Matemática - BIC JÚNIOR

Introdução à criptografia RSA

Iara Ferreira Canestri - Bolsista do programa BIC-Jr UFLA

Marlon Pimenta Fonseca - Orientador DMM-UFLA - Orientador(a)

Resumo

A criptografia estuda os métodos de codificar uma mensagem de tal forma que apenas o destinatário consiga decodificá-la, gerando assim uma segurança na troca de mensagens. Desde os tempos antigos muitas formas de codificar mensagens foram criadas. Contudo, com o advento da computação e da internet, houve necessidade de uma melhoria nos métodos de criptografia. Neste contexto, Rivest, Shamir e Adleman desenvolveram um método de criptografia, chamado criptografia RSA, utilizando a teoria dos números inteiros. Na criptografia RSA, a mensagem é codificada a partir de uma chave pública, e decodificada por meio de uma chave privada, que deve ser mantida escondida. A chave pública e privada são, respectivamente, um número inteiro n e o par (d, n), onde n é o produto de dois primos, p e q, e satisfazem determinadas relações. A segurança da criptografia RSA se baseia no fato de que para obter a chave privada a partir da pública é necessário fatorar o número natural n, contudo se os primos p e q foram escolhidos de forma adequada, a fatoração de n se torna praticamente impossível. Neste trabalho visamos responder a seguinte pergunta: Como e porque a criptografia RSA funciona? Para responder tal questionamento desenvolvemos alguns conceitos matemáticos, como relação de equivalência, congruência entre números inteiros e aritmética modular, além de alguns resultados necessários, como o Pequeno Teorema de Fermat e o Teorema Chinês dos Restos. Também procuramos entender o quão segura é essa criptografia, ou seja, o quão difícil pode ser fatorar um número inteiro. Deste modo, estudamos dois algoritmos para encontrar a fatoração de um número composto, o algoritmo simples e o de Fermat, e também estudamos o crivo de Eratóstenes, o qual determina todos os números primos menores que um inteiro qualquer.

Palavras-Chave: Matemática, Teoria do números, criptografia.
Instituição de Fomento: FAPEMIG

Link do pitch: https://www.youtube.com/watch?v=AwLHbxyhwP0