MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

RSA Factoring Challenge: RSA-470

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-470

For solving the RSA-470 challenge it is necessary to factor the following decimal number with 470 decimal digits:

N = 1705147378468118520908159923888702802518325585214915
96835889183698096753980368977114423836025263145191923
36661227059581551031197088611676317766996441181409574
86602388713064698304619191359016382379244440741228665
45522954536883748558744552128950445218096208188788876
32439504936237680657994105330538621759598404770960395
43124476927252768875945906587929399246092612647885720
32212334726855302571883565912645432522077138010357669
55555507104409085708953932056496357677028541336969

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.