

768-bit RSA cracked

Vložil/a [Bystroushaak](#) [1], 10 Leden, 2010 - 15:11

Researchers have decomposed a 768-bit number with 232 decimal places into its two prime factors and published a paper with their results. The number is the string released as "RSA-768" under the now defunct RSA Challenge. As a result, RSA encryptions with 768-bit keys must, from now on, be considered cracked.

<http://www.h-online.com/security/news/item/768-bit-RSA-cracked-898986.html> [2]

URL článku: <https://security-portal.cz/clanky/768-bit-rsa-cracked>

Odkazy:

[1] <https://security-portal.cz/users/bystroushaak>

[2] <http://www.h-online.com/security/news/item/768-bit-RSA-cracked-898986.html>