Universidad Nacional Autónoma de México

Facultad de Ingeniería

Estructura de Datos y Algoritmos I

Actividad 2: Escítala

Sánchez Hernández Marco Antonio

Fecha: 08/marzo/2021

¿Qué es la criptografía?

La palabra criptografía proviene del griego “κρυπός” (/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.

La escítala

“*Cuestiones militares, religiosas y comerciales impulsaron desde tiempos remotos el uso de escrituras secretas*” (Fernández S., 2004). Es precisamente el ámbito militar el que da origen al que hoy en día es considerado el primer método de criptográfico. Durante la guerra entre Atenas y Esparta, los espartanos desarrollaron la escítala, la cual le permitía a los gobernantes enviar sus instrucciones, de manera eficiente y secreta, a los generales de su ejército.

> “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”. (Fernández S., 2004)

Johnk C. (2015). Escítala [figura]. Recuperado de https://blog.lib.uiowa.edu/eng/new-exhibit-on-the-history-of-the-typewriter/

Algoritmo

DATOS DE ENTRADA: Mensaje que desea ser enviado.
DATOS DE SALIDA: Mensaje que fue enviado.

La solución planteada en este algoritmo consiste en la creación de un arreglo matricial, el cual tendrá un tamaño dinámico definido por el usuario, esto asemejaría las características físicas del palo utilizado por los espartanos, dentro del arreglo se almacenarán los caracteres del mensaje escrito para posteriormente cambiar su orden y no hacer posible la lectura de este sin conocer las características del arreglo matricial (renglones y columnas).

1 Seleccionar si se desea escribir o leer un mensaje.
2 Si se desea escribir un mensaje se realiza lo siguiente:
  2.1 Solicitar un primer número entero, el cual corresponderá al número de columnas del arreglo matricial.
  2.2 Solicitar un segundo número entero, el cual corresponderá al número de renglones del arreglo matricial.
  2.3 Crear un primer arreglo matricial con el número de renglones y columnas indicado por el usuario.
  2.4 Se crea un segundo arreglo matricial de caracteres donde el número de renglones sea igual al primer número ingresado (número de columnas), y el número de columnas sea igual al segundo número ingresado (número de renglones).
  2.5 Se crean dos variables, i y j, que inicien en cero y funcionan como contadores.
  2.6 Solicitar una cadena de caracteres que corresponderá al mensaje que se desea cifrar.
  2.7 Si la variable i es menor que el primer número entero (número de columnas del primer arreglo) se realiza lo siguiente:
    2.7.1 Se inicia la variable j en cero.
    2.7.2 Si la variable j es menor que el segundo número entero (número de renglones del primer arreglo) se realiza lo siguiente:
      2.7.2.1 Se toma el valor que contenga la posición (i, j) del primer arreglo.
      2.7.2.2 Se asigna ese valor al segundo arreglo.
      2.7.2.3 Se incrementa j en uno.
      2.7.2.4 Regresar al paso 2.7.2

2.8 Se incrementa i en uno.

2.9 Se regresa al paso 2.7

2.10 Se envía el mensaje cifrado, almacenado en el segundo arreglo, y las características del primer arreglo al usuario deseado.

3 Si desea leer un mensaje se realiza lo siguiente:

3.1 Solicitar un primer número entero, que corresponde al número de columnas del arreglo que contiene el mensaje que se va a leer (segundo arreglo).

3.2 Solicitar un segundo número entero, que corresponde al número de renglones del arreglo que contiene el mensaje que se va a leer (primer arreglo).

3.3 Si el primer número entero es igual al número de columnas del arreglo que contiene el mensaje (primer arreglo) y el segundo número entero es igual al número de columnas del arreglo que contiene el mensaje (primer arreglo) se realiza lo siguiente:

3.3.1 Se crea un tercer arreglo matricial de caracteres que tiene el mismo número de renglones y columnas que el primer arreglo.

3.3.2 Se crean dos variables k y l que funcionen como contadores e inicien en cero.

3.3.3 Si la variable k es menor que el número de columnas del segundo arreglo, se realiza lo siguiente:

3.3.3.1 l se inicia en cero.

3.3.3.2 Si la variable l es menor que el número de renglones del segundo arreglo, se realiza lo siguiente:

3.3.3.2.1 Se toma el valor que contenga la posición (k, l) del segundo arreglo.

3.3.3.2.2 Se asigna ese valor al tercer arreglo.

3.3.3.2.3 Se incrementa en uno.

3.3.3.2.4 Se regresa al paso 3.3.3.2

3.3.3.3 Se incrementa k en uno.

3.3.3.4 Se regresa al punto 3.3.3

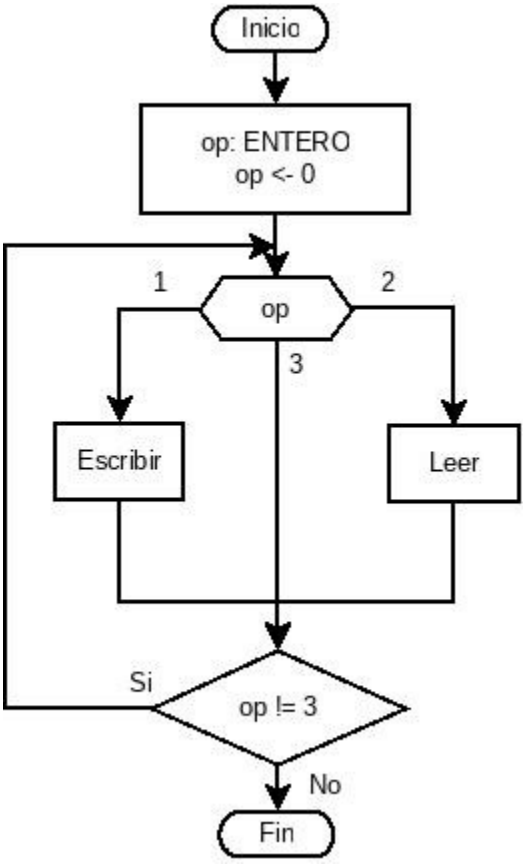
3.3.4 Se muestra el mensaje contenido en el tercer arreglo, el cual corresponde al mensaje descifrado.

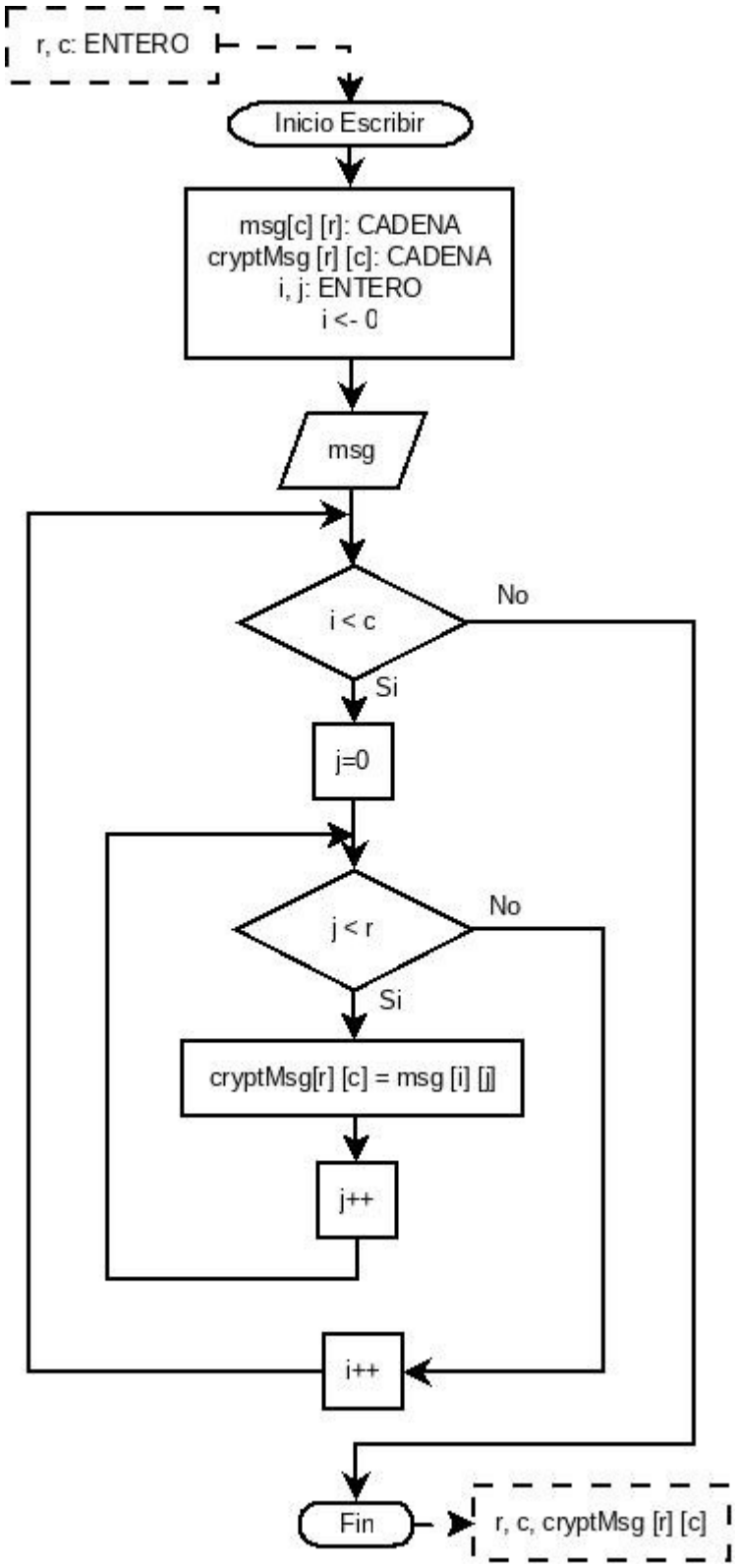
3.4 Se muestra el mensaje contenido en el segundo arreglo, el cual corresponde al mensaje cifrado.

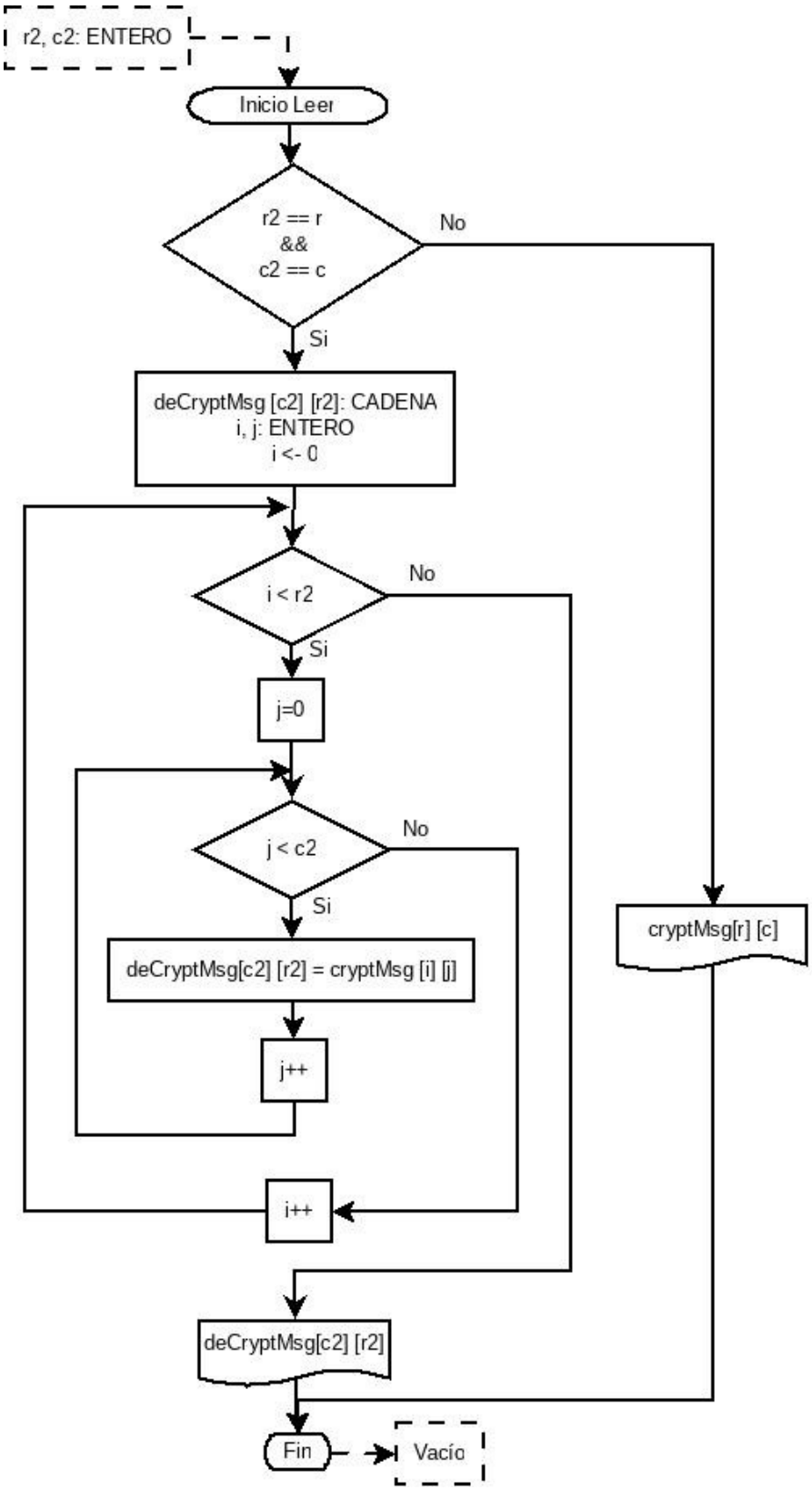
Diagrama de flujo

Notas importantes:

Las variables msg[c] [r], cryptMsg[r] [c] y deCryptMsg[c2] [r2], representan arreglos multidimensionales de caracteres. La función escribir regresa como valor el mensaje encriptado, así como las características del arreglo de caracteres que debe ser utilizado para la lectura de este.




r, c: ENTERO
Inicio Escribir
msg[c] [r]: CADENA
cryptMsg [r] [c]: CADENA
i, j: ENTERO
i <- 0
msg
i < c
No
Si
j=0
j < r
No
Si
cryptMsg[r] [c] = msg [i] [j]
j++
i++
Fin
r, c, cryptMsg [r] [c]


r2, c2: ENTERO
Inicio Leer
r2 == r
&&
c2 == c
No
Si
deCryptMsg [c2] [r2]: CADENA
i, j: ENTERO
i <- 0
i < r2
No
Si
j=0
j < c2
No
Si
deCryptMsg[c2] [r2] = cryptMsg [i] [j]
j++
i++
deCryptMsg[c2] [r2]
cryptMsg[r] [c]
Fin
Vacío

Referencias

Anónimo. (s. f.). Instituto de Matemáticas. *Criptografía.* Recuperado de https://www.matem.unam.mx/~rajsbaum/cursos/web/presentacion_seguridad_1.pdf

Vélez C. (s. f.). Instituto de Ingeniería. *Criptografía*. Recuperado el 6 de marzo de 2021, de http://www.ii.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/criptografia.aspx

Fernández S. (2004). *La criptografía clásica.* Recuperado de https://d1wqtxts1xzle7.cloudfront.net/38520592/9_Criptografia_clasica.pdf?1440040574=&response-content-disposition=inline%3B+filename%3DLA_CRIPTOGRAFIA_CLASICA.pdf&Expires=1615066662&Signature=NWxQHGVg2hYdf4HFOFoT7BPwG~ZzE43Q9l8uXxDBu0LAOHYrDq3ub~jaU~QibhQ9DPcj1LMKzuWeqlVriHbPo11ljR0A2-dPqzMjh2ULP4WhJSKbq758EPjGqie7kHHMMQnjBKb69-VabRrfMVgu1AiUJYcQgXiEXbRfNJ9kzrBHhdtGOEptUyYJYyTYFe~ElipD2aMeGFeNHKcGz-TLnULNiArcyEeQbLtT~b2-bsGFoLAsVzoz6KSeKfZq78WNOkcfNOg79s3Y421U9C1Gp9xCoU1JOvmC7MfN7acD0avxjx21~fHHTeH8epAgqU29fP1VoNLrStbKKKNRls3jJQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA