I Encontro Acadêmico de Modelagem Computacional do LNCC
Petrópolis, Rio de Janeiro, Brasil
10–11 de Março de 2008

Motivando o Estudo da Matemática através da Criptografia

Fábio Borges,
LNCC, Petrópolis, RJ
E-mail: borges@lncc.br

Muitas áreas da Matemática são conhecidas como árduas e sem aplicações, um exemplo, é a Teoria dos Números. Em geral as aplicações se encontram após um profundo estudo, tornando difícil a compreensão de quem está no começo de uma longa caminhada. Experimente perguntar a um estudante para que servem os números primos. Tais números são importantíssimos para o RSA, método criptográfico amplamente usado na Internet.

Uma bela aplicação de números complexos está na descrição de um fluido irrotacional e incompressível, no entanto, não é possível explicar tal aplicação a alunos do ensino médio, nem mesmo em algumas graduações, pois requer um grande conhecimento de Análise. Na Criptografia é diferente, existem aplicações para várias áreas e níveis de conhecimento, logo as aplicações podem partir do conteúdo do ensino fundamental e chegarem aos maiores problemas da atualidade.

O objetivo básico da Criptografia é transmitir uma mensagem a um destinatário sem que outra pessoa possa compreender seu conteúdo. Para uma criança podemos ensinar um método por substituição, já um pós-doutorando pode tentar provar a Hipótese de Riemann que afirma que as raízes interessantes de

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

estão em $\mathscr{R}(s) = 1/2$. Esta conjectura tem forte relação com a distribuição dos números primos e conseqüentemente grande impacto nos métodos de Criptografia. Atualmente existe um premio de um milhão de dólares para quem demonstrá-la, sendo um dos sete Problemas do Milênio. Outro Problema do Milênio fortemente vinculado a Criptografia é uma questão de complexidade computacional, o famoso P versus NP, ou seja, determinar se todos os algoritmos não determinísticos podem ser resolvidos deterministicamente em tempo polinomial. Podemos facilmente fazer um algoritmo que encontre os fatores de $n = p \times q$. Mas como encontrar os primos p e q em tempo polinomial? O produto nos números naturais é ensinado junto com o processo de alfabetização, no entanto os alunos de graduação se espantam quando são questionados pela operação inversa, isto é, dado n encontre um fator primo.

Além de ter amplo potencial para enriquecer o ensino de Matemática, a Criptografia desperta grande interesse por estar lindando com segurança, seja de um e-mail pessoal ou das transações financeiras de uma grande instituição. Isto desperta a curiosidade e aguça a imaginação dos estudantes.

A experiência com alunos no curso de graduação em computação tem sido muito satisfatória, tendo-se conseguido inserir até noções de álgebra abstrata, para respondermos as questões dos alunos. Perguntas do tipo: Por que é inseguro? Por que é seguro? Incondicionalmente seguro?

O ensino da Criptografia tem demonstrado ser um facilitador da compreensão da Matemática em virtude das aplicações em segurança da informação.

Keywords: *Criptografia, Ensino, Matemática*