ENEPEX
ENCONTRO DE ENSINO, PESQUISA E EXTENSÃO
9° ENEPE UFGD • 6° EPEX UEMS

UM ESTUDO SOBRE O MÉTODO CRIPTOGRÁFICO ECC

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

[1] Aluno do curso de ciência da computação – UEMS.

[2] Professora do curso de ciência da computação – UEMS

O projeto de iniciação científica, possibilita que o aluno participante desenvolva um conteúdo estritamente ligado ao seu curso, porém que inicialmente não está presente na grade curricular de seu curso. Na área da computação a pesquisa científica tem papel fundamental para a evolução tecnológica e produção de uma documentação relacionada à pesquisa desenvolvida.

Juntamente a professora Adriana Betânia de Paula Molgora, foi desenvolvido uma pesquisa relacionada aos conceitos matemáticos e computacionais referentes à criptografia desenvolvida com base em curvas elípticas. A criptografia pode ser definida como a arte de codificar e decodificar uma mensagem. A muito tempo o homem sente a necessidade do sigilo de informações, desde então muitos métodos de criptografia foram desenvolvidos para auxiliar este sigilo. Entre os métodos encontra-se a criptografia baseada nas curvas elípticas e esse será o método desenvolvido e estudado neste trabalho.

A criptografia baseada nas curvas elípticas, é uma técnica de criptografia de chave pública ou assimétrica, primeiramente proposta por Victor Miller e Neal Koblitz em 1985. Tornou-se uma atraente técnica criptográfica pelo fato de seus criadores assegurarem que o método consegue obter o mesmo nível de segurança com chaves consideravelmente menores.

Foram realizados estudos matemáticos dos seguintes conteúdos: Números Primos, Unicidade da fatoração, Divisibilidade, Máximo divisor comum, Inteiros Módulo n, Grupos, Subgrupos, Corpo, Anéis e também houve um estudo sobre curvas elípticas e algumas aplicações na criptografia. Foi realizado também a implementação de um programa em linguagem C, no qual é exemplificado o processo de criptografia pelo método estudado.

Palavras-Chave: Curvas elípticas, Criptografia de dados, Linguagem C.