Lobachevskii Journal of Mathematics 2016 vol.37 N3, pages 284-287

RSA cryptosystem for dedekind rings

Petukhova K., Tronin S.
Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

© 2016, Pleiades Publishing, Ltd.May soon be invented quantum computer and some known cryptosystems (such as RSA) will be threatened breaking. This paper is aimed at establishing necessary conditions for the maximum possible algebraic generalization of the classical RSA algorithm. We substitute ideals of a Dedekind ring for integers. Ideals in Dedekind rings allow the unique decomposition into a product of maximal ideals, but may not be the principal ideals. Also we define Euler's ϕ-function for ideal of a Dedekind ring and describe some properties of this function. We hope that our proposed method will help to develop algorithms for encryption, which is hard to crack using a quantum computer.

http://dx.doi.org/10.1134/S1995080216030197

Keywords

Algebraic cryptography, algebraic numbers, cryptographic protocol, Dedekind ring, Euler's function, ideal, RSA, security