



THE CRYPTO CHALLENGE CONTEST

RSA FACTORING CHALLENGE: RSA-704

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-704

For solving the RSA-704 challenge it is necessary to factor the following decimal number with 212 decimal digits (704 bit):

$N = 7403756347956171282804679609742957314259318888923128$
9084936232638972765034028266276891996419625117843995
8943305021275853701189680 98286733173273108930900552
5051168770632990723963807867100860969625379346505637
96359

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.