ENEPEX
ENCONTRO DE ENSINO, PESQUISA E EXTENSÃO
13º ENEPE UFGD - 10º EPEX UEMS
PESQUISA E TECNOLOGIA: AÇÕES PARA UM FUTURO SUSTENTÁVEL

CURVAS ADEQUADAS AO MÉTODO DAS CURVAS ELÍPTICAS

OLIVEIRA, Eduardo Maximiano de [1] (eduardomaxoliveira@gmail.com); **MOLGORA, Adriana Betânia de Paula**[2] (adrianamolgora@gmail.com)

[1]Discente do curso Ciência da Computação da UEMS - Dourados;
[2]Docente do curso Ciência da Computação da UEMS - Dourados;

A fatoração de inteiros é um problema em aberto para o qual ainda não foi encontrado um método eficiente que fatore números inteiros extremamente grandes. Esse problema de fatoração garante a segurança de alguns criptossistemas, como o RSA. Entre os diversos métodos de fatoração, existe o método ECM que é um dos mais importantes. O método das curvas elípticas utiliza a estrutura de grupo dos pontos de uma curva elíptica para encontrar um fator de um número inteiro dado, ou seja, durante o processo de fatoração, uma curva elíptica é escolhida e através dela realiza-se a tentativa de fatoração. O objetivo desta iniciação foi pesquisar os tipos de curvas elípticas existentes e ver quais curvas podem ser usadas para melhorar o desempenho do método ECM. A primeira curva estudada é a de Weierstrass que é definida pela seguinte equação $y^2 = x^3 + ax + b$, onde $4a^3 + 27b^2 \neq 0$, está é curva usada no método ECM. Uma desvantagem nas curvas de Weierstrass é que em certo ponto do cálculo os denominadores de λ, dados por $x_2 - x_1$ e $2y_1$, sejam invertíveis e isso tem um custo. Esse problema não acontece com a próxima curva conhecida como curvas de Edward, definida sobre um campo K $\neq 2$ com a equação $x^2 + y^2 = 1 + dx^2y^2$, pois pode se usar coordenadas projetivas para homogeneizar a equação da curva e com isso evitar inversões na fórmula de adição. A última curva estudada foi a de Montgomery definida pela equação $By^2 = x^3 + Ax^2 + x$, com $A, B \in K$, $B \neq 0$ e $A \neq \pm 2$, que também usa coordenadas projetivas em sua fórmula de adição e é livre de inversão. Também podemos definir um método de adição de tal forma que nós não precisamos computar um MDC toda vez que calcular a soma de dois pontos, evitando cálculos desnecessários. No final as curvas de Edward fornecem um desempenho superior, pois podem fornecer uma fórmula de adição mais rápida.

Palavras-chave: Fatoração, ECM, criptografia.

Agradecimentos: A Universidade Estadual de Mato Grosso do Sul (UEMS) pela concessão de bolsa de iniciação científica ao primeiro autor.