

MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

RSA FACTORING CHALLENGE: RSA-310

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-310

For solving the RSA-310 challenge it is necessary to factor the following decimal number with 310 decimal digits:

$N =$ 1848210397825850670380148517702559371400899745254512
5219257074455803347106014125276757082979328578439013
8810476689842943312641913946269652458346498372465163
1481888473364151368736236317783587518465017087145416
7340264246156906116201163809824841208576884836765760
94865930188367141388795454378671343386258291687641

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.