

# MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

## RSA FACTORING CHALLENGE: RSA-480

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-480

For solving the RSA-480 challenge it is necessary to factor the following decimal number with 480 decimal digits:

$N = 3026570752950908697397302503155918035891122835769398$   
5839552963263430597614457144169659817040125185215913  
8533455982172343712313383247732107268535247763784105  
1865492461998880703310884628557435208806712993028955  
4682269549296857738070679584280220082941119842229732  
6020823369315258921162990168697393348736236081296604  
1851456906399528297817679014976052139554853281419653  
4676974259747930685864584926832898568742388185363260  
4706175564461719396117318298679820785491875674946700  
413680932103

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_Factoring_Challenge)  
[http://en.wikipedia.org/wiki/RSA\\_numbers](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.