

# MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

## RSA FACTORING CHALLENGE: RSA-490

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-490

For solving the RSA-490 challenge it is necessary to factor the following decimal number with 490 decimal digits:

N = 1860239127076846517198369354026076875269515930592839  
1502010283538370310259713738522164743327949206433999  
0682255318550725546067821388008411628660373933246578  
1718042017172224499540303152935478714013629615010650  
0248655268866341574597589257935941656510207892200673  
114169260769497776760490610706193787354060159427473  
1617619377537419071307115490065850326946551649682856  
8654377183190586953764069804493263889349245791475085  
5858980849190488385315076922453755527481137671909614  
4119390052199027715691

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.