Matemática

CRIPTOGRAFIA RSA

Priscilla Nádia Aparecida Ferreira - 6º módulo de Matemática, UFLA, iniciação científica voluntária.

José Alves Oliveira - Orientador DMM, UFLA. - Orientador(a)

Resumo

A criptografia RSA é um dos métodos atuais mais conhecidos e utilizados de criptografia de chave pública. Foi inventado em 1977 pelos criptográficos R. L. Rivest, A. Shamir e L. Adleman, e as letras RSA correspondem às iniciais dos nomes dos inventores (Rivest - Shamir - Adleman). Basicamente, são utilizados os estudos dos conceitos matemáticos, onde destacam-se os números inteiros, que representam um importante papel na criptografia RSA, além dos critérios de fatoração e divisibilidade, os números primos, o MDC, a aritmética modular, onde inclui os métodos de congruências. Utilizamos assim, conceitos da teoria dos números para explicar a criptografia na codificação e decodificação de mensagens, de modo que somente o destinatário autêntico da mensagem consiga interpretá-la. Inicialmente, podemos implementar este conceito simplesmente escolhendo dois números primos p e q grandes e distintos, e o produto deles resultará em um número n. Para codificar uma mensagem, utilizamos o n, para decodificar os números primos p e q, onde n pode-se tornar público, mas p e q não. Para decodificar o RSA, simplesmente consiste em fatorar o n, com o intuito de chegar em p e q, porém, se n for muito grande, este processo levaria muito tempo. Como é um método amplamente utilizado e muito conhecido, seu estudo resulta nos objetivos de entender tais processos de codificação e decodificação de uma determinada mensagem, e como estamos tratando de métodos matemáticos, como a fatoração de n, trata-se de um estudo amplo, onde demanda conceitos de várias áreas da matemática para chegar no resultado final da decodificação do produto destes números, o que não é tão trivial. Na criptografia RSA, podemos concluir a importância dos estudos matemáticos para a resolução de diferentes problemas deste âmbito. O modelo RSA, que tem como base o conjunto dos números inteiros e primos em sua explicação, possibilita o esclarecimento de codificação e decodificação de diferentes tipos de mensagens através dos estudos dos critérios de divisibilidade e de congruência, parte da aritmética modular. A base desta pesquisa foram estudos teóricos de materiais deste tema, além de demais estudos matemáticos como uma forma introdutória e preparatória para o entendimento do assunto a ser abordado.

Palavras-Chave: Criptografia RSA, números primos, teoria dos números.
Instituição de Fomento: Universidade Federal de Lavras

Link do pitch: https://www.youtube.com/watch?v=XoOE4tHocHk