

MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

RSA FACTORING CHALLENGE: RSA-440

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-440

For solving the RSA-440 challenge it is necessary to factor the following decimal number with 440 decimal digits:

$N = 2601428211955602590070788487371320550539810804595235$
2894235085896633912708374310252674800592426746319007
9788900653375731605419428681140656438533272294845029
9423322261711239266063575232577368936674523411922479
0516838789368452481803077294973049597108473379738051
4567326311991648352970360740543275296663078122345977
6639075044144531440817180207090407273927593041029935
9006059619305590701939627725296116299946059898442103
959412221518213407370491

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.