RESOLUÇÃO DO PROBLEMA DE DECODIFICAÇÃO DE MENSAGENS VIA PROBLEMA DA MOCHILA

Pedro Henrique Gomes Machado
Escola Nacional de Ciências Estatísticas
Rua André Cavalcanti, 106 - Santa Tereza, Rio de Janeiro - RJ
machado.gomesph@gmail.com

José André de Moura Brito
Escola Nacional de Ciências Estatísticas
Rua André Cavalcanti, 106 - Santa Tereza, Rio de Janeiro - RJ
jambrito@gmail.com

Juscelino Bezerra dos Santos
Escola Nacional de Ciências Estatísticas
Rua André Cavalcanti, 106 - Santa Tereza, Rio de Janeiro - RJ
jotalino@gmail.com

RESUMO

O presente trabalho propõe um estudo concernente à aplicação de métodos matemáticos e computacionais para abordar o problema de decodificação de mensagens via problema da mochila.

A necessidade de dar segurança à informação é algo disseminado há muito tempo. Mais especificamente, existem registros que remontam ao Egito Antigo, 1900 AC. O procedimento que propicia a segurança dos dados foi evoluindo e ficou conhecido como criptografia. A criptografia agrega um conjunto de princípios e técnicas que transformam as informações, ou seja, mensagens transmitidas via internet por bancos ou grandes corporações, por exemplo, de um formato original em um formato indecifrável. Ela trabalha com segredos denominados chaves, e é dividida em dois sistemas, sendo um desses sistemas denominado criptografia de chave pública. Esse sistema foi criado por Diffie e Hellman e posteriormente foi desenvolvido por pesquisadores gerando o algoritmo RSA. Esse sistema trabalha com duas chaves, uma (pública) que é amplamente divulgada e outra (privada) que fica sob o domínio do proprietário, assim como outras necessidades que permitem o processo de codificação (cifragem) e decodificação (decifragem).

Observa-se que o problema de decodificação por ser mapeado em um problema clássico da área de otimização combinatória, qual seja, o problema da mochila. Dessa forma, o entendimento e o equacionamento do problema de decodificação estão diretamente associados ao estudo de conceitos de pesquisa operacional e de aritmética modular. Particularmente, no que diz respeito à aritmética modular, foi estudada toda a parte de congruência e o conceito de inverso multiplicativo.

A partir do estudo desses conceitos e do estudo do problema de criptografia, foi desenvolvido um conjunto de funções em linguagem ***R***. Essas funções permitem a simulação de um sistema de criptografia de chave pública e a aplicação dos procedimentos de codificação e decodificação no mesmo, mediante a aplicação de três métodos, sejam eles: um de enumeração exaustiva, um de enumeração implícita (aplicação de uma formulação de programação inteira) e um que trabalha com a subtração dos parâmetros adequados até achar a solução.

Os três métodos citados acima foram aplicados em algumas instâncias, ou seja, mensagens com as suas respectivas chaves, sendo os resultados desses métodos apresentados neste trabalho.

PALAVRAS CHAVE: Criptografia, Problema da mochila, Aritmética modular.