V Seminário de Pesquisa, Inovação e Pós-Graduação
22ª Semana Nacional de Ciência e Tecnologia
04 a 13 de novembro
Iniciação Científica

A CRIPTOGRAFIA RSA E SEUS FUNDAMENTOS MATEMÁTICOS

V Seminário de Pesquisa, Inovação e Pós-Graduação da Universidade Federal de Uberlândia (Iniciação Científica), 1ª edição, de 04/11/2025 a 13/11/2025
ISBN dos Anais: 978-65-5465-171-4

SANTOS; Rafael Luiz Gonçalves dos [1], SILVA; Mateus Teixeira [2]

RESUMO

Este estudo aborda a aplicação da teoria dos números na criptografia, com foco no algoritmo RSA, cuja segurança reside na dificuldade computacional de fatorar números primos gigantes. O objetivo principal é dominar conceitos matemáticos fundamentais, como divisibilidade, primos e congruências, e conectá-los à prática através da implementação do RSA em Python. Adicionalmente, o trabalho propõe uma introdução à criptografia pós-quântica, como o método CRYSTALS-Kyber, essencial diante da ameaça que a computação quântica representa ao RSA. O estudo detalhou as etapas de implementação (geração de chaves, cifragem e decifragem), revisando seus fundamentos matemáticos e utilizando Python para a aplicação prática. Como principal resultado, foi desenvolvida uma criptografia RSA funcional e validada, o que consolidou o aprendizado da teoria e sua aplicação na segurança de dados. O projeto proporcionou também um entendimento inicial sobre os desafios da criptografia pós-quântica. Dessa forma, o trabalho cumpriu seus objetivos ao integrar com sucesso teoria e prática, reforçando a relevância destes conhecimentos para a segurança digital atual e futura.

PALAVRAS-CHAVE: RSA, Criptografia, Teoria dos números, Matemática, Python, Codificação

[1] Universidade Federal de Uberlândia, rlg.santos123@gmail.com
[2] Universidade Federal de Uberlândia, mateusteixeira1512@ufu.br