INICIAÇÃO À CRIPTOGRAFIA RSA

Fabrício Adolfo Veríssimo
Faculdade de Educação, Ciências e Artes Dom Bosco de Monte Aprazível, FAECA
15150-000, Monte Aprazível, SP
E-mail: fabricio@faeca.com.br

Luís Eduardo Bilharva Presoto
Faculdade de Educação, Ciências e Artes Dom Bosco de Monte Aprazível, FAECA
15150-000, Monte Aprazível, SP
E-mail: edu_lebp@hotmail.com

RESUMO

A criptografia RSA foi desenvolvida na década de 70, por três matemáticos do MIT (Instituto de Tecnologia de Massachusets), Ron **R**ivest, Adi **S**hamir e Len **A**dleman (RSA). O método se baseia em teoremas e resultados conhecidos há alguns séculos que, a princípio, não tinham nenhuma finalidade prática e que fazem parte da teoria dos números.

O RSA é um método de criptografia de chave pública, ou seja, a chave de codificação pode ser conhecida por todos e a chave de decodificação conhecida apenas pelo receptor, que transforma a mensagem na forma original. O RSA também foi um dos primeiros métodos a possibilitar a assinatura digital.

Para implementá-lo, num primeiro momento é necessário escolher os parâmetros de criptografia que são dois números primos (p, q) de no mínimo 60 algarismos. Num segundo momento calcula-se a função de Euler $\phi(n) = (p-1)(q-1)$, com $n = p \cdot q$, que será utilizada para encontrar o parâmetro e que junto a n formam a chave de codificação (n, e) e o parâmetro d que junto a n formam a chave de decodificação (n, d).

Este trabalho tem por objetivo desenvolver uma descrição do método de criptografia RSA, isto é, mostrar como obter os parâmetros e e d utilizados no processo de codificação e decodificação, como trabalhar uma mensagem no processo de codificação e decodificação, mostrando como o receptor recebe a mensagem codificada, e o que torna o método RSA tão seguro.

Referências

[1] S. C. Coutinho, Números Inteiros e Criptografia RSA, IMPA/SBM. Rio de Janeiro: 2000.

[2] E. Alencar Filho, Teoria Elementar dos Números, 2. ed. São Paulo: Nobel, 1985.

[3] E. G. Pimentel, Teoria dos Números e o RSA, 2006. Disponível em: <http://www.mat.ufmg.br/OBMEP/criptografia.pdf >. Acesso em: 15 abr. 2008.