****

**INGENIERIA EN DESARROLLO Y GESTION DE SOFTWARE**

****

**CIFRADO ESCÍTALA**

**ASIGNATURA:**

**SEGURIDAD INFORMÁTICA**

**ALUMNA:**

* **AVELINA HERNÁNDEZ HERNÁNDEZ 20210667**

**DOCENTE:**

**ING. ANA FELIPE REDONDO**

**HUEJUTLA, HIDALGO OCTUBRE 18 DEL 2023**

**Introducción**

La criptografía y el cifrado han desempeñado un papel fundamental en la seguridad de la información y la comunicación a lo largo de la historia. En un entorno de desarrollo, la seguridad de la información es una preocupación crucial, ya que el acceso no autorizado a datos confidenciales puede tener consecuencias graves. Los métodos de cifrado, como la Escítala y otros similares, desempeñan un papel fundamental en la protección de datos en tránsito y en reposo.

La Escítala pertenece al tipo de cifrado de transposición, que implica reorganizar los caracteres en un mensaje sin modificar su contenido. La Escítala es un cifrado de transposición vertical.

La importancia del cifrado en un entorno de desarrollo se basa en varios aspectos:

**Confidencialidad:** El cifrado protege la información sensible y confidencial de ser accedida por personas no autorizadas. En un entorno de desarrollo, esto es esencial para proteger datos como contraseñas, información financiera y otros datos sensibles.

**Integridad:** El cifrado también se utiliza para garantizar que los datos no se hayan modificado durante la transmisión o el almacenamiento. Esto ayuda a detectar cambios no autorizados en los datos.

**Autenticación:** El cifrado se utiliza en la autenticación de datos y usuarios, asegurando que los datos provengan de una fuente confiable y no de un atacante.

**Protección contra ataques:** Los ataques cibernéticos, como la interceptación de datos y el acceso no autorizado, son una amenaza constante en el desarrollo de software. El cifrado proporciona una defensa sólida contra estos ataques.

Otros Métodos Semejantes:

**Cifrado de la Columna:** En este método, se reorganizan las letras en columnas antes de leer el mensaje cifrado.

**Cifrado de la Ruta de Ferrocarril:** Este método implica escribir el mensaje en una forma de patrón de vías de ferrocarril antes de leerlo en un patrón específico.

**Cifrado de la Matriz:** En lugar de usar una varilla, este método utiliza una matriz de filas y columnas para organizar y leer el mensaje cifrado.

**Cifrado de la Grilla:** Se utiliza una cuadrícula para cifrar y descifrar el mensaje, similar a la Escítala.

**Desarrollo**

En nuestra clase, exploramos el cifrado de la Escítala realizando un Decágono y descifrando oraciones este tema fue abordado de manera integral Este método de cifrado se basa en la reorganización de las letras en un mensaje para ocultar su significado.

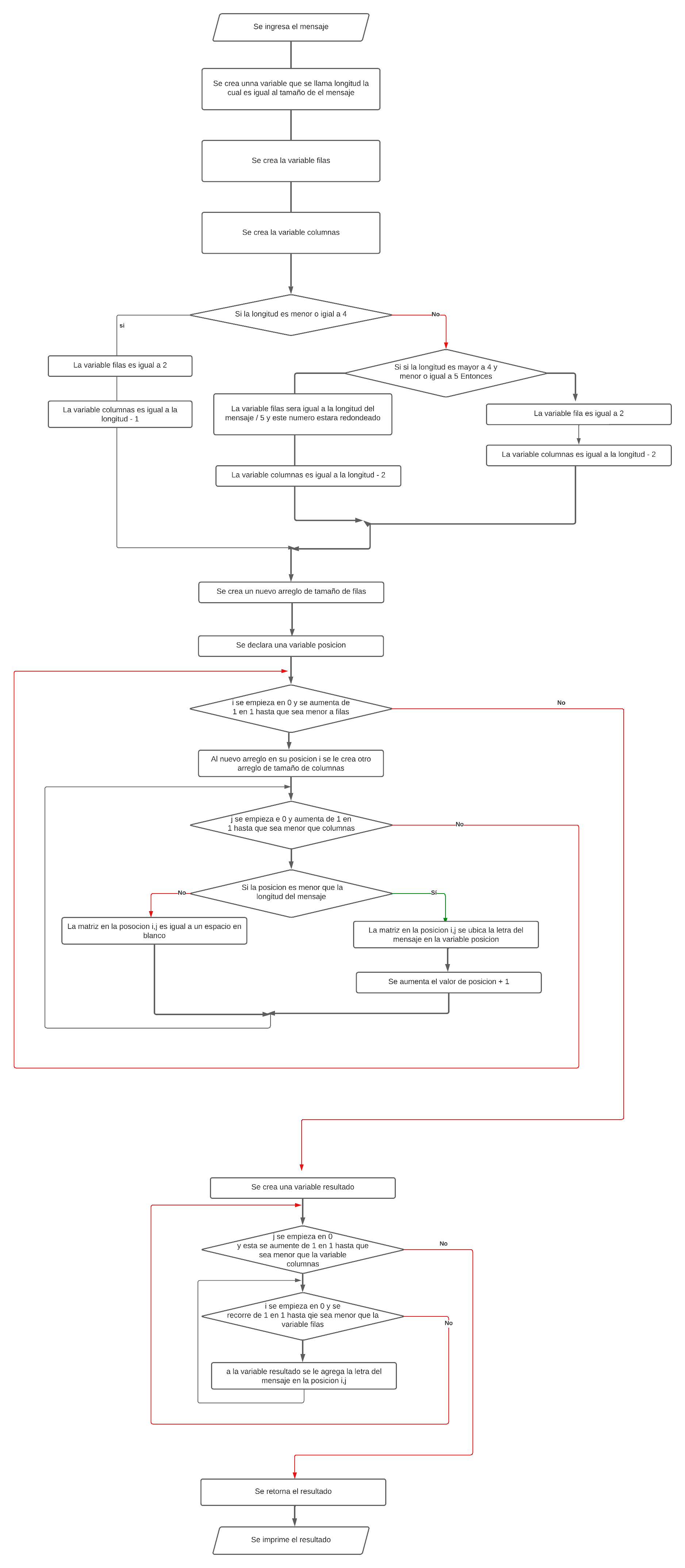
Esta actividad, se desarrolló en un programa que permite aplicar el cifrado Escítala. Para ello, utilizamos HTML para la estructura del programa, Bootstrap para crear un diseño sencillo y atractivo, y JavaScript para la lógica que cifra el texto de acuerdo con el algoritmo del cifrado Escítala.

## Cifrar y descifrar



**Repositorio: https://github.com/AvelinaHdez/CIFRADO\_TRANSPOSICION.git**

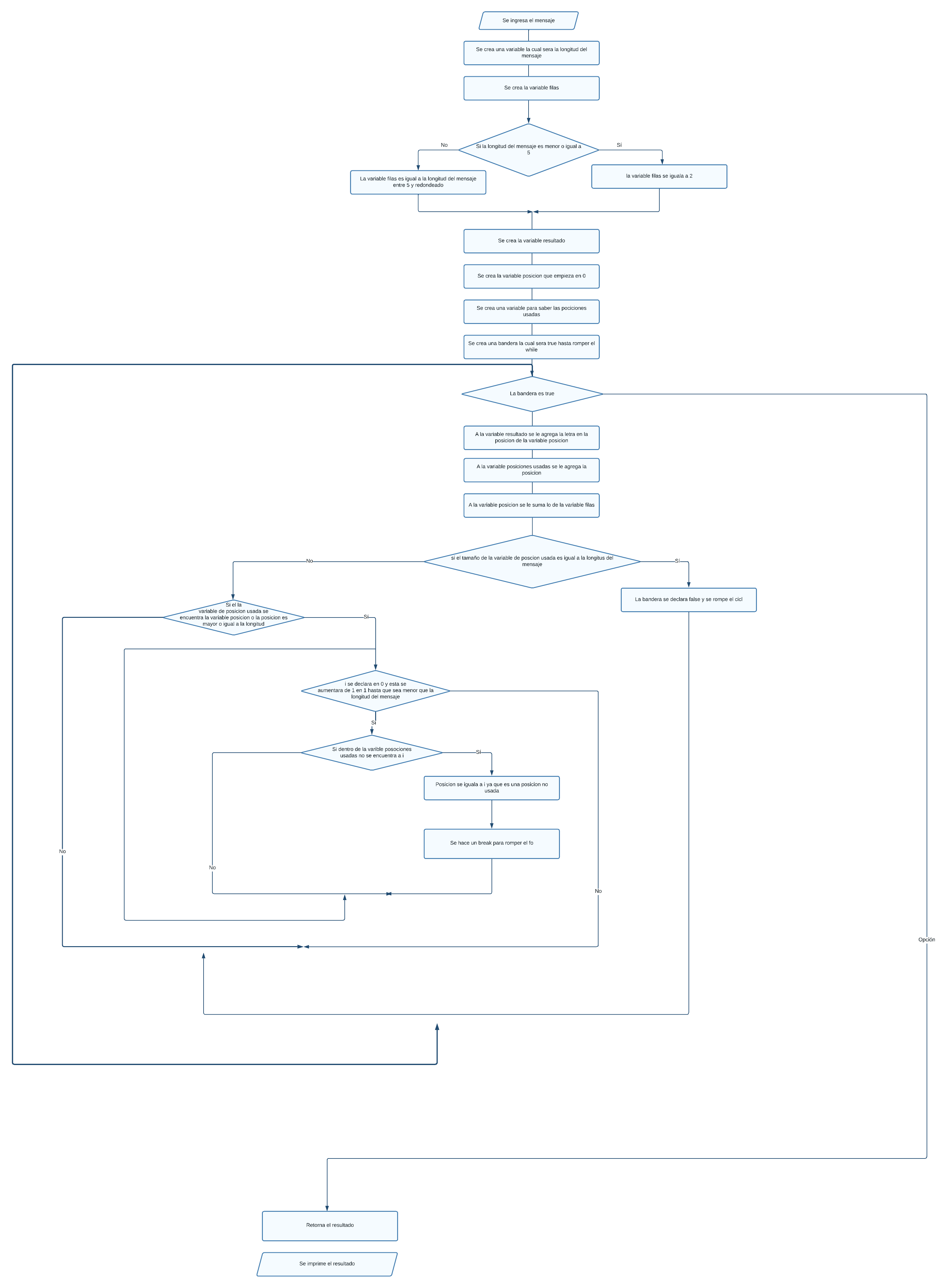
## Diagrama



Si

No

La variable columna es igual a 5



## Aplicación

La librería js-ktc: Es una herramienta fundamental en el contexto del cifrado por transposición en aplicaciones Vue.js. Proporciona una serie de módulos criptográficos que facilitan la implementación de técnicas de cifrado, incluyendo el cifrado por transposición.

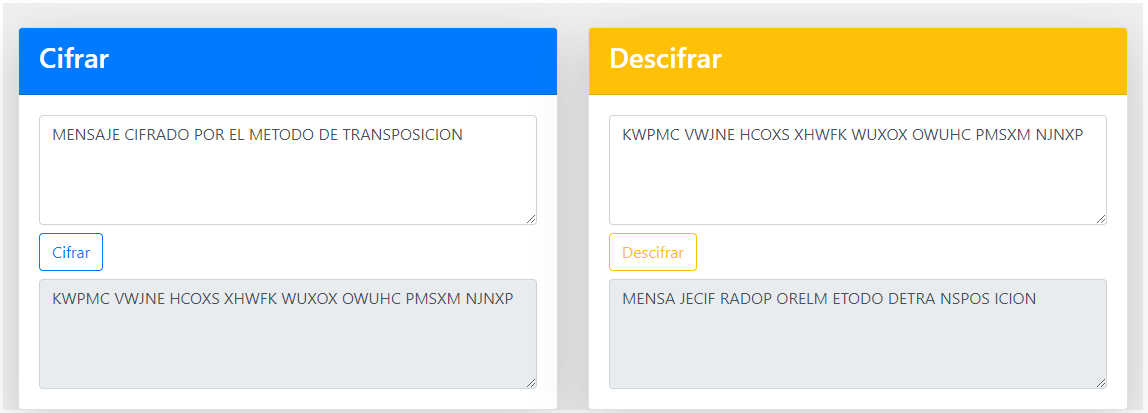
El módulo: Se encuentra dentro del paquete de cifrado de la librería js-ktc y es esencial para llevar a cabo el cifrado por transposición en proyectos Vue.js. Ofrece las funciones y métodos necesarios para la ejecución del cifrado.

El paquete: Incluye una serie de herramientas criptográficas en la librería js-ktc y permite a los desarrolladores acceder a un conjunto completo de funciones para implementar diversas técnicas de cifrado, incluyendo el cifrado por transposición.

La extensión JS: Hace referencia al uso de JavaScript en conjunto con Vue.js para implementar funcionalidades de cifrado por transposición ofrecidas por la librería js-ktc. JavaScript es el lenguaje de programación utilizado para crear la lógica de cifrado en aplicaciones web.

El método o función: Se llama encrypt y decrypt, y se utilizan para cifrar y descifrar mensajes respectivamente. Estas funciones toman como argumento el mensaje que se desea cifrar o descifrar, y en algunos casos, pueden requerir argumentos adicionales, como una clave de cifrado, dependiendo de la implementación específica en un proyecto.

En resumen, js-ktc es una librería que proporciona módulos de cifrado por transposición para proyectos Vue.js, y su uso implica importar un módulo desde el paquete de cifrado, lo que permite la implementación de cifrado por transposición en aplicaciones web con JavaScript. Los métodos encrypt y decrypt son esenciales para realizar el cifrado y descifrado de mensajes de manera segura.

****

**Repositorio: https://github.com/AvelinaHdez/CIFRADO\_TRANSPOSICION\_FRAMEWORK.git**

# Conclusión

La criptografía y el cifrado desempeñan un papel esencial en la seguridad de la información y las comunicaciones en un entorno de desarrollo. La protección de datos confidenciales y la prevención del acceso no autorizado son preocupaciones críticas en el mundo digital. La Escítala, un ejemplo de cifrado de transposición vertical, ilustra cómo reorganizar los caracteres de un mensaje sin alterar su contenido.

La importancia del cifrado en el desarrollo se sustenta en varios aspectos fundamentales. Primero, garantiza la confidencialidad al proteger datos sensibles, como contraseñas y datos financieros, de miradas indiscretas. Segundo, promueve la integridad al detectar cambios no autorizados en la información durante su transmisión o almacenamiento. Además, se utiliza en la autenticación de datos y usuarios para confirmar la fuente confiable de la información y prevenir ataques cibernéticos, como la interceptación de datos y el acceso no autorizado.