

MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

RSA FACTORING CHALLENGE: RSA-250

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 paid. 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-250

For solving the RSA-250 challenge it is necessary to factor the following decimal number with 250 decimal digits:

$N =$ 2140324650240744961264423072839333563008614715144755
0177977549208814180234471401366433455190958046796109
9285187247091458768739626192155736304745477052080511
9056493106687691590019759405693457452230589325976697
471681738069364894699871578494975937497937

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.