ANALISE DE DESEMPENHO DO MÉTODO RSA

SILVA, Jonas Forte[1] (jonas.f.forte@gmail.com); **MOLGORA, Adriana Betânia de Paula**[2] (adrianamolgora@gmail.com);

[1] Discente do curso de Ciência da Computação da UEMS – Dourados; PIBEX/UEMS;
[2] Docente do curso de Ciência da Computação da UEMS – Dourados;

Dada a evolução das civilizações humanas, tornou-se cada vez maior a importância de segurança nos processos de envio e recebimento de informações. Com a entrada da era da informação, por volta da década de 50, e impulsionada pelas disputas da Segunda Guerra Mundial, a criptografia se destacou como uma arte de cifrar e decifrar dados em um meio computacional. Através de muitas pesquisas, diversos métodos criptográficos foram criados e, dentre eles o RSA. O método RSA se destaca por sua eficiência e trivial praticidade. Esse método consiste em um algoritmo criptográfico que é considerado uma das melhores escolhas para a implementação de sistemas de chaves assimétricas. O algoritmo RSA baseia sua segurança na dificuldade de fatoração de números primos gigantes, sendo essa, a solução mais válida para ataques ao método. Esse método é muito utilizado em diversos ramos e de diversas maneiras como, por exemplo, em servidores de e-mail e compras online. Nesse trabalho foi realizada uma implementação de uma versão básica deste algoritmo, levando em consideração os passos matemáticos fundamentais para a execução do mesmo. Também foram realizadas medições de fatores de desempenho na execução do algoritmo, como o consumo de memória e os tempos de execução com tamanhos variados de informação e execução com diferentes tamanhos de chaves (públicas e privadas). Para a implementação, foram utilizadas bibliotecas computacionais, que auxiliam a manipulação de números inteiros gigantes e medições de tempo e memória no período de execução. Após o período de testes foi obtida uma grande quantidade de dados, que originaram tabelas e gráficos relacionados ao desempenho do método estudado. Por meio desses testes foram constatadas a eficácia e segurança oferecida pelo método, tendo uma grande usabilidade nesta implementação para proteção de arquivos dentro de um sistema operacional. Todos os testes e implementações do método foram realizados em um sistema operacional Linux, em linguagem de programação C.

Palavra-chave: Criptografia, RSA, Chave-Assimétrica.

Agradecimentos: Ao Programa Institucional de Bolsas de Extensão PIBEX, vinculado à Pró- reitoria de Extensão, Cultura e Assuntos Comunitários - PROEC/UEMS pela concessão de bolsa de extensão e a minha orientadora Adriana Betânia de Paula Molgora.