

MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

RSA FACTORING CHALLENGE: RSA-460

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-460

For solving the RSA-460 challenge it is necessary to factor the following decimal number with 460 decimal digits:

N = 1786856020404004433262103789212844585886400086993882
9550810515785076348075241464078819812169681394445771
4763346084886877462543182928286033961495626230363564
5546753552581286559710032014178315212224644686666427
6604414664193378883689324522173213548604843532961314
0382117586289099859865385837383562865435188048063622
3164308238684873105235011577671552114945370886842810
8303016983133390041636551546685700490084750164480807
68256389182668489641536264864604484300734909

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.