Russian Mathematics 2011 vol.55 N4, pages 12-17

One approach to factorization of positive integers

Boiko A., Ziyatdinov D., Ishmukhametov S.
Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

Factorization of positive integers into primes is a hard computational task. Its complexity lies in the base of the most popular method of cryptography, the RSA method. In this paper we propose a new technique in a factorization procedure which combines ideas of the Number Field Sieve (NFS) and the Quadratic Sieve (QS) in a special manner. © Allerton Press, Inc., 2011.

http://dx.doi.org/10.3103/S1066369X11040037

Keywords

Factorization, NFS, Number field sieve, QS, Quadratic sieve