSA-380 | 380 | 1261 | | |
| RSA-390 | 390 | 1294 | | |
| RSA-400 | 400 | 1327 | | |
| RSA-410 | 410 | 1360 | | |
| RSA-420 | 420 | 1393 | | |
| RSA-430 | 430 | 1427 | | |
| RSA-440 | 440 | 1460 | | |
| RSA-450 | 450 | 1493 | | |
| RSA-460 | 460 | 1526 | | |
| RSA-1536 | 463 | 1536 | $150,000 USD | |
| RSA-470 | 470 | 1559 | | |
| RSA-480 | 480 | 1593 | | |
| RSA-490 | 490 | 1626 | | |
| RSA-500 | 500 | 1659 | | |
| RSA-617 | 617 | 2048 | | |
| RSA-2048 | 617 | 2048 | $200,000 USD | |

^ * The number was factored after the challenge became inactive.

^ ** RSA-129 was not part of the RSA Factoring Challenge, but was related to a column by Martin Gardner in *Scientific American*.

^ *** RSA-170 was also independently factored by S. A. Danilov and I. A. Popovyan two days later.[7]

## See also

- RSA numbers, decimal expansions of the numbers and known factorizations
- The Magic Words are Squeamish Ossifrage, the solution found in 1993 to another RSA challenge posed in 1977
- RSA Secret-Key Challenge
- Integer factorization records

## Notes

1. RSA Laboratories, The RSA Factoring Challenge (http://www.emc.com/emc-plus/rsa-labs/historical/the-rsa-factoring-challenge-faq.htm). Retrieved on 2013-11-09.
2. RSA Laboratories, The RSA Factoring Challenge FAQ (http://www.emc.com/emc-plus/rsa-labs/historical/the-rsa-factoring-challenge-faq.htm). Retrieved on 2013-11-09.
3. RSA Laboratories. "The RSA Factoring Challenge FAQ" (http://www.emc.com/emc-plus/rsa-labs/historical/the-rsa-factoring-challenge-faq.htm). Retrieved 2008-08-05.
4. http://www.ontko.com/~rayo/primes/rsa_news.txt
5. RSA Honor Roll (http://www.ontko.com/~rayo/primes/hr_rsa.txt)
6. On the factorization of RSA-120 - Springer (http://www.springerlink.com/content/n9tvubu089l1x58y). Springerlink.com. Retrieved on 2014-05-11.
7. http://eprint.iacr.org/2010/270.pdf
8. RSA-210 factored (http://www.mersenneforum.org/showpost.php?p=354259), mersenneforum.org

# External links

- RSA Security: The RSA factoring challenge (https://web.archive.org/web/20130507091636/http://www.rsa.com/rsalabs/node.asp?id=2092)
- MathWorld: RSA Number (http://mathworld.wolfram.com/RSANumber.html)
- Mathematica package for RSA numbers (https://web.archive.org/web/20050408020446/http://mathworld.wolfram.com/packages/RSANumbers.m)
- The original challenge announcement on sci.crypt (https://www.google.com/groups?selm=BURT.91Mar18092126%40chirality.rsa.com)
- The original challenge announcement on sci.crypt (updated link) (https://groups.google.com/forum/#!original/sci.crypt/AA7M9qWWx3w/EkrsR69CDqIJ)
- Certicom ECC Challenge (https://www.certicom.com/index.php?action=ecc,ecc_challenge)
- MTC3 (https://www.mysterytwisterc3.org) Thanks to RSA Inc, the crypto contest MTC3 contains all unsolved RSA numbers and offers users additional information and feedback about these factorization challenges.

Retrieved from "https://en.wikipedia.org/w/index.php?title=RSA_Factoring_Challenge&oldid=809407207"

**This page was last edited on 8 November 2017, at 22:25.**