Evento	Salão UFRGS 2022: SIC - XXXIV SALÃO DE INICIAÇÃO CIENTÍFICA DA UFRGS
Ano	2022
Local	Campus Centro - UFRGS
Título	Criptografia RSA
Autor	JEREMY ORTIZ MORETTO
Orientador	JOAO MATHEUS JURY GIRALDI

Introdução à criptografia: O método RSA

Bolsista: Jeremy Ortiz Moretto
Orientador: João Matheus Jury Giraldi
Instituição de origem: UFRGS

Uma vez que vivemos em um era digital e garantir a segurança e a privacidade das informações/dados compartilhados entre pessoas é de suma importância, surge a necessidade de estudar criptografia, seja elaborando ou melhorando os métodos já existentes para encriptar as informações digitais. Neste trabalho tivemos como objetivo estudar o método de criptografia RSA. Antes disto, tivemos de estudar/reforçar as noções de álgebra para melhor entender o método. Dentre elas, destacamos as definições e teoremas básicos da teoria algébrica dos números. Este estudo se deu principalmente através do livro *Números inteiros e criptografia RSA* de S. C. Coutinho. Dentre outras fontes de conteúdo que foram utilizadas, evidenciamos as aulas que constam no canal *Programa de Iniciação Cientifica da OBMEP* no YouTube. Durante o período da iniciação científica, não focamos apenas nos pré-requisitos para o método de criptografia estudado, mas também vimos diversos conteúdos da área de álgebra/informática relacionados à teoria algébrica dos números. Por exemplo, estudamos um pouco de teoria de grupos e também os algoritmos computacionais para fatoração em números primos que se encontram no livro *Prime numbers and computer methods for factorization* de H. Riesel. Ressaltamos que durante o período da iniciação científica, o bolsista desenvolveu a prática de estudar de forma autônoma, o que é indispensável para a pesquisa científica. O objetivo do vídeo é introduzir o método de criptografia RSA, com o foco em apresentar o método a estudantes que já estão familiarizados com resultados da teoria algébrica dos números, motivando-os ao estudo da álgebra e suas aplicações.