Universidad Autónoma de Aguascalientes

Centro de Ciencias Basicas

Ingeniería en Sistemas Computacionales

Materia: SEGURIDAD EN SISTEMAS

Primeros pasos cifrando

Yahir Guevara Cardona

ID: 349804

Semestre: 8° Grupo: B

Profesor: ARTURO OCAMPO SILVA

Aguascalientes, Ags. Viernes 20 de Febrero del 2026

ÍNDICE

Introducción....3
Objetivo....3
Desarrollo....4
Arquitectura del Sistema Web....4
Implementación de los Algoritmos....4
Estrategia de Documentación Segura....5
Conclusión....5
Bibliografía....6

Introducción

Desde que la humanidad comenzó a generar información de valor, surgió la necesidad inquebrantable de protegerla de miradas hostiles. Los primeros intentos de ocultamiento, como el Cifrado César (desplazamiento) y el Atbash (sustitución inversa), representaron los cimientos de la criptografía clásica. Sin embargo, la aparente seguridad de estos métodos fue destrozada por el intelecto de أبو يوسف يعقوب بن إسحاق الكندي (Al-Kindi).

Al-Kindi revolucionó la criptoanálisis al documentar por primera vez la técnica del análisis de frecuencias en el siglo IX. Él demostró que, dado que ciertas letras se repiten con mayor frecuencia en un idioma, se podía romper cualquier cifrado de sustitución simple (como César o Atbash) analizando el texto cifrado y mapeando las repeticiones con las estadísticas del lenguaje original.

Hoy en día, el uso de cifrados como César y Atbash ya no es viable para la protección de datos reales. Su espacio de claves es minúsculo (por ejemplo, solo 25 claves posibles en un César básico) y su susceptibilidad al análisis de frecuencias hace que un procesador moderno, o un simple script, pueda romperlos mediante fuerza bruta en cuestión de milisegundos. Quedan relegados a la academia como un recordatorio de que la seguridad por oscuridad siempre termina cediendo ante la lógica.

Objetivo

Desarrollar y desplegar una aplicación web del lado del cliente que permita el cifrado y descifrado de cadenas de texto mediante los algoritmos clásicos César y Atbash. El sistema debe ser capaz de procesar un conjunto de caracteres (alfabeto) definido por el usuario, seleccionar dinámicamente el módulo de desplazamiento, y operar de forma independiente y en tiempo real.

Desarrollo

Arquitectura del Sistema Web

El programa fue desarrollado eliminando dependencias de servidores backend, utilizando una arquitectura pura de Frontend (HTML5, CSS3, JavaScript). Esto permite que el procesamiento criptográfico ocurra directamente en el navegador del usuario, garantizando que los datos en texto plano nunca viajen a través de la red. La aplicación está alojada y publicada mediante GitHub Pages.

Implementación de los Algoritmos

El sistema permite al usuario alimentar un "Conjunto de Caracteres Base" (alfabeto) personalizado, el cual puede incluir letras, números, espacios y caracteres especiales basados en ASCII.

Algoritmo César: Se implementó una lógica matemática modular que busca el índice de cada carácter en el alfabeto base y le suma o resta el "Módulo" ingresado por el usuario ((pos + modulo) % longitud_alfabeto).

Algoritmo Atbash: Se invirtió el índice del carácter dentro del alfabeto base mediante la fórmula (longitud_alfabeto - 1) - pos.

La interfaz intercepta cada pulsación de tecla y procesa el cifrado en tiempo real, inyectando el resultado en un monitor de datos.

Estrategia de Documentación Segura

Para dar cumplimiento a la directiva de generar una "documentación segura" prescindiendo de la impresión física, este proyecto se ha documentado bajo los siguientes parámetros:

Formato Inmutable: La presente documentación se entrega en formato PDF de solo lectura.

Transparencia de Código: El código fuente completo, detallado y comentado, reside de manera inalterable en un repositorio público de control de versiones (GitHub). Esto garantiza la trazabilidad de los cambios, la autoría del código y permite auditorías sin necesidad de trasladar papel. El enlace al repositorio funge como la llave de acceso a la documentación técnica profunda.

Conclusión

El desarrollo de este módulo de cifrado demuestra que, si bien las matemáticas detrás de César y Atbash son triviales para los estándares modernos, la lógica de la sustitución sigue siendo un concepto fundamental. Construir esta herramienta desde cero, controlando cada variable y el alfabeto completo, reafirma que la verdadera seguridad no reside en depender de herramientas opacas, sino en comprender el código fuente y la estructura subyacente de la información. La historia de Al-Kindi nos enseña que ningún candado es eterno frente al análisis metódico.

Bibliografía

Singh, S. (1999). Los códigos secretos. Editorial Debate.

Al-Kadi, I. A. (1992). The origins of cryptology: The Arab contributions. Cryptologia, 16(2), 97-126.

MDN Web Docs. (2023). JavaScript Data Structures. Mozilla Foundation.