
Universidad Nacional Autónoma de México


Facultad de Ingeniería

Ingeniería en computación (110)

Estructuras de Datos y Algoritmos I

Actividad asíncrona miércoles 04: Cifrado César

Martínez Miranda Juan Carlos

(19/03/2021)

**Cifrado César**

El cifrado de César, como su nombre lo intuye, fue utilizado por Juilo César para mantener una comunicaión segura con sus generales codificando sus mensajes y así evitar que el enemigo descubra sus alineaciones, sus ataques y sus planes. Este sistema consiste en alinear el alfabeto en una fila y debajo de esta fila, colocar de nuevo el alfabeto pero comenzando tres letras o más después de la 'A', de esta manera, los mensajes codificados no podrían ser comprendidos por personas que sepan cuántas letras del alfabeto se recorrieron para codificarlo.

| A | B | C | D | E | F | G | H | I | J | K | L | M | Ñ | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| E | F | G | H | I | J | K | L | M | N | Ñ | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |

Si queremos cifrar la frase: "DILES QUE LO APROVECHEN", tenemos que observar la tabla y reemplazar las letras de la fila superior por sus correspondientes en la fila inferior: "HMOIW UYI OS ETVSZIGLIR", así podríamos mandar nuestro mensaje cifrado, quien lo reciba deberá realizar el proceso inverso que realizamos nosotros, de la fila inferior, reemplazar sus correspondientes de la fila superior.

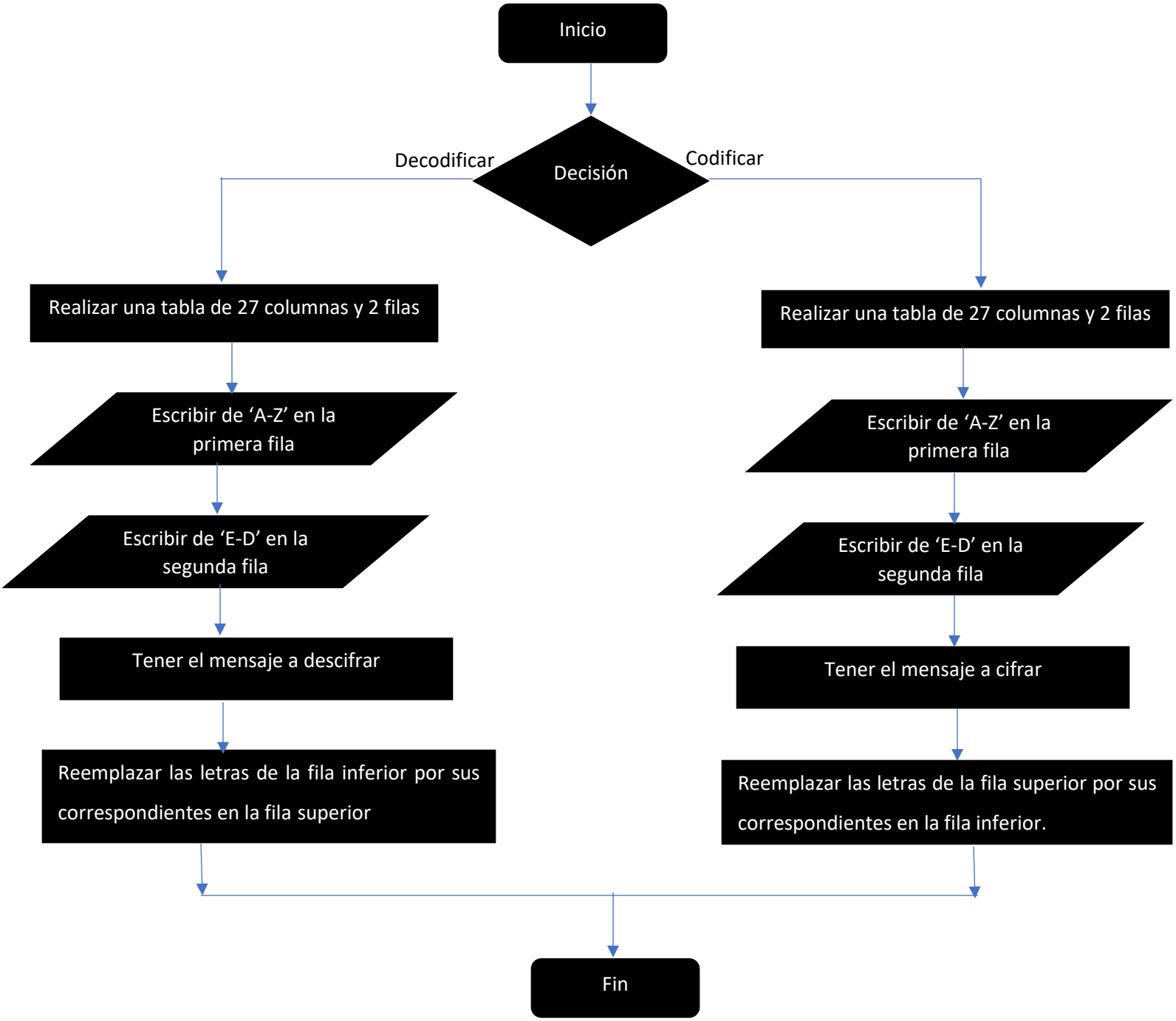
**Algoritmo para cifrar con este mecanismo**

1. Realizar una tabla de 27 columnas y dos filas
2. En la primera fila escribir el alfabeto en orden de 'A-Z'
3. En la segunda fila escribir el alfabeto a partir de la 4 letra después de la A ('E-D")
4. Tener el mensaje a cifrar
5. Reemplazar las letras de la fila superior por sus correspondientes en la fila inferior.
6. Fin

**Algoritmo para descifrar con este mecanismo**

1. Realizar una tabla de 27 columnas y dos filas
2. En la primera fila escribir el alfabeto en orden de 'A-Z'
3. En la segunda fila escribir el alfabeto a partir de la 4 letra después de la A ('E-D")
4. Tener el mensaje a descifrar
5. Reemplazar las letras de la fila inferior por sus correspondientes en la fila superior
6. Fin

## *Diagrama de flujo*




***Fuentes de consulta***


http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/cesar.html