CENTRO DE CIENCIAS BÁSICAS

INGENIERÍA EN SISTEMAS COMPUTACIONALES

Primeros pasos cifrando

Alumnos:

Nombre:	ID:
Escareño Pérez Armando	246518
Hernández Martínez Leonardo Javier	274258
Varela Martínez Jaime Adolfo	295482

8° B

Docente:

Ocampo Silva Arturo

Curso:

Seguridad en Sistemas

Aguascalientes, Ags. Febrero de 2024

Índice

Introducción

Escareño Pérez Armando: El cifrado es una parte esencial de la seguridad de la información y la privacidad en la era digital. Uno de los métodos de cifrado más antiguos y conocidos es el cifrado César, nombrado así por Julio César, quien, según se informa, lo utilizó para comunicaciones seguras. Este método es un tipo de cifrado por sustitución que implica cambiar cada letra en el texto original por una letra un número determinado de posiciones más adelante en el alfabeto. A pesar de su simplicidad, el cifrado César juega un papel crucial en la introducción de los conceptos básicos de cifrado y seguridad de la información. Aunque en la actualidad existen métodos de cifrado más sofisticados y seguros, el cifrado César sigue siendo relevante para entender los fundamentos del cifrado y cómo se puede utilizar para proteger la información. Además, este método de cifrado puede ser útil en situaciones donde el nivel de seguridad requerido no es muy alto, o como una capa adicional de seguridad en combinación con otros métodos de cifrado más robustos. Sin embargo, es importante recordar que ninguna técnica de cifrado es completamente segura y que la seguridad de la información depende tanto de la robustez del algoritmo de cifrado como de cómo se manejan y se protegen las claves de cifrado.

Hernández Martínez Leonardo Javier: En esta práctica, se presenta un algoritmo de cifrado y descifrado implementado en JavaScript. El propósito de este algoritmo es proporcionar una forma de proteger la información mediante la aplicación de un cifrado basado en un valor de módulo. Esta técnica de cifrado utiliza una fórmula matemática para alterar los caracteres del texto original, lo que dificulta su comprensión para cualquier persona que no tenga acceso a la clave de descifrado.

El algoritmo se divide en varias funciones clave: cifrar(), actualizar(), y actualizarR(). La función cifrar() se encarga de aplicar el cifrado o descifrado al texto según el valor del módulo y el parámetro de cifrado proporcionado. Por otro lado, las funciones actualizar() y actualizarR() se utilizan para actualizar dinámicamente los campos de texto con los resultados cifrados y descifrados, respectivamente, en respuesta a los eventos de entrada del usuario.

A través de esta práctica, se busca proporcionar una comprensión práctica de los conceptos básicos de cifrado y descifrado, así como también fomentar la familiaridad con el uso de event listeners para actualizar la interfaz de usuario en tiempo real en respuesta a las acciones del usuario.

Varela Martínez Jaime Adolfo: A medida que fue posible almacenar información, se necesitaron desarrollar métodos para protegerla y evitar que cayera en manos de individuos no autorizados. Uno de los métodos más importantes fue el cifrado César. Este método consiste en desplazar el valor de cada letra una cantidad específica de posiciones en el alfabeto. Aunque pueda parecer simple, resulta bastante interesante. Aunque hoy en día pueda no parecer muy sofisticado, en su momento fue una herramienta invaluable para resguardar la información.

Es importante adentrarnos en términos de código, es importante comprender qué es ASCII. En términos simples, ASCII es un conjunto de caracteres utilizado para representar texto en sistemas informáticos. Cada carácter está asociado a un número único, lo que facilita la comunicación y el intercambio de información entre diferentes dispositivos y programas. Por otro lado, Unicode es un estándar de codificación de caracteres que va más allá de ASCII al asignar un número único a cada símbolo, letra o carácter utilizado en la escritura de la mayoría de los idiomas del mundo, así como también caracteres especiales, emojis y símbolos gráficos. Como herramientas solo haremos uso de HTML, CSS y JavaScript.

Objetivo

El propósito de este proyecto es crear un sitio web que permita a los usuarios introducir texto y cifrarlo según el método y módulo de su elección. La plataforma ofrecerá una variedad de módulos de cifrado para adaptarse a las preferencias individuales de los usuarios. Entre estos módulos, se empleará como base la codificación ASCII y se incluirá una opción para utilizar el estándar Unicode que amplía las posibilidades de cifrado al admitir una gama más amplia de caracteres y símbolos, lo que resulta especialmente útil para idiomas que utilizan alfabetos no latinos y para la representación de emojis y otros símbolos gráficosbrindando así flexibilidad y versatilidad en el proceso de cifrado.

El proceso de cifrado se llevará a cabo de manera transparente para el usuario, quien podrá seleccionar el método de cifrado deseado y proporcionar el texto original. El sitio web realizará entonces las operaciones necesarias según el algoritmo seleccionado y devolverá el mensaje cifrado al usuario.

Desarrollo

1. En esta sección agregamos a los campos que pueden ser editados un listener que va a estar escuchando cuando se haga una modificación a cada campo y llama a actualizar.
2. Verificamos si módulo es válido dentro de nuestro rango y llamamos a cifrar si todo está bien.
3. Ciclamos los caracteres dentro del texto para obtener su código, se verifica que esté dentro del rango efectivo y hacemos las operaciones correspondientes para cambiar el carácter.
4. Igual que el punto anterior, ahora el rango es mucho mayor, hasta 65535, pero el funcionamiento es igual.
5. Se recibe el texto y modulo y desciframos por el texto por el modulo, el resultado se guarda como string y se retorna a actualizar.
6. Actualizar tiene ciclos anidados, se genera una pseudotabla de 32 filas por 3 columnas donde se imprimen los 94 resultados al descifrar en todos los módulos.

Sitio web: https://cifrado-cesar-nu.vercel.app/

Código fuente: https://github.com/JaimeVarelaa/Cifrado_Cesar

Conclusión

Escareño Perez Armando: El cifrado César, aunque simple y fácil de descifrar en la era moderna, es una excelente introducción a los conceptos de cifrado. Su simplicidad permite entender los principios básicos de la seguridad de la información. Aunque no es adecuado para alta seguridad, puede ser útil donde el nivel de seguridad requerido no es alto, o como una capa adicional en combinación con otros métodos de cifrado más robustos. La seguridad de la información depende tanto del algoritmo de cifrado como de cómo se manejan y protegen las claves de cifrado.

Hernández Martínez Leonardo Javier: En esta práctica, hemos explorado la implementación de un algoritmo de cifrado y descifrado en JavaScript, que utiliza un valor de módulo para proteger la información sensible. A través de la comprensión de este algoritmo, hemos podido apreciar la importancia de la seguridad de la información en el desarrollo de aplicaciones y sistemas.

Al utilizar técnicas de cifrado, como la que hemos analizado, los desarrolladores pueden garantizar la confidencialidad de los datos transmitidos o almacenados, lo que es crucial en entornos donde la privacidad y la seguridad son prioritarias.

Además, hemos observado cómo las funciones de actualización dinámica de la interfaz de usuario permiten una experiencia más fluida para el usuario, al proporcionar retroalimentación instantánea sobre los resultados del cifrado y descifrado a medida que se ingresan los datos.

En resumen, esta práctica nos ha brindado una visión más profunda de los fundamentos del cifrado, destacando su importancia en el ámbito de la seguridad de la información y su aplicación práctica en el desarrollo de aplicaciones web y sistemas informáticos.

Varela Martínez Jaime Adolfo: Al finalizar este proyecto se logró cumplir satisfactoriamente el objetivo del mismo, se ha creado completamente un sitio web el cual permite cifrar y descifrar texto por ASCII y UNICODE dando opción al usuario de elegir el módulo de cifrado, personalmente considero que el sitio tiene un buen aspecto para el usuario, sencillo y es fácil de utilizar, ahora podremos cifrar nuestros mensajes a nuestro gusto, pues, hemos comprendido lo básico de cifrar.

Bibliografía

Unicode Character Table - Full List of Unicode Symbols (◕‿◕) SYMBL. (s. f.).

https://symbl.cc/en/unicode/table/#latin-extended-b

Peter. (s. f.). El código ASCII Completo, tabla con los codigos ASCII completos, caracteres simbolos letras ascii, ascii codigo, tabla ascii, codigos ascii, caracteres ascii, codigos, tabla, caracteres, simbolos, control, imprimibles, extendido, letras, vocales, signos, simbolos, mayusculas, minusculas, alt, teclas, acentos, agudo, grave, eñe, enie, arroba, dieresis, circunflejo, tilde, cedilla, anillo, libra, esterlina, centavo, teclado, tipear, escribir, español, ingles, notebook, laptop, asccii, asqui, askii, aski,20240220. El Código ASCII Completo. https://elcodigoascii.com.ar/

colaboradores de Wikipedia. (2024, 27 enero). Unicode. Wikipedia, la Enciclopedia Libre. https://es.wikipedia.org/wiki/Unicode

colaboradores de Wikipedia. (2024b, febrero 8). ASCII. Wikipedia, la Enciclopedia Libre. https://es.wikipedia.org/wiki/ASCII