DESENVOLVIMENTO DE UM SISTEMA DE CRIPTOGRAFIA EM LINGUAGEM DE PROGRAMAÇÃO C BASEADO NO MODELO RSA (APOIO UNIP)

Aluno: Leandro Persona

Orientador: Prof. Avelino Palma Pimenta Junior

Curso: Ciência da Computação

***Campus*:** Ribeirão Preto

O objetivo deste estudo foi o desenvolvimento de um sistema de criptografia baseado no modelo RSA (Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman), utilizando a linguagem de programação C. Com foco voltado para rotinas otimizadas em grande parte por aritmética inteira foi possível desenvolver todo o sistema de forma eficiente e eficaz, garantindo segurança e ao mesmo tempo estabilidade. Uma cadeia de caracteres foi submetida ao processo de criptografia para posterior envio em um canal de comunicação inseguro (internet) e o resultado foi muito significativo visto que o processo é instantâneo, independente do tamanho da chave. O grande diferencial dessa técnica de criptografia consiste na dificuldade da fatoração de grandes números pelos atuais processadores e o fato de a chave privada não precisar se deslocar do receptor até o emissor da mensagem. O principal conceito envolvendo a resolução do problema foi a utilização de rotinas com exponenciação modular garantindo que, apesar de toda a limitação da linguagem escolhida, fosse possível criptografar as informações. Desta forma, conclui-se que o algoritmo de criptografia RSA justifica seu uso em grande parte na grande rede mundial de computadores, principalmente por sua facilidade na implementação e por ser praticamente inviável atualmente um ataque para se quebrar a chave privada.