

MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

RSA FACTORING CHALLENGE: RSA-370

Author: RSA Inc

January 2012

Introduction

The RSA crypto system by Rivest, Shamir and Adleman is the most well-known modern crypto system. In 1991 RSA Inc [1] published 54 challenges with various key lengths for the modulus N (100 to 617 decimal digits).

These RSA cipher challenges [2] were the most well-known crypto challenges. RSA Inc initially advertised prize money for the solution of 14 of these challenges [3]. When RSA Inc stopped the contest in 2007, the money for 8 prizes was already payed. By now (status January 2012), 16 of initially 54 challenges have been solved.

RSA Inc permitted the MTC3 team to host the remaining 38 challenges and to offer it within the MTC3 contest as challenges. Thanks to Ari Juels.

RSA-370

For solving the RSA-370 challenge it is necessary to factor the following decimal number with 370 decimal digits:

N = 1888287707234383972842703127997127272470910519387718
0623809855230049870767017212819937261952549039800018
9611225867126246614422885027456814543631704846907379
4495250347974943216943521462713202965796237266310948
2249345567254149154427009931528792352727792665782922
0716103274629754608002579386403054361786262087880224
4305286292772467355603044265985905970622730682658082
529621

For the solution, please hand in one of the two prime factors as a decimal number.

Sources

[1] <http://www.rsa.com>

[2] http://en.wikipedia.org/wiki/RSA_Factoring_Challenge
http://en.wikipedia.org/wiki/RSA_numbers

[3] <http://www.rsa.com/rsalabs/node.asp?id=2093>

Appendix

A "cipher challenge" is a cryptographic problem that has been published, sometimes with a prize offered for cracking it.

When a cipher challenge has not yet been cracked despite many attempts, then confidence in the propagated system rises. If someone succeeds in cracking the problem, then the cryptosystem with the specified parameters is no longer regarded as secure.