



Universidad Nacional Autónoma de México

Facultad de Ingeniería



Asignatura:

Estructura de Datos y Algoritmos I

Actividad #2 | Escítala espartana

Nombre del Alumno:

Sánchez Estrada Angel Isaac

Maestro:

M.I. Marco Antonio Martínez Quintana

Grupo:

15

Fecha:

08/03/2021



ESCÍTALA ESPARTANA

¿Qué es la Criptografía?

La palabra criptografía proviene del griego “κρυπτός” (/kryptos/), que significa ocultar, y “γραφειν” (/grafein/), que significa escribir. Es decir, la palabra criptografía significa escritura oculta. A partir de este significado es que nace su definición.

La criptografía se define como, la ciencia que estudia la codificación de información mediante el uso de llaves (claves), con la finalidad de que, solo el propietario, y aquellos que este autorice, sean capaces de decodificarla y leerla.

¿Qué es la escítala espartana?

Es un artefacto cilíndrico que resulta de proyectar un polígono regular de n lados, sobre el cual se enrosca una tira de cuero o papiro, es considerado uno de los primeros métodos de cifrado o sistema de criptografía, el cual fue utilizado en la guerra entre Atenas y Esparta para proteger el contenido de sus mensajes de los ojos del enemigo al ser enviados.

Para comunicarse los militares espartanos enrollaban en forma de espiral una tira de cuero o papiro en una escítala (palo o bastón). Sobre esa tira se escribía el mensaje longitudinalmente, luego se desenrollaba y se enviaba a destino. Si alguien interceptaba el mensaje, aunque leyera la tira no entendería su contenido debido a que las letras aparecerían mezcladas. Este método requería que el receptor dispusiera de una escítala idéntica a la utilizada para cifrar el mensaje, para que, enrollando la tira en el bastón, pudiera descifrarlo.



Berrondo, R., Cabrera, N., Franco, G., Frederico, M., Mariani, F., & Rodríguez, L. (2015). Criptografía: una cuestión de códigos.

Algoritmo para cifrar y descifrar con escítala espartana

En vida real de los espartanos

PROBLEMA: La manera de cifrar y descifrar un mensaje atreves de la escítala espartana

DATOS DE ENTRADA: Mensaje a cifrar o descifrar

DATOS DE SALIDA: Mensaje descifrado o cifrado

1. Si vas a cifrar un mensaje entonces:
 - 1.1. Tomar una vara de un diámetro determinado.
 - 1.2. Cortar una hoja o un cuero en forma de tira.
 - 1.3. Enrollar la tira en la vara en espiral sobre la vara.
 - 1.4. Escribir sobre la tira antes enrollada el mensaje a lo largo de la vara.
 - 1.5. Desenrollar la tira de la vara y el mensaje ya está cifrado.
2. Si vas a descifrar un mensaje entonces:
 - 2.1. Se toma una vara con el mismo grosor con la que fue cifrado el mensaje.
 - 2.2. Enrollar el mensaje cifrado en forma de espiral en la vara del mismo grosor con el que fue encriptado el mensaje
 - 2.3. Leer el mensaje a lo largo de la vara
 - 2.4. Y obtener el mensaje descifrado

En papel y Excel

1. Deseas cifrar o descifrar
2. Si desea cifrar entonces
 - 2.1. Hacer una tabla con el número de columnas y filas deseadas para cifrar el mensaje
 - 2.2. Acomodar el mensaje horizontalmente tomando todas las columnas deseadas
 - 2.3. Escribir el mensaje poniendo las letras de arriba a hacia abajo con orden de las columnas
 - 2.4. Poner el mensaje con el nuevo orden de manera horizontal
 - 2.5. Mandar el mensaje oculto
3. Si desea descifrar entonces
 - 3.1. Conocer el número de columnas que conforma el mensaje
 - 3.2. Hacer una tabla de acuerdo con los datos recibidos
 - 3.3. Ir rellenando los espacios de la tabla en base del mensaje no codificado
 - 3.4. Leer el mensaje horizontalmente en orden al número de filas de izquierda a derecha
 - 3.5. Obtienes el mensaje oculto

En programa de computadora (CODIFICADO)

PROBLEMA: La manera de cifrar y descifrar un mensaje atreves de la escítala espartana

DATOS DE ENTRADA: Mensaje a cifrar o descifrar y numero entero de columnas y renglones

DATOS DE SALIDA: Mensaje descifrado o cifrado

1. Aparece el título de Bienvenidos a escítala espartana
2. Aparece un menú donde puede escoger si se desea escribir o leer un mensaje.
3. Si se desea la escritura de un mensaje se realiza lo siguiente:
 - 3.1. Solicitar escribir un número entero el cual corresponderá al número de columnas del arreglo de la matriz.
 - 3.2. Solicitar escribir un segundo número entero el cual corresponderá al número de renglones del arreglo de la matriz.
 - 3.3. Se creará el arreglo matricial con los números registrados por el usuario.
 - 3.4. Se creará un segundo arreglo matricial de caracteres donde los datos serán iguales a los ingresados para el primer arreglo matricial.
 - 3.5. Se crearan dos variables a,b que inicien en 0 y servirán como contadores.
 - 3.6. Solicitar la cadena de caracteres o el mensaje que se desea cifrar.
 - 3.7. Si la variable "a" es menor a la del primer número entero se hace lo siguiente:
 - 3.7.1. Se iniciará la variable a en cero.
 - 3.7.2. Si la variable "b" es menor que el número que se ingresó para renglones se hace lo siguiente:
 - 3.7.2.1. Se roma el valor de las posiciones [a],[b] del primer arreglo.
 - 3.7.2.2. Se asigna los valores al segundo arreglo
 - 3.7.2.3. Se incrementa b en uno
 - 3.7.2.4. Regresamos a la instrucción o paso 3.7.2 hasta que se cumpla los valores requeridos
 - 3.8. Se incrementa a en uno hasta que se cumpla los valores requeridos
 - 3.9. Se regresa al punto 3.7 para completar los espacios requeridos para el arreglo matricial
 - 3.10. Se envía el mensaje al primer arreglo
 - 3.11. Aparece en pantalla el mensaje cifrado
4. Si desea leer un mensaje se realiza lo siguiente
 - 4.1. Solicitar escribir un número entero el cual corresponderá al número de columnas del arreglo de la matriz.
 - 4.2. Solicitar escribir un segundo número entero el cual corresponderá al número de renglones del arreglo de la matriz.
 - 4.3. Se crea un tercer arreglo matricial con la misma longitud que los datos metidos o registrados
 - 4.4. Se ocupan las mismas variables a y b que funcionaran como contadores
 - 4.5. Solicitar la cadena de caracteres o el mensaje que se desea descifrar.

4.6. Si la variable “a” es menor a la del primer número entero se hace lo siguiente:

4.6.1. “b” se inicia en cero

4.6.2. Si la variable “b” es menor que el número que se ingresó para renglones se hace lo siguiente:

4.6.2.1. Se toma el valor de las posiciones [a],[b] del primer arreglo.

4.6.2.2. Se asigna los valores al segundo arreglo

4.6.2.3. Se incrementa b en uno

4.6.2.4. Regresamos a la instrucción o paso 4.6.2 hasta que se cumpla los valores requeridos

4.6.3. Se incrementa a en uno hasta que se cumpla los valores requeridos

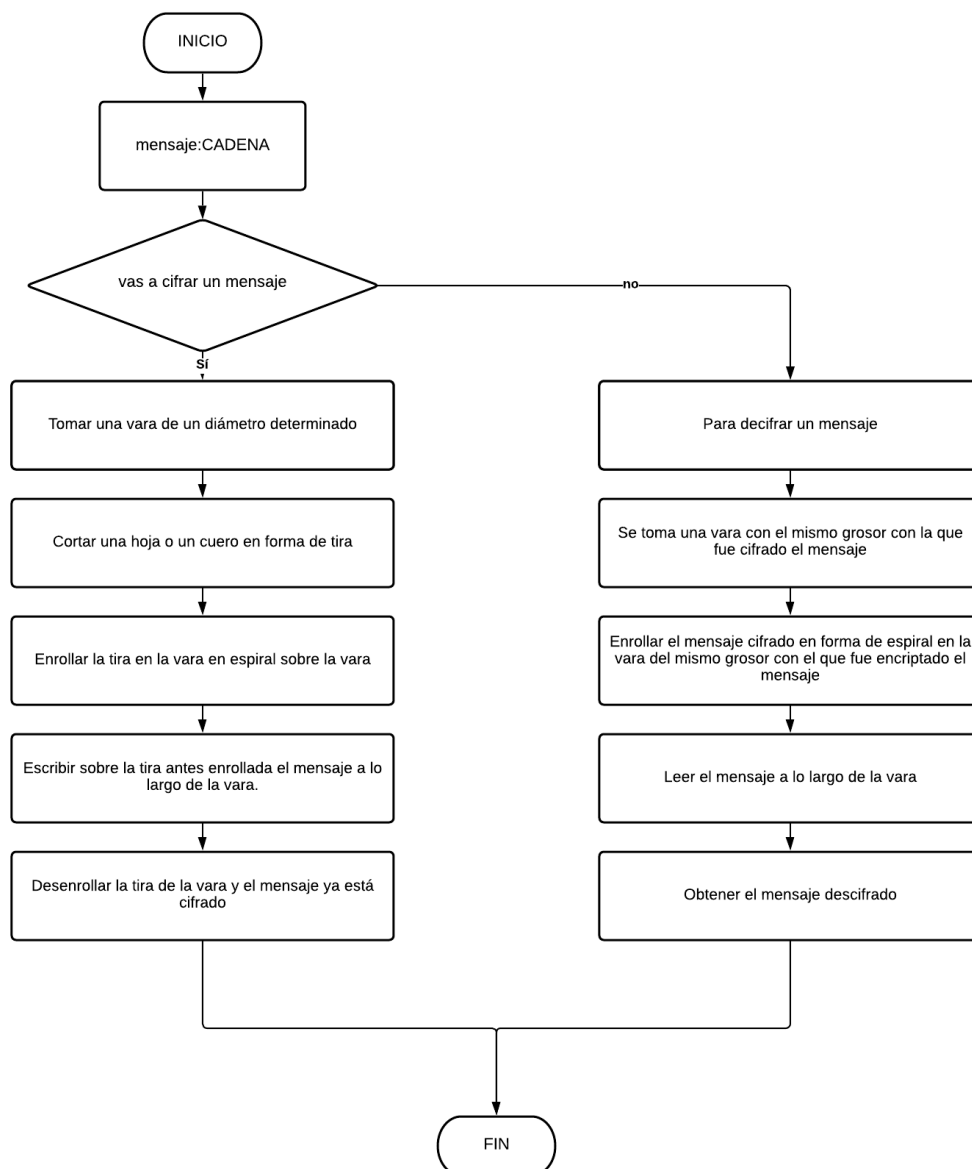
4.6.4. Se regresa al punto 4.6 para completar los espacios requeridos para el arreglo matricial

4.7. Se envía el mensaje al primer arreglo

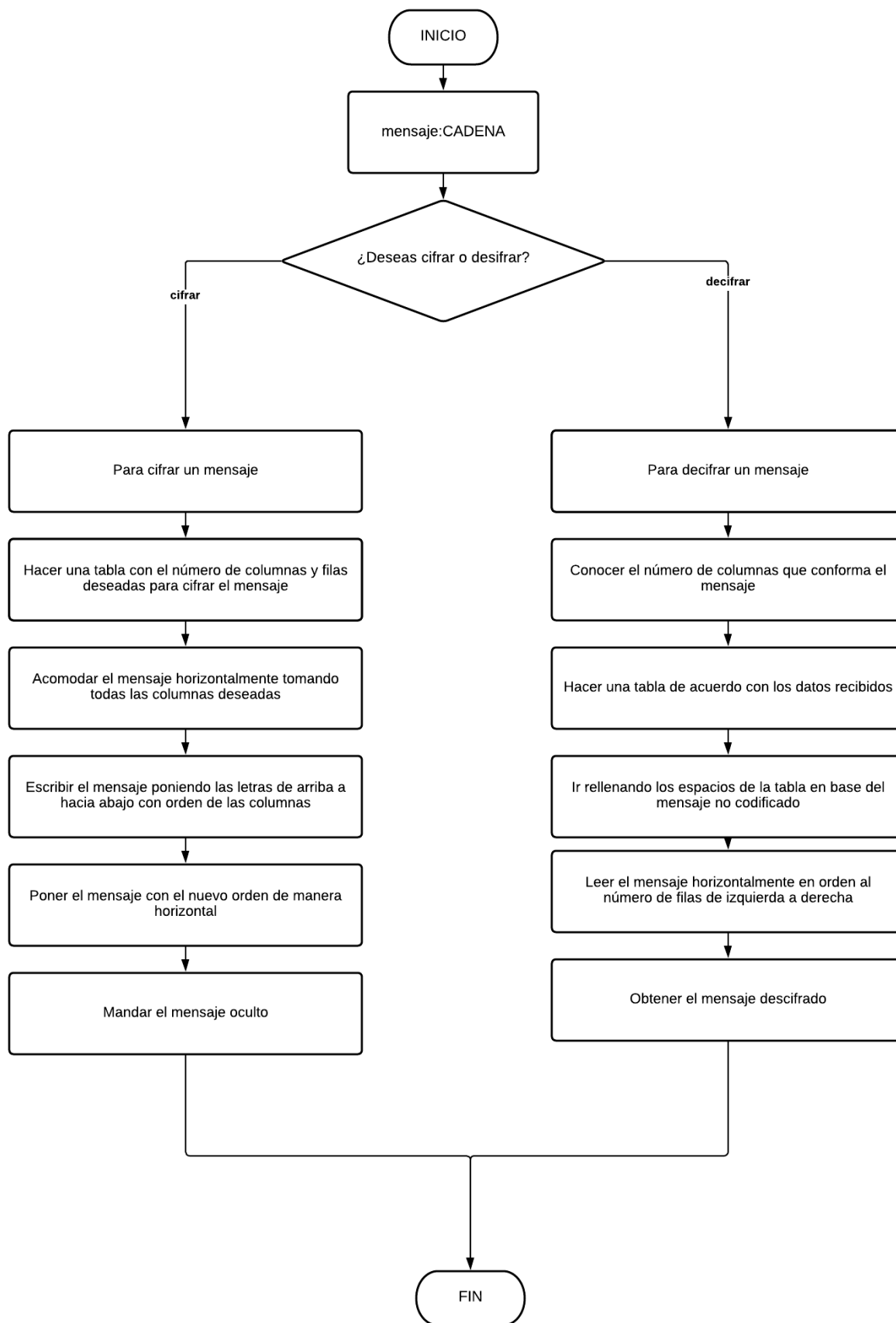
4.8. Aparece en pantalla el mensaje descifrado

Diagramas de flujo

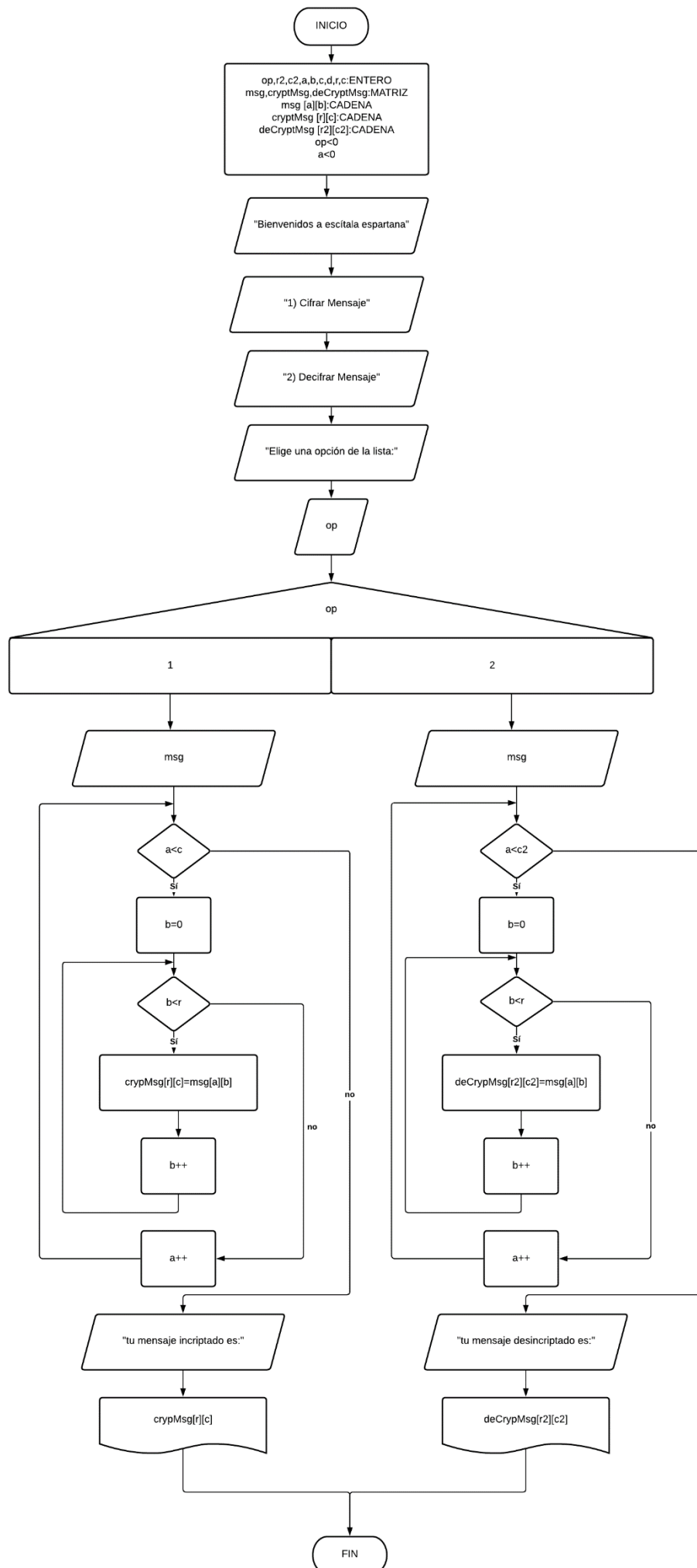
En vida real de los espartanos



En papel y Excel



En programa de computadora (CODIFICADO)



Bibliografías:

- Gil, P. C. (2003). Introducción a la Criptografía. Alfaomega.
- Berrondo, R., Cabrera, N., Franco, G., Frederico, M., Mariani, F., & Rodríguez, L. (2015). Criptografía: una cuestión de códigos.

Referencias:

- Algoritmos de Cifra. (s. f.). Sistemas de Comunicación. Recuperado 5 de marzo de 2021, de <http://sistemasdecomunicacion-gt.blogspot.com/2017/01/algoritmos-de-cifra.html#:~:text=Escitala%2C%20o%20Escitala%20Espartana.,cifrado%20Rot13%2C%20ni%20por%20n%C3%BAmeros.&text=Para%20hacerlo%2C%20los%20espartanos%20enrollaban,tira%2C%20resultaba%20el%20texto%20cifrado>
- Escítala griega - Experimentos con materiales cotidianos. (s. f.). Experimentos con materiales cotidianos. Recuperado 5 de marzo de 2021, de <https://sites.google.com/site/experimentossencillos/inventos-y-maquinas/escitala-griega>
- Font, F. V. (s. f.). ESCITALA ESPARTANA. prezi.com. Recuperado 5 de marzo de 2021, de <https://prezi.com/p/sxlds66kmosm/escitala-espartana/>
- Gomez, V. (s. f.). EscÃ-tala espartana. prezi.com. Recuperado 5 de marzo de 2021, de <https://prezi.com/p/9hjkhlxsoshp/escitala-espartana/#:~:text=Es%20un%20sistema%20de%20criptograf%C3%ADa,puede%20ver%20en%20la%20imagen>.