Proyecto Matemáticas Discretas

Integrantes: Randy Rivera, Dhamar Quishpe e Hilda Angulo

Título: Gestor de Contraseñas Seguro con Cifrado RSA

Objetivo general

Desarrollar un gestor de contraseñas seguro utilizando el algoritmo RSA para cifrar y proteger las contraseñas almacenadas, asegurando que solo el usuario autorizado pueda acceder a ellas y validando la robustez del sistema mediante análisis de vulnerabilidades y ataques.

Objetivos específicos

- Crear una interfaz de usuario fácil de usar que permita a los usuarios almacenar, recuperar y gestionar sus contraseñas de forma eficiente y segura.
- Analizar cómo la selección de números primos grandes y pequeños afecta la seguridad y el rendimiento del algoritmo RSA realizando pruebas de seguridad, incluyendo simulaciones de ataques de brute forcing y otros métodos de explotación en busca de debilidades, tales como fallos en la generación de claves.
- Usar conocimientos de matemáticas discretas, investigar y comprender la teoría de números, así como los principios de divisibilidad, primalidad, análisis de algoritmos y el funcionamiento del algoritmo RSA.

Descripción

El proyecto consiste en crear una aplicación utilizando Python, de gestión de contraseñas que emplee el algoritmo RSA para cifrar y proteger las contraseñas almacenadas, garantizando un acceso restringido únicamente al usuario autorizado. La aplicación permitirá a los usuarios almacenar, recuperar y gestionar sus contraseñas de forma segura. Se abordarán conceptos como la divisibilidad, la primalidad, el teorema fundamental de la aritmética y la complejidad temporal y de recursos del algoritmo.

En la segunda parte del proyecto, se evaluará la resistencia del sistema a ataques como backdoor cuando modifica el algoritmo pseudorandom para generar primos no aleatorios, backdoor al generar números primos pequeños, brute forcing y otros ataques.