Laboratório de Criptografia Simétrica, Algoritmo RSA

Cícero Alves da Silva[1], Fladson Thiago Oliveira Gomes[1]

[1]Departamento de Ciências Exatas e Aplicadas
Universidade Federal do Rio Grande do Norte (UFRN) – Caicó, RN – Brasil

cicerojprn@gmail.com, fladsonthiago@gmail.com

1. Escolhas quanto ao tamanho das chaves *p* e *q*

Após muitos testes com os tamanhos das chaves *'p'* e *'q'*, podemos perceber que se as mesmas possuírem um valor primo muito baixo, fica muito fácil para um invasor descobrir, a um baixo custo, qual a chave privada do usuário, que no caso é *'d'* por meio do processo de fatoração de '*N'* e depois descobrindo as chaves *'p'* e *'q'*. Porém, no caso de os números primos escolhidos serem muito altos o algoritmo leva muito tempo para realizar os cálculos de exponenciação modular, pois esse cálculo exige um poder de processamento grande, dependendo da forma como é realizada.

A solução encontrada para esse problema foi limitar o valor máximo das chaves *'p'* e *'q'* geradas, para um valor aceitável de cálculo da exponenciação modular e trocar a forma que estava sendo realizado esse cálculo para uma forma mais eficiente. O método escolhido foi o "*Exponenciação Modular: Repetead Squaring*" [1], com essa mudança o processo de decriptação teve o tempo reduzido ao ponto de ser aceitável ao usuário e inviável para o invasor realizar o processo de fatoração de *'N'*.

Mas por motivos que desconheço esse método ainda não fez o procedimento a um tempo aceitável, peço desculpas ao professor, mas acredito que tenha valido pela tentativa.

[1] http://www.usna.edu/Users/math/wdj/book/node27.html