ESTUDO DO MÉTODO ECM EM COORDENADAS AFINS

MATTOS, Leandro Barra de[1] (leanmattos93@gmail.com); **MOLGORA, Adriana Betânia de Paula**[2] (adrianamolgora@gmail.com);

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

A segurança de vários sistemas criptográficos como o RSA só é garantida graças a não descoberta de um método que fatore números inteiros extremamente grandes. Sendo assim, várias pesquisas têm sido feitas na procura de uma solução eficiente. O método ECM em coordenadas afins vem se mostrando uma ótima solução, pois apesar de não ser o mais rápido, consegue fatoras números grandes de forma eficiente. O objetivo desse trabalho é o entendimento do método ECM em coordenadas afins e o estudo de algoritmos para esse fim. Os estudos foram conduzidos na Universidade Estadual de Mato Grosso do Sul, Unidade Universitária de Dourados (UEMS/UUD), através da revisão bibliográfica em artigos, sites e livros que abordavam as pesquisas mais recentes sobre o método ECM em coordenadas afins, bem como os algoritmos que o implementam, posteriormente foi realizado a implementação dos algoritmos e testes e pôr fim a análise dos resultados e documentação. Com o estudo foi possível compreender que o processo de fatoração pelo método ECM envolve aspectos teóricos e computacionais. Teoricamente, para fatorar um inteiro dado, o método se utiliza de operações em curvas elípticas como a adição e duplicação de pontos na curva. Com as pesquisas foi possível descobrir um novo método pouco explorado que se utiliza do método ECM, mas em uma curva chamada de Edwards. Os algoritmos foram desenvolvidos na linguagem C++ e os testes realizados em um Laptop da Acer modelo Aspire 5 (A515-51G-5536), que possui um processador Intel Core i5 de 2.5 GHz e 8 GB de memória DDR4. Nos testes foi possível observar que o tempo necessário para encontrar um fator depende quase inteiramente do tamanho do fator a ser encontrado e muito pouco sobre o tamanho do número em si. Foi possível concluir que muitas melhorias ainda podem ser feitas para aumentar a eficiência dos algoritmos que o implementam, visto que com o passar do tempo houve um aperfeiçoamento tanto do hardware quanto do software e descobrir essas melhorias é uma tarefa árdua, mais não impossível. No entanto, entender procedimentos e teorias empregados nesse contexto não é uma tarefa trivial.

Palavras-chave: ECM, curvas elípticas, criptografia, segurança.

Agradecimentos: **Ao Programa Institucional de Iniciação Científica da Universidade Estadual de Mato Grosso do Sul (PIC/UEMS) pela concessão de bolsa de iniciação científica ao autor.**