Programa de Cifrado Híbrido con AES y RSA

Chávez Ruíz Pedro

March 18, 2025

Objetivo

Desarrollar un sistema de cifrado híbrido basado en AES y RSA para proteger archivos de forma segura y eficiente. El programa tendrá una interfaz de línea de comandos sencilla y se desarrollará en un plazo de dos semanas.

Contexto

La seguridad de la información es crucial en ámbitos académicos, laborales y personales. Compartir archivos sin medidas adecuadas puede exponerlos a accesos no autorizados o manipulación malintencionada, especialmente en dispositivos públicos o compartidos.

Relevancia

El cifrado de archivos es fundamental para preservar la confidencialidad y autenticidad de la información. Este proyecto busca no solo brindar seguridad al usuario, sino también ilustrar de manera práctica el uso de algoritmos de cifrado simétrico y asimétrico de manera sencilla a través de la programación.

Justificación

En los últimos semestres de la carrera, he cursado diferentes materias que han abordado el tema del cifrado, su historia, evolución y aplicaciones. Sin embargo, estos temas han sido tratados de forma teórica, sin ir más allá de diapositivas o ejemplos ilustrativos. Debido a esto y a mi curiosidad por la seguridad informática,

surge la idea de aplicar estos conceptos en un entorno real mediante una implementación práctica, que a pesar de su sencillez, sea la base para un proyecto mas grande e importante que pueda aplicarse en diferentes situaciones.

Problema a Resolver

Se busca ofrecer una herramienta accesible para cifrar archivos con un enfoque práctico. Además, el proyecto sienta un primer paso hacia un sistema de autenticación basado en un cifrado híbrido que garantize mayor seguridad al acceder a archivos.

Usuarios

El programa está dirigido a personas con conocimientos básicos en línea de comandos y que requieren manejar archivos sensibles. También podría ser útil para entidades que buscan fortalecer la validación de identidad en sistemas digitales. Habiendo mencionado lo anterior, el sistema debe implementarse con buenas prácticas para evitar vulnerabilidades, como ataques de fuerza bruta o manipulación de claves. La correcta gestión de llaves y la protección contra accesos no autorizados son esenciales para garantizar la seguridad del programa.