



UNIVERSIDAD AUTÓNOMA
DE AGUASCALIENTES

INGENIERÍA EN SISTEMAS COMPUTACIONALES

SEGURIDAD EN SISTEMAS

PRIMEROS PASOS CIFRANDO

**ALUMNA: MARTHA MELINNA FLORES
HERNÁNDEZ**

DOCENTE: ARTURO OCAMPO SILVA

ENTREGA: 20 DE FEBRERO DE 2026

Índice

Índice	pág. 1
Introducción	pág. 2
Objetivo	pág. 2
Desarrollo	pág. 3
Conclusión	pág. 5
Bibliografía	pág. 5

Introducción

La historia de la criptografía dio un giro fundamental en el siglo IX gracias a أبو يوسف يعقوب بن إسحاق الكندي (Al-Kindi). En su "Manuscrito sobre el desciframiento de mensajes criptográficos", Al-Kindi introdujo por primera vez la técnica del análisis de frecuencias, la cual permite romper cifrados de sustitución simple mediante el estudio estadístico de la repetición de caracteres en un idioma. Su aporte es considerado el nacimiento del criptoanálisis, ya que proporcionó la primera herramienta científica para hackear sistemas de encriptación que hasta entonces se consideraban seguros.

En el contexto actual de la seguridad informática, el uso de métodos como el cifrado César (sustitución por desplazamiento) y Atbash (sustitución por inversión) ya no resulta viable para la protección de datos reales. Esto se debe a dos razones principales:

- ✚ Vulnerabilidad ante el análisis de frecuencias: Al ser cifrados monoalfabéticos, mantienen la estructura estadística del texto original, lo que permite descifrarlos fácilmente con la técnica de Al-Kindi.
- ✚ Espacio de claves reducido: Estos métodos poseen un número muy limitado de combinaciones posibles (25 en el caso del César clásico), lo que permite que una computadora moderna los rompa por fuerza bruta en una fracción de segundo.

Por lo tanto, aunque estos algoritmos son pilares educativos para entender la lógica de la ocultación de información, carecen de la robustez necesaria para enfrentar las amenazas de ciberseguridad contemporáneas.

Objetivo

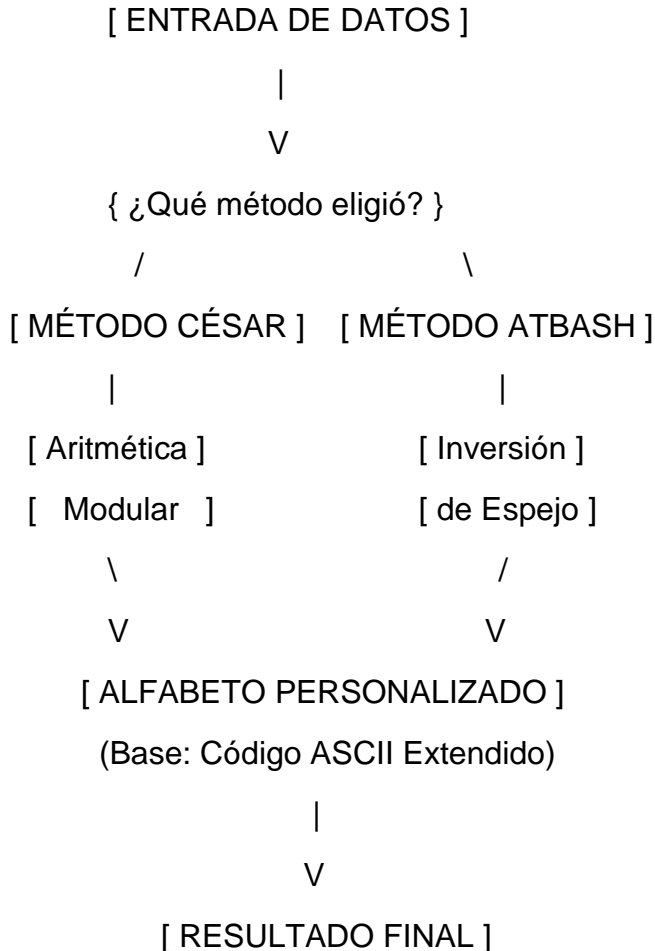
Diseñar e implementar una herramienta digital basada en entorno web que permita realizar procesos de cifrado y descifrado de información mediante los algoritmos clásicos César y Atbash. El sistema tiene como finalidad secundaria demostrar la importancia de la flexibilidad en la seguridad de datos al permitir el uso de un conjunto de caracteres (alfabeto) personalizado basado en el estándar ASCII, garantizando que el usuario pueda alimentar el sistema con diversos símbolos y validar la correcta identificación del módulo de cifrado utilizado.

Desarrollo

El sistema se desarrolló como una aplicación web responsiva enfocada en la seguridad lógica, de la cual está de la siguiente manera:

1. Arquitectura Lógica

Dado que el sistema debe identificar el módulo o tipo de cifrado utilizado, el flujo de datos se estructuró así:



2. Implementación de Algoritmos

El sistema cumple con el requisito de utilizar el código ASCII como base, permitiendo al usuario alimentar el conjunto de caracteres: Cifrado César: Se implementó mediante la fórmula matemática $C = (P + n) \bmod L$, donde P es la posición del carácter en el alfabeto ingresado por el usuario, n el desplazamiento y L la longitud total del conjunto, esto garantiza que el cifrado sea cíclico. Cifrado Atbash: Se diseñó como un cifrado de sustitución recíproco, el

sistema calcula la posición inversa exacta dentro del alfabeto personalizado, logrando el efecto de "espejo" característico de este método. Flexibilidad de Alfabeto: A diferencia de los cifradores tradicionales, este sistema permite ingresar cualquier cadena de texto como alfabeto base (letras, números, espacios y símbolos ASCII), cumpliendo con el requerimiento de alimentación dinámica de caracteres.

3. Tabla de Verificación de Funcionamiento

Para validar que el sistema identifica y procesa correctamente los módulos, se realizó las siguientes pruebas lógicas:

Módulo Seleccionado	Entrada (Plaintext)	Alfabeto Base	Parámetro	Resultado (Ciphertext)
César (Cifrar)	A	ABC	Desp: 1	B
César (Descifrar)	B	ABC	Desp: 1	A
Atbash	HOLA	ABC...XYZ	N/A	SLOZ
ASCII Extendido	123	0123456789	Desp: 2	345

Links:

<https://marneko0.github.io/Cifrado-de-Abecedario/>

<https://github.com/MarNeko0/Cifrado-de-Abecedario>

Conclusión

En este proyecto, vi la importancia de comprender los fundamentos de la criptografía clásica para entender la evolución de la seguridad informática, además la implementación de los algoritmos César y Atbash me dejó ver cómo la lógica matemática se aplica a la protección de datos, mientras que el estudio de Al-Kindi me mostró que la seguridad absoluta no existe frente al análisis estadístico. Finalmente, el uso de herramientas modernas como VS Code y GitHub ha facilitado una documentación segura y profesional, cumpliendo con los estándares actuales de desarrollo web.

Bibliografía

- Al-Kindi. (s.IX). Manuscrito sobre el desciframiento de mensajes criptográficos.
- Kahn, D. (1996). The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Scribner.
- Singhal, A. (2021). Cryptography and Network Security. McGraw Hill.