

# MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

## RSA FACTORING CHALLENGE: RSA-350

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-350

For solving the RSA-350 challenge it is necessary to factor the following decimal number with 350 decimal digits:

$N =$  2650719995173539473449812097373681101529786464211583  
1624674545482293445855043495841191504413349124560193  
1604781465284337078077168653919828230617514191516068  
4965557504967646864473791707114248731286314681680195  
4812702917123189212728868259282632393834443989482096  
4980002198783774200949834726366790897650136033823229  
72552204068806061829535529820731640151

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.