MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

RSA Factoring Challenge: RSA-500

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 permited the MTC3 team to host the remaining 38 challenges and to offer it within the MTC3 contest as challenges. Thanks to Ari Juels.

RSA-500

For solving the RSA-500 challenge it is necessary to factor the following decimal number with 500 decimal digits:

N = 189719413374862665633053474331720252723718359195342830318458112306245045887076876059432123476257664274945547644195154275867432056593172546699466049824197301601038125215285400688031516401611623963128370629793265939405081077581694478604172141102464103804027870110980866421480002556045468762513774539341822154948212773356717351534726563284480011349409264424384401989109086032526788147850601132077287172819942445113232019492229554237898606631074891074722425617396803191692438146762357129342922999744113 61

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.