**Projeto Semestral**

**UC – Estruturas matemáticas**

**Tema Central:** **Criptografia e Teoria dos Números Aplicada ao Desenvolvimento de um Sistema Seguro**

**Introdução**

No mundo digital moderno, a segurança das informações é um dos pilares fundamentais para o funcionamento de diversas aplicações, desde simples trocas de mensagens até transações financeiras complexas. À medida que a tecnologia avança, também aumentam as ameaças e vulnerabilidades que colocam em risco a privacidade e a integridade dos dados. Nesse contexto, a criptografia surge como uma ferramenta essencial, capaz de proteger informações sensíveis contra acessos não autorizados.

A criptografia, em sua essência, é profundamente enraizada em conceitos matemáticos, especialmente na teoria dos números e nas estruturas algébricas. Técnicas criptográficas modernas, como o RSA e o AES, dependem de operações matemáticas complexas, como a fatoração de números primos, transformações lineares e a aritmética modular. Assim, compreender a matemática por trás desses algoritmos é crucial para qualquer profissional que deseje trabalhar com segurança da informação.

**Objetivo**

O objetivo do projeto é explorar a aplicação de conceitos de estruturas matemáticas na criação de algoritmos criptográficos e desenvolver um protótipo de sistema seguro que implemente esses algoritmos. Deve-se utilizar uma linguagem de programação para codificar os algoritmos, integrá-los em uma aplicação funcional, e testar sua eficiência e segurança.

**FICHA DE ACOMPANHAMENTO DO GRUPO**

**PROJETO SEMESTRAL**

**Turma:** [Estruturas matemáticas - presencial](https://classroom.google.com/c/NzA4NzQ2MzUyMDk0) / Ciência da Computação

**Campus:** Mooca

**Turno (Diurno/Noturno):** Noturno

|  |  |  |
| --- | --- | --- |
| **Passo** | **Nome completo** | **RA** |
| **1** | Andrey de Freitas Souza | 823217536 |
| **2** | Gabrielle Garcia Paz | 823126085 |
| **3** | Bianca Alves Ribeiro | 8222240261 |
| **4** | Bruno de Oliveira Santos | 823223513 |
| **5** | Webster Diógenes Rodrigues | 8222242764 |
| **6** |  |  |

**Tema do projeto**

Utilizar a aplicação de conceitos de estruturas matemáticas na criação de algoritmos criptográficos.

**Breve descrição do projeto**

Uso do RSA para o Conexão SSH remota nosso projeto iria criar servidor SSH e mostrar uma troca de comunicação com a autenticação do RSA, pretendemos utilizar a linguagem Python ou Java