

# Guía Práctica de Laboratorio

## Sesión 12: INTRODUCCIÓN A LA PROGRAMACIÓN

### MLBC - VACJ - CJFV

## 1. Cifrado de mensajes

En el mundo del espionaje, uno de los temas más apasionantes es construir y descubrir mensajes cifrados. Se conocen varias técnicas para ello.

Se requiere programar un analizador de estos mensajes, que permita jugar el rol de cifrador y decifrador de mensajes, utilizando la estrategia de sustitución, que consiste en sustituir letras del mensaje por otras.

En esta versión del analizador de mensajes, cada mensaje tiene una clave, que se utiliza para obtener el mensaje cifrado.

Por ejemplo, si el mensaje es “esta noche habra un ataque de dragones” y la clave de cifrado es “eucalipto”; el mensaje cifrado será “usol neahu hlbrl en lolqcu du drlgenus”, lo que se ha hecho es reemplazar cada letra del mensaje original que aparece en la clave con la letra que le sigue en la clave. En este caso toda letra ‘e’ se reemplaza con ‘u’, toda ‘u’ se reemplaza con ‘c’ y así sucesivamente usando la palabra clave. Cuando llegas a la ‘o’ ésta se reemplaza con la ‘e’.

Para que esta estrategia, tenga un mensaje cifrado no ambiguo se requiere que la clave sea una en la que no existen letras repetidas; por ejemplo: “casa” no es una buena clave de cifrado. La palabra clave no puede incluir espacios en blanco, ni símbolos de puntuación.

Considerando este contexto se te pide diseñar un programa que permita:

- dado un mensaje, conseguir el mensaje cifrado (método *cifrar*)
- dado un mensaje cifrado, conseguir el mensaje original (método *decifrar*)
- mantener el registro de los mensajes que ha atendido
- reportar los mensajes que no han podido ser cifrados y/o decifrados a causa de una clave no adecuada
- reportar todos aquellos mensajes en los cuales la palabra “guerra” este presente

Recuerda que cada mensaje tiene su propia clave de cifrado.

## 2. Mas cifrado

Otra estrategia de cifrado es la traslación de letras del mensaje de un lugar a otro, de acuerdo a una clave.

En esta versión del analizador, la clave es un número entero positivo; con el cual cada mensaje se transforma.

Por ejemplo, si el mensaje es “tengo frio habra temporada de hielo” y la clave es 453789; el mensaje cifrado será “tenr ofgoi hatar bmepordad a ehiecaobled”, lo que se ha hecho es aplicar la clave para reubicar (trasladar), caracteres del mensaje en cada porción de diez caracteres. En caso de que el mensaje no tenga bloques de diez caracteres, lo que se hace es completar la cadena con tantas letras como le falte, considerando el alfabeto ingles.

Para entender el proceso, se muestra la forma de cifrar el mensaje anterior con clave 453789:

clave	mensaje
	tengo frio habra temporada de hieloabcde
	0123456789012345678901234567890123456789
453789	^^ ^^ ^^ ^^
--	teng ofrio habar temporaad de hielaobcde
	0123456789012345678901234567890123456789
453789	^ ^ ^ ^ ^ ^ ^ ^
--	tenr ofgio hatar bempordad ae hiecaoblde
	0123456789012345678901234567890123456789
453789	^^ ^^ ^^ ^^
--	tenr ofgoi hatar bmepordad a ehiecaobled
	0123456789012345678901234567890123456789

Hay casos especiales que debes considerar para esta técnica de cifrado, a continuación se presenta algunos.  
**CASO 1:**

clave	mensaje
	cuento las horasabcd 01234567890123456789
3845744	^ ^ ^ ^
--	cueato lns hocasabrd 01234567890123456789
3845744	^^ ^^
--	cueaot lns hocsaabrd 01234567890123456789
3845744	^ ^ ^ ^
--	cuealt ons hocbaasrd 01234567890123456789
3845744	^ ^ ^ ^
--	lueact onsbhoc aasrd

En caso de faltarte un dígito para trasladar debes usa el 0 como la pareja a rotar  
**CASO 2:**

clave	mensaje
	cuento las horasabcd 01234567890123456789
3344556	
--	se ignora este cambio y se avanza en 1 cuento las horasabcd
3344556	01234567890123456789
--	^^ ^^
	cuetno las hoarsabcd 01234567890123456789
3344556	^^ ^^
--	cueton las hoasrabcd 01234567890123456789
3344556	^^ ^^
--	cueto nlas hoasarbcd

En caso de tener dos dígitos iguales en la aplicación de la traslación, entonces se ignora uno y se continua con el siguiente dígito para emparejar.

### CASO 3:

```
clave      mensaje
           cuento las horasabcd
           01234567890123456789
3333333
--         se ignora este cambio y se avanza en 1
3333333
--         se ignora este cambio y se avanza en 1
3333333
--         se ignora este cambio y se avanza en 1
3333333
--         se ignora este cambio y se avanza en 1
3333333
--         se ignora este cambio y se avanza en 1
3333333
--         se ignora este cambio y se avanza en 1
```

En caso de tener la clave no es correcto por lo que se debería informar que hay un error en el cifrado y/o descifrado.

En este caso, es posible que el mensaje cifrado, tenga más caracteres que el mensaje original.

En caso de que quieras decifrar un mensaje, el mensaje siempre tendrá un número múltiplo de 10 de caracteres, caso contrario decifrar será imposible - es un error.

Ejemplo del decifrar del primer mensaje sería:

```
clave      mensaje
           tenr ofgoi hatar bmepordad a ehiecaobled
           0123456789012345678901234567890123456789
453789
--         tenr ofgio hatar bempordad ae hiecaoblde
           0123456789012345678901234567890123456789
453789
--         teng ofrio habar temporaad de hielabcde
           0123456789012345678901234567890123456789
453789
--         tengo frio habra temporada de hielabcde
```

Considerando este contexto se te pide diseñar un programa que permita:

- dado un mensaje, conseguir el mensaje cifrado
- dado un mensaje cifrado, conseguir el mensaje original
- mantener el registro de los mensajes que ha atendido
- reportar los mensajes que no ha podido cifrar y/o decifrar a causa de una clave no adecuada