



# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE  
INGENIERÍA

MI. Marco Antonio Martínez  
Quintana

Estructura de Datos y  
Algoritmos

Asignatura:

Estructura de Datos y Algoritmos 1



Actividad Viernes

#2 Criptografía, algoritmo y diagrama de flujo



Alumna

Citlali Cuahtepitzi Cuatlapantzi

Fecha

(07/marzo/2021)



# Criptografía, algoritmo y diagrama de flujo

## Escítala espartana

El primer caso claro de uso de métodos criptográficos se dio durante la guerra entre Atenas y Esparta. El historiador griego Plutarco, describe la escítala de la siguiente manera:

“La escítala era un palo o bastón en el cual se enrollaba en espiral una tira de cuero. Sobre esa tira se escribía el mensaje en columnas paralelas al eje del palo. La tira desenrollada mostraba un texto sin relación aparente con el texto inicial, pero que podía leerse volviendo a enrollar la tira sobre un palo del mismo diámetro que el primero”.

Con este sistema los gobernantes de Esparta transmitieron, con eficacia, sus instrucciones secretas a los generales de su ejército, durante las campañas militares. Lógicamente, este procedimiento suponía que tanto el emisor como el receptor del mensaje dispusieran de un palo o bastón con las mismas características físicas: grosor y longitud.



Ejemplo:



El texto a remitir: **ASI CIFRABAN CON LA ESCITALA**

Texto cifrado o criptograma: **AAC SNI ICT COA INL FLA RA AE BS**

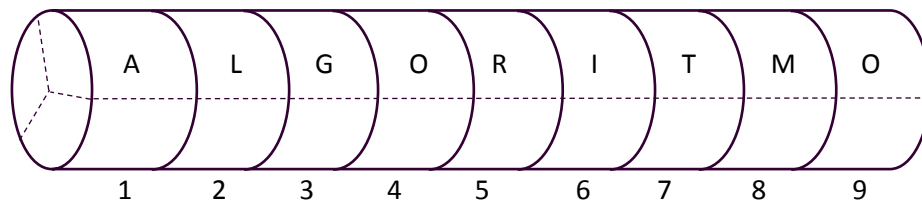
## Diseño de algoritmo para cifrar y descifrar

Entradas: Mensaje

Salidas: Mensaje cifrado y descifrado

Restricciones (ejemplo) :

Palo o bastón en forma cilindro con un radio de  $\pi$  y una longitud de  $9\pi$ , permitiendo 9 lugares a lo largo y 3 alrededor del círculo.



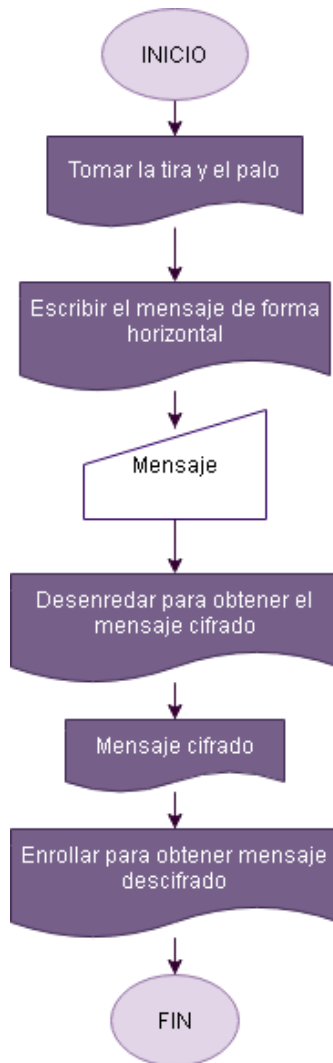
La tira tendrá un ancho de  $\pi$  y un largo de  $25\pi$  permitiendo un mensaje final de 25 caracteres.

A			└			G			O			R			—			┐			Σ			O
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Algoritmo (No computacional):

1. Inicio
2. Tomar la tira y el palo
3. Enrollar la tira alrededor del palo
4. Escribir el mensaje de forma horizontal
5. Desenredar para obtener el mensaje cifrado
6. Enrollar para obtener el mensaje descifrado
7. Fin

## Diagrama de flujo



Fernández, S. (2004). La criptografía clásica. *Sigma: Revista de matemáticas*, 119-142. Recuperado de:

[https://d1wqtxts1xzle7.cloudfront.net/38520592/9\\_Criptografia\\_clasica.pdf?1440040574=&response-content-disposition=inline%3B+filename%3DLA\\_CRIPTOGRAFIA\\_CLASICA.pdf&Expires=1614961323&Signature=Hu5igYoZPAhOZKUrVMG6WN-1aq2ty6sqNcVI0wig-jQhJ7SHltYthcU7OMai5A12ud4~6TEI-tAdW9tH5PCZQ0yjRSER1tnpx2QAQKyF9iQsS363soW~l2Zl8WtIA19YymDOCEdoUqhpDKEt0rs66D-BBAoc3OiGORQyIUmkqtaUGl8YvIZ0jdPlht9xl~4UaBH4FqbzrzK2NaxvkzdQ4CljNvbS5VlsfzDOhlcHZ5wz6ebUU7LzsHmdfXARQrpNEmbo643f~p2FTGAbuOdPvCFz5x5-Y1cEy5~u-SVOFEuJ6j4NCea8Q19uRBZPuMI7aw5vANKYepePXLSGE4jtIQ\\_\\_&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA](https://d1wqtxts1xzle7.cloudfront.net/38520592/9_Criptografia_clasica.pdf?1440040574=&response-content-disposition=inline%3B+filename%3DLA_CRIPTOGRAFIA_CLASICA.pdf&Expires=1614961323&Signature=Hu5igYoZPAhOZKUrVMG6WN-1aq2ty6sqNcVI0wig-jQhJ7SHltYthcU7OMai5A12ud4~6TEI-tAdW9tH5PCZQ0yjRSER1tnpx2QAQKyF9iQsS363soW~l2Zl8WtIA19YymDOCEdoUqhpDKEt0rs66D-BBAoc3OiGORQyIUmkqtaUGl8YvIZ0jdPlht9xl~4UaBH4FqbzrzK2NaxvkzdQ4CljNvbS5VlsfzDOhlcHZ5wz6ebUU7LzsHmdfXARQrpNEmbo643f~p2FTGAbuOdPvCFz5x5-Y1cEy5~u-SVOFEuJ6j4NCea8Q19uRBZPuMI7aw5vANKYepePXLSGE4jtIQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA)