CRIPTOGRAFIA DE CURVAS ELÍPTICAS – ANÁLISE DE DESEMPENHO

SALAZAR, Douglas Correia[1] (douglassalazar_dcs@hotmail.com); **MOLGORA, Adriana Betânia de Paula**[2] (adrianamolgora@gmail.com);

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

A criptografia pode ser definida por um conjunto de técnicas ou métodos que visam proteger as informações. Os métodos criptográficos devem garantir que pessoas não autorizadas não tenham acesso à informação de forma que o conteúdo não seja alterado. Além disso, devem garantir a identidade do emissor e impedir que ocorra negação do envio/recepção da informação. Atualmente existem diversos métodos de criptografia, porém esses métodos podem ser classificados em duas classes de criptografia: a criptografia simétrica e a criptografia assimétrica. A primeira é também denominada criptografia de chave privada e a segunda de criptografia de chave pública. Como exemplo temos o ECC (criptografia de curvas elípticas) e o RSA caracterizados como assimétricos e o AES (advanced encryption standard) caracterizado como simétrico. O método criptográfico ECC se utiliza das propriedades da adição de pontos em curvas elípticas para realizar os processos de codificação e decodificação de dados. Entender o funcionamento desse método não é uma tarefa trivial, pois demanda o estudo de conceitos de teoria dos números, curvas elípticas e dos algoritmos envolvidos em seu funcionamento. Este projeto teve como intuito desenvolver durante o período da bolsa PIBIC, um estudo teórico e prático do método ECC detalhando os processos de codificação de decodificação de dados, analisar o desempenho da implementação em meio computacional, a partir de tempo de codificação de decodificação de dados e detalhar os dados obtidos. Após o término da implementação, foram realizados testes utilizando três tipos de curvas elípticas, M-221, M-511 e secp256k1 para diversos arquivos de texto que variavam em tamanho obtendo assim o tempo de execução, com isso a curva M-221 conseguiu o menor tempo de execução. Dessa forma, foi possível observar a importância da escolha da curva em relação a velocidade de criptografia, um obstáculo muito grande quando se trata de segurança de informações e velocidade. O desenvolvimento desse projeto também possibilitou o aprofundamento e aquisição de novos conhecimentos relacionados à criptografia de dados.

PALAVRAS-CHAVE: Criptografia, Curva Elíptica, ECC.

AGRADECIMENTOS: À Professora Adriana Betânia de Paula Molgora que acompanhou todo o projeto, o Programa Institucional de Bolsas de Iniciação Cientifica PIBIC pela concessão de bolsa de Iniciação Cientifica e ao CNPq, FUNDECT, UEMS.