2º Encontro da SBPC em MS/
XI ENEPEX / XIX ENEPE/
22ª SNCT - UEMS / UFGD 2025

TÍTULO: NÚMEROS PRIMOS E A CRIPTOGRAFIA RSA.

Instituição: UEMS – Câmpus de Nova Andradina

Área temática: Pesquisa – Ciências Exatas e da Terra

SILVA, Gleison Franklin Mendes[1] (gleisondasilva8@gmail.com); **PAVANI,** Gustavo Antonio[2] (gustavo.pavani@uems.br).

[1] – Bolsista de Iniciação Científica FUNDECT e discente do Curso de Matemática do Câmpus de Nova Andradina;
[2] – Orientador e Professor do Curso de Matemática do Câmpus de Nova Andradina.

Os números primos são um dos tópicos mais básicos de estudo no ramo da matemática chamado Teoria dos Números. Números primos são números que só podem ser divididos igualmente por eles mesmos e por 1. Uma das razões pelas quais os números primos são importantes na teoria dos números é que eles são, em certo sentido, os blocos de construção dos números naturais. De fato, O Teorema Fundamental da Aritmética afirma que qualquer número natural, maior que um, pode ser fatorado de forma única em um produto de primos. Os números primos também formam a base da criptografia RSA. Este código foi inventado em 1978 por R. L. Rivest, A. Shamir e L. Adleman, que na época trabalhavam em Massachuts Institute of Technology (M.I.T). As letras RSA correspondem às iniciais dos inventores do código. Neste método de criptografia, amplamente utilizado na criptografia de dados de e-mail e outras transações digitais atualmente, os dados são criptografados usando números primos. Assim, pessoas indesejadas são impedidas de acessar os dados. Nesse método, onde o produto de dois números primos grandes é usado como chave de criptografia, os números primos selecionados permanecem ocultos e somente a pessoa que conhece os números primos que são os fatores dessa chave pode descriptografá-la. Como é difícil fatorar números grandes em primos, o método de criptografia RSA usa tantos números primos quanto possível, aumentando assim a segurança da criptografia. Nosso objetivo nesse projeto é estudar os números primos e suas propriedades, bem como aplicá-los no estudo da criptografia RSA. Para isso, foi necessário o estudo rigoroso e aprofundado dos seguintes tópicos: algoritmos fundamentais: algoritmo da divisão e algoritmo euclidiano; fatoração única: existência da fatoração única, fatoração de Fermat, propriedades dos números primos (infinidade dos primos e crivo de Eratóstenes) e números irracionais; aritmética modular: inteiros módulo n, critérios de divisibilidade, potências, equações diofantinas, pequeno Teorema de Fermat e sistemas de congruências. Também estudamos a Teoria de Grupos, como grupos de simetrias, grupos aritméticos, subgrupos e o Teorema de Lagrange e por fim aplicamos todos esses conceitos para o desenvolvimentos de algoritmos de criptografia RSA. Além disso, esse projeto busca suprir algumas fragilidades da grade curricular do curso de licenciatura em Matemática de Nova Andradina, o qual não contempla a disciplina de Teoria dos Números. A metodologia utilizada é a pesquisa na literatura especializada e a elaboração de algoritmos computacionais. Como resultado esperamos adquirir conhecimento matemático sólido na área de Teoria dos Números, possibilitando assim, a qualificação para pesquisas mais avançadas, como futuramente, a realização de um curso de mestrado ou doutorado. Conclusão: a criptografia de dados é importante porque ajuda a proteger a privacidade das pessoas e protege os dados contra invasores e outras ameaças à segurança cibernética para organizações como saúde, educação, finanças, bancos e varejo. Mostramos também que toda a teoria da criptografia RSA baseia-se, essencialmente, na Teoria dos Números primos.

PALAVRAS-CHAVE: Números primos, aritmética modular, criptografia RSA.

AGRADECIMENTOS: Agradecemos à FUNDECT pela Bolsa de Iniciação Científica.