Universidad Nacional Autónoma de México

Facultad de Ingeniería

Ingeniería en Computación

Estructuras de Datos y Algoritmos I

Actividad Asíncrona Viernes 2

“Escítala espartana”

Alumno: Carmona García Gabriel Alexander

Profesor: Marco Antonio Martínez

07/03/2021

¿Qué es la escítala espartana?

En la antigua Grecia, los espartanos empleaban un curioso método para trasmitir informaciones confidenciales. La referencia a este método se encuentra en el tomo *III* de las *Vidas Paralelas* de Plutarco. Este es un sistema de criptografía utilizado por los éforos espartanos para el envío de mensajes secretos. Está formada por dos varas de grosor variable (pero ambas de grosor similar) y una tira de cuero o papiro, a las que ambas se pueden denominar escítala.

El sistema consistía en dos varas del mismo grosor que se entregaban a los participantes de la comunicación. Para enviar un mensaje se enrollaba una cinta de forma espiral a uno de los bastones y se escribía el mensaje longitudinalmente, de forma que en cada vuelta de cinta apareciese una letra de cada vez. Una vez escrito el mensaje, se desenrollaba la cinta y se enviaba al receptor, que sólo tenía que enrollarla a la vara gemela para leer el mensaje original.

Este funcionaba con una interpretación de la siguiente manera, imaginemos que tras enrollar la tira escribimos un mensaje formado por 3 filas de 9 caracteres de longitud. Al desenrollarla obtenemos una tira con 27 letras. La primera letra de la tira es la primera letra de la primera línea, la segunda letra de la tira es la primera letra de la segunda línea. Así hasta la tercera letra. La letra 4 de la tira es la segunda de la primera fila y continuamos hasta el final. En general la j-ésima letra de la i-ésima fila ocupará el lugar: 3(j−1)+i

E	r	n	u		
n		c	y	n	a
	d	h	o	o	c
u	e	a			o
n		,	n	q	r
	l		o	u	d
l	a	d	m	i	a
u		e	b	e	r
g	M		r	r	m
a	a	c	e	o	e

E	n		u	n		l	u	g	a
r		d	e		l	a		M	a
n	c	h	a	,		d	e		c
u	y	o		n	o	m	b	r	e
	n	o		q	u	i	e	r	o
	a	c	o	r	d	a	r	m	e

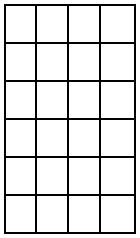
Cuando el mensaje no llena (o cabe, según se considere) completamente la tabla, debe considerarse (esto es: largo(mensaje)/caras no es entero) que se debe añadir 1 fila más y los caracteres de esta fila incompleta considerarse espacios en blanco.

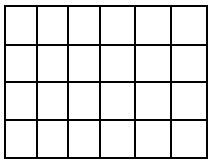
De cara a descifrar un mensaje tal conjunto de caracteres vacíos, pueden suponer una pista para interceptar el número de caras (ancho de la tabla sin cifrar, alto de la tabla cifrada), con que está cifrado el mensaje.

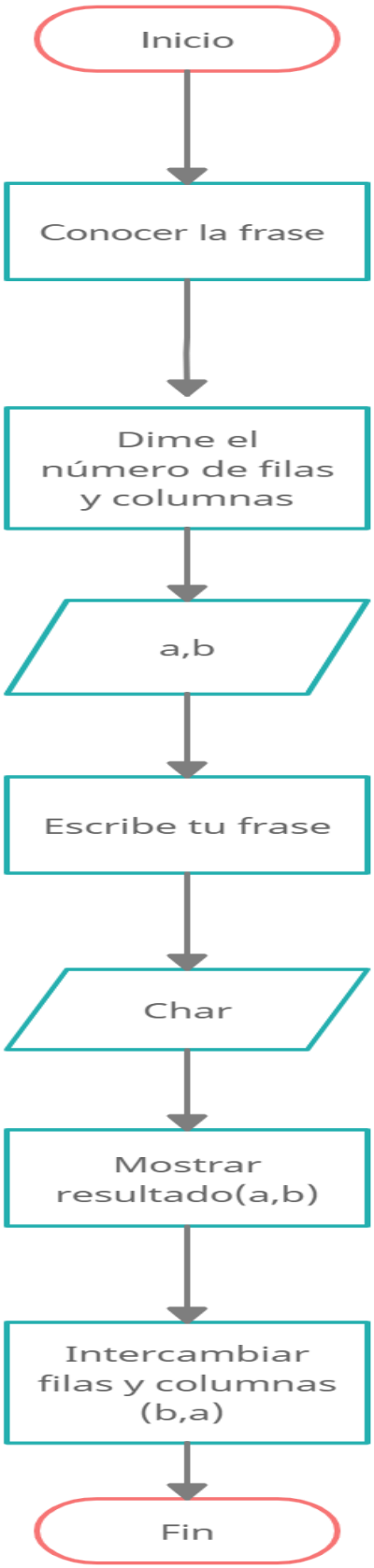
Tanto el primer carácter como el último son los únicos que conservan su posición antes y después del cifrado. En textos muy cortos (palabras, frases cortas), pueden usarse dichos 2 caracteres como un sencillo método de verificación de integridad. Si la tabla es cuadrada, todos los elementos que forman la diagonal (desde la posición 0 hasta el final) también conservan su posición original antes y después del cifrado.

Diseñar un algoritmo para cifrar y descifrar con este mecanismo

1. Conocer la frase que se quiere mandar.
2. Especificar el tamaño del arreglo (filas y columnas).
3. Empezar a escribir la frase.
4. Colocar en orden horizontal las letras puestas hasta que se llene la columna, entonces llenar la siguiente columna (si es necesario dejar espacios en blanco).
5. Mostrar en pantalla el resultado de como quedo para estar seguros.
6. Una vez completado se deberá intercambiar las columnas por las filas y viceversa, por ejemplo, si tenemos 6 filas y 4 columnas, después tendremos 4 filas y 6 columnas.
7. Mostrar el nuevo mensaje.






Inicio
Conocer la frase
Dime el número de filas y columnas
a,b
Escribe tu frase
Char
Mostrar resultado(a,b)
Intercambiar filas y columnas (b,a)
Fin

Bibliografía:

https://joseluistabaracarbajo.gitbooks.io/criptografia-clasica/content/Cripto03.html

https://es.wikipedia.org/wiki/Esc%C3%ADtal