Universidad Nacional Autónoma de México

Facultad de Ingeniería

Asignatura: Estructura de Datos y Algoritmos 1

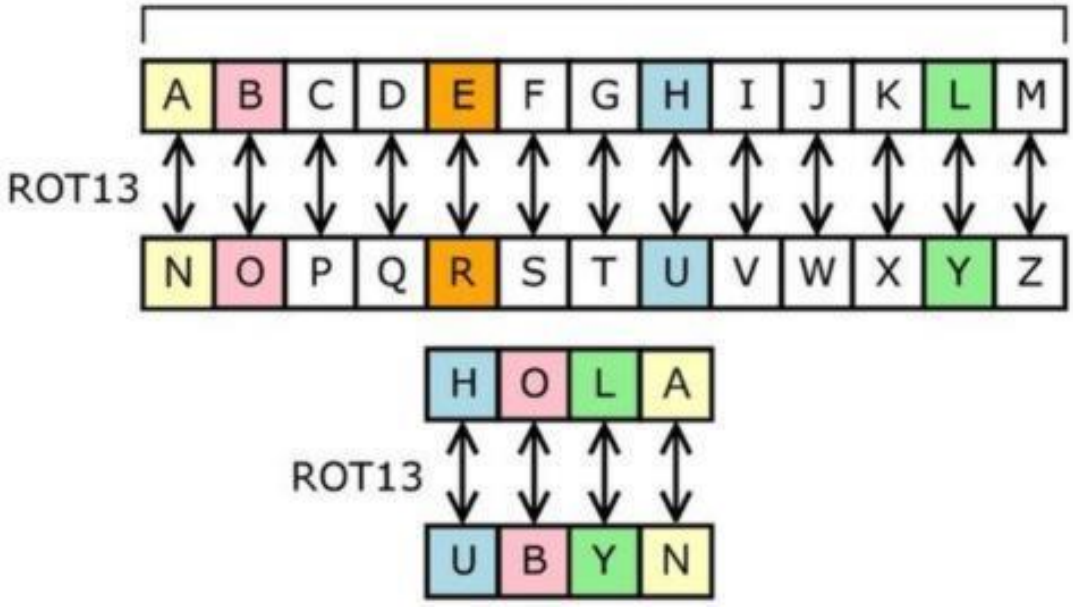
Actividad 4: Cifrado César

Alumna: Hernández Vázquez Daniela

Profesor: M.I. Marco Antonio Martínez Quintana

Fecha: 18/03/2021

2021-2



Actividades:

- Buscar y describir en qué consiste el cifrado César, realizar un algoritmo y diagrama de flujo para su implementación.

Cifrado César

Un cifrado César es una técnica de cifrado sencilla, la cual consiste en sustituir cada letra del abecedario por una letra desplazada un determinado número de posiciones, por ejemplo, si la "clave" es 1, entonces remplazaríamos la A con la B, la C con la D, la O con la P y así sucesivamente hasta que la Z sea sustituida por la A, es decir, nos desplazaríamos una posición. En caso que le pongamos por ejemplo 13, entonces la letra adquirirá el valor de la letra cuyo valor sea la 13va posición a partir de ella, ósea la A será N, la B será O, etc.

El cifrado Cesar lleva este nombre ya que era el método que el famoso gobernante romano Julio César (100 a. C. – 44 a. C.) utilizaba para encriptar mensajes militares y comunicación secreta. Es uno de los métodos de cifrado más simple, se considera un método débil de criptografía, ya que es fácil decodificar el mensaje. En el siglo XIX, la sección de anuncios personales en los periódicos a veces se usaba para intercambiar mensajes encriptados usando esquemas de cifrado simples.

Algoritmo

- *Datos de entada: Mensaje encriptado/desencriptado, "clave" (número entero entre 1 y 27).*
- *Datos de salida: Mensaje encriptado/desencriptado.*

1. Inicio
2. Si se desea encriptar continúe en el paso 3, si se desea desencriptar continúe en el paso 8.
3. Introducir la clave o el número de lugares que se va a desplazar el alfabeto para la encriptación (entre 1 y 27, enteros). Ej: 5
4. Escribe el alfabeto
5. Elige una letra, cuenta 5 espacios luego de esta y anota la letra de la casilla donde te encuentras ahora.

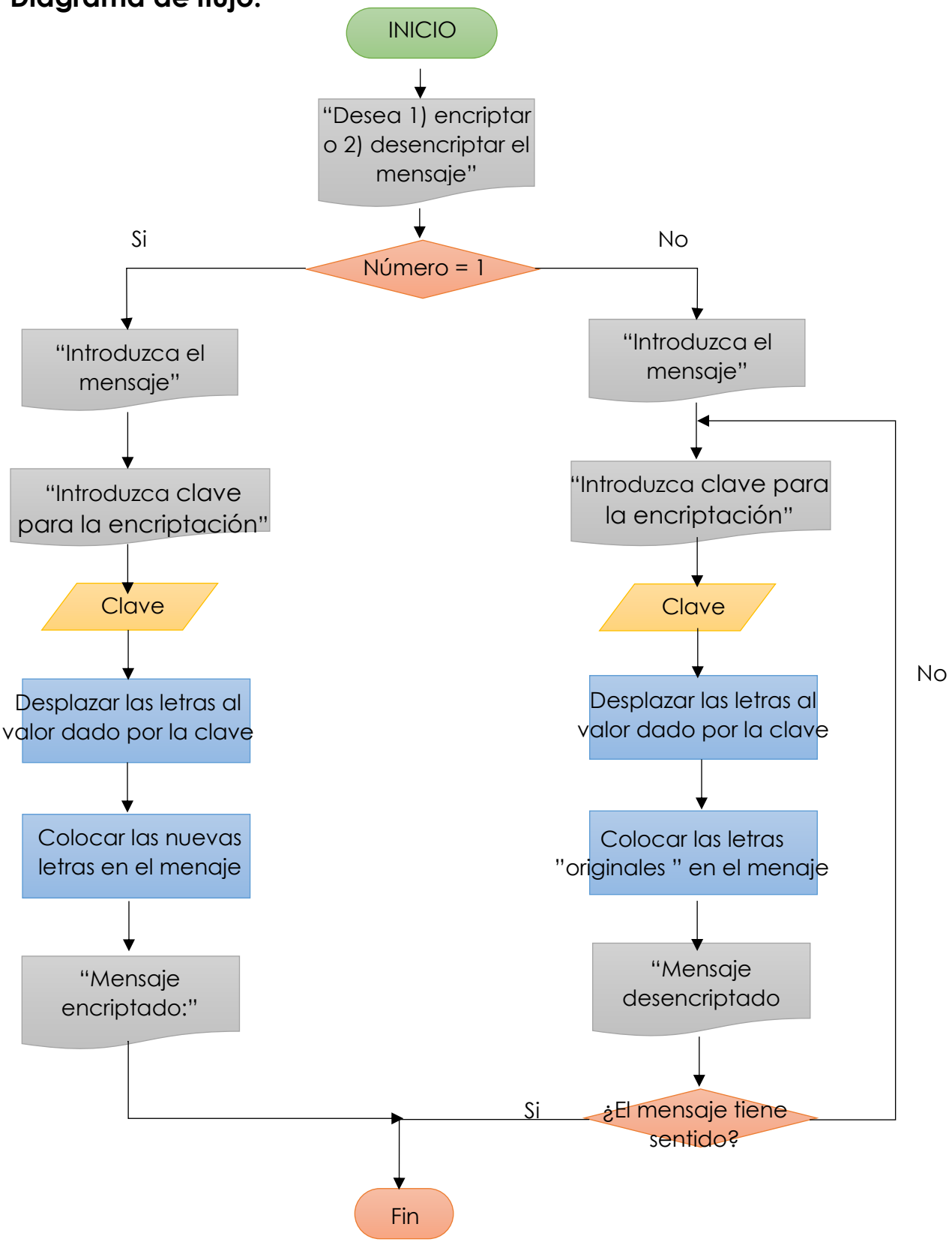
1	2	3	4	5	6	7	8	9	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

6. Escribir el mensaje que deseas cifrar. Ej: "EL OBJETIVO FUE ELIMINADO"
7. El texto cifrado se obtiene sustituyendo cada letra por la posición de su valor más 5, en este caso el mensaje cifrado será: "JP TGÑJYNAT KZJ JPNQNRFIT"
8. Introducir la clave o el número de lugares que se va a desplazar el alfabeto para la desencriptación (entre 1 y 27, enteros). Ej: 5
9. Escribir el mensaje que deseas descifrar. Ej: "JP TGÑJYNAT KZJ JPNQNRFIT"
10. Acomoda el abecedario, cuenta 5 espacios luego de las letras y escribe el nuevo abecedario.

1	2	3	4	5	6	7	8	9	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

11. Sustituye las letras del mensaje encriptado con las del nuevo alfabeto
12. lee el mensaje
13. Si el mensaje no tiene sentido regresar al punto 8 y cambia la clave hasta que el mensaje tenga sentido.
14. Fin

Diagrama de flujo.



Conclusión:

El cifrado César no tiene mucha seguridad que digamos ya que es muy sencillo desencriptarlo, este cifrado es uno de los más simples ya que solo hay 27 combinaciones posibles (una por cada lugar dentro del abecedario).

Este tipo de cifrado se puede implementar en un dispositivo de rueda como en algunos lugares que investigue que tiene el alfabeto impreso, una segunda rueda más pequeña y móvil con el mismo alfabeto. La rueda interior se puede girar para que cualquier letra de una rueda se pueda alinear con cualquier letra de la otra rueda. Y desplazarlas hasta encontrar la clave del mensaje.

Bibliografía

- El lenguaje de programación C. Brian W. Kernighan, Dennis M. Ritchie, segunda edición, USA, Pearson Educación 1991.
- Anónimo. (2020). ¿Qué es el cifrado César y cómo funciona?. (18.03.21), de Ayuda Ley Protección Datos (LOPDGDD) Sitio web: https://ayudaleyprotecciondatos.es/2020/06/10/cifrado-cesar/