CC3078 Cifrado de Información
Sección 11
Erick Stiv Junior Guerra Muñoz – 21781
Brandon Ronaldo Sicay Cumes -

Laboratorio 4 - Análisis y Diseño

Objetivos

Desarrollar una aplicación segura que permita a los usuarios registrarse y autenticarse mediante JWT (JSON Web Tokens), garantizando el almacenamiento seguro de contraseñas mediante técnicas de hashing. Una vez autenticados, los usuarios podrán firmar digitalmente archivos, eligiendo entre algoritmos criptográficos como ECC (Elliptic Curve Cryptography) o RSA, según sus necesidades de seguridad y rendimiento. Además, la aplicación asegurará la integridad de los archivos mediante hashes SHA-256, protegiéndolos contra modificaciones no autorizadas. Por último, los usuarios podrán acceder a archivos cifrados utilizando sus llaves privadas, implementando un sistema de cifrado asimétrico para garantizar la confidencialidad de los datos.

Alcance del proyecto

Funcionalidades principales: Registro e inicio de sesión. Los usuarios deberán registrarse con una combinación de correo y contraseña para poder acceder al sitio. Para asegurar la seguridad de la contraseña, esta estará encriptada a través de Hashing. Asimismo, la sesión se mantendrá a través de un JWT (Json Web Token), el cual contará con un tiempo de expiración de 1 hora para controlar el acceso de los usuarios.

Una vez dentro del sitio, el usuario podrá generar nuevas parejas de llaves públicas y privadas según lo solicite, así como acceder a un formulario para guardar un archivo (con opción de firmarlo si lo desea a partir de su llave primaria, seleccionando entre ECC o RSA para generar la firma). Podrá ver también el listado de archivos disponibles dentro del sitio (subidos por él mismo u otros usuarios) con opción de descargar el archivo que desee (junto con la llave pública del usuario que lo subió). Antes de descargar el archivo, se desplegará también la opción de validar la firma del archivo si se considera necesario.

Usuarios objetivo: Cualquier persona que desee transferir archivos a través del sitio, especialmente por su cuidado en seguridad y autenticación.

Tecnologías utilizadas:

Backend:

- Python
- Flask
- Pycryptodome

Frontend:

- React
- Javascript
- CSS
- HTML