

# MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

## RSA FACTORING CHALLENGE: RSA-617

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-617

For solving the RSA-617 challenge it is necessary to factor the following decimal number with 617 decimal digits:

N = 227018012937850141935804051202045867410612359627665839070  
940218792151714831191398948701330911110449016834009494838  
468182995180417635079489225907749254660881718792594659210  
265970467004498198990968620394600177430944738110569912941  
285428918808553627074076707225937377726669734409773612433  
363973080517630915068363107953126072395203652900321058488  
395079814523072994171857157962974549950235053160409198591  
937180233074148804462179228008317660409386563445710347785  
534571210805307363945359239326518660305150410609664373133  
236728315393235000679371075419554373624332483612425259458  
68802353916766181532375855504886901432221349733

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.