NÚMEROS INTEIROS E CRIPTOGRAFIA RSA

Rafaela Fernandes de Souza Pontes[1], Leomaques Francisco Silva Bernardo[2].

RESUMO

A Teoria dos Números é um dos ramos mais antigos da matemática e tem por objetivo o estudo dos números inteiros e suas propriedades. Vários problemas foram discutidos dentro dessa teoria, um deles é a identificação se determinado número é ou não primo. Na tentativa de encontrar soluções para essa problemática, diversos matemáticos se dedicaram a busca do que é chamado de testes de primalidade. Dentre as mais diversas aplicações dessa teoria, se encontra a criptografia, área que estuda meios de codificar mensagens, a fim de proporcionar uma segurança na comunicação. Alguns desses meios fazem uso de números primos grandes, em particular, a criptografia RSA. Diante do exposto, o presente trabalho tem o intuito de estudar a base matemática necessária para implantar o método de criptografia RSA, que na sua aplicação faz uso da teoria dos números e um pouco da teoria de grupos. A pesquisa se deu por meio de estudos bibliográficos, especialmente no livro “Números interios e Criptografia RSA”, de Severino Collier Coutinho.

Palavras-chave: números primos, criptografia RSA, grupos.

[1]Aluna do curso de Licenciatura em Matemática, Unidade Acadêmica de Matemática, UFCG, Campina Grande, PB, e-mail: rafaela.rf37@gmail.com
[2]Doutor, professor, Unidade Acadêmica de Matemática, UFCG, Campina Grande, PB, e-mail: leomaques@mat.ufcg.edu.br

NÚMEROS INTEIROS E CRIPTOGRAFIA RSA

ABSTRACT

Number theory is one of the oldest areas of mathematics and its objective is to study integer numbers and its properties. Several problems were discussed in this theory, one of them is identifying if a given number is or not prime. In the attempt to find solutions to this problem, several mathematicians devoted themselves to the pursuit of what are called primality tests. Among the most diverse applications of this theory is cryptography, an area which studies means to codify messages in order to provide security in the communication. Some of these means make use of large prime numbers, in particular, RSA criptography. Given the above, this work aims to study the necessary mathematical basis to implement the RSA criptography method, which in its application makes use of the number theory and a small part of group theory. The research took place through bibliographic studies, specially in the book “Números inteiros e Criptografia RSA”, by Severino Collier Coutinho.

Key words: prime numbers, RSA criptography, groups.