

**Informe de proyecto #1**

**Materia:** Criptografía y seguridad informática

**Docente:** Ing. Perez Delgadillo Shirley Eulal

**Grupo:** JAVA

**Integrantes:**

* Soldado Brandon
* Astete Yaroslav
* Perez Luis
* Hidalgo Riffarachi Osmar Javier

Contenido

[Métodos de cifrado 2](#_Toc135774650)

[Cifrado por transposición 2](#_Toc135774651)

[Cifrado por transposición en grupos 2](#_Toc135774652)

[Cifrado por transposición en series 4](#_Toc135774653)

[Cifrado por transposición en columnas 5](#_Toc135774654)

[Cifrado por transposición en filas 6](#_Toc135774655)

[Cifrado por transposición en zigzag 7](#_Toc135774656)

[Cifrado por sustitución 8](#_Toc135774657)

[Cifrado por sustitución monoalfabetica 9](#_Toc135774658)

[Cifrado por sustitución polialfabetica 11](#_Toc135774659)

# Métodos de cifrado

Existen varios tipos de cifrado y sus orígenes se remontan a tiempos de culturas antiguas como la griega o romana aun así se podrían dividir en dos categorías principales:

* Cifrado por transposición
* Cifrado por sustitución

## Cifrado por transposición

En criptografía, un cifrado de transposición (también conocido como cifrado de permutación) es un método de cifrado que codifica las posiciones de los caracteres (transposición) sin cambiar los caracteres mismos.

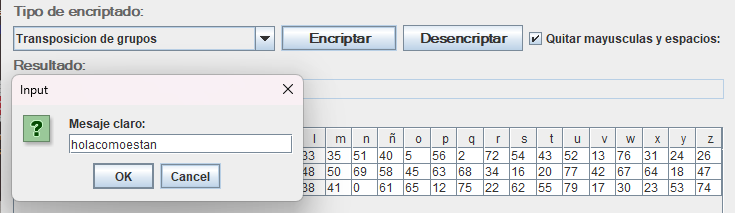
Para la implementación se reconoce a la agrupación de carácter que se usan para conformar un texto plano como alfabeto.

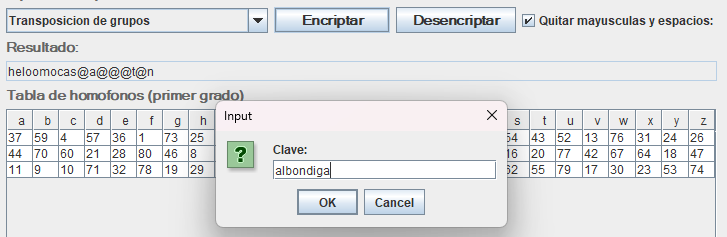
### Cifrado por transposición en grupos

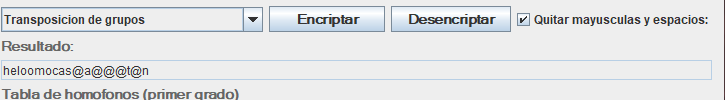
La permutación por grupos se realiza dividiendo el mensaje a cifrar en unidades homogéneas de n elementos y realizando una permutación entre los elementos de este grupo de n elementos.

Para su implementación se ingresa una clave por parámetro y se divide el tamaño del mensaje a cifrar por el de la clave con esto se obtiene la cantidad de grupos a separar y las posiciones de las palabras en la clave en función del alfabeto para permutar cada grupo.

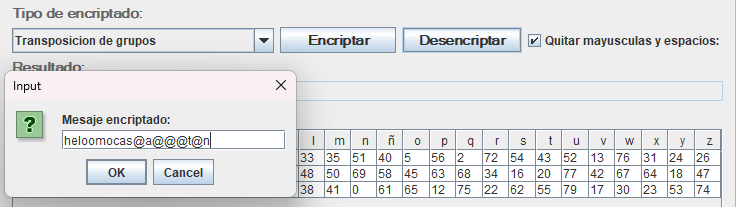
**Cifrado**

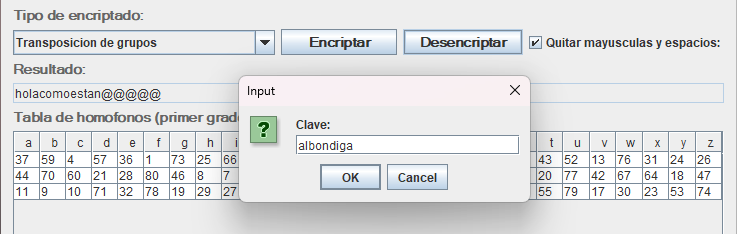


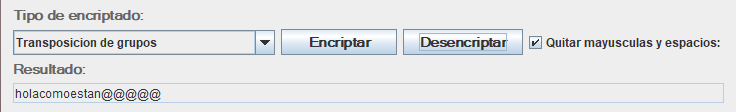




**Descifrado**







### Cifrado por transposición en series

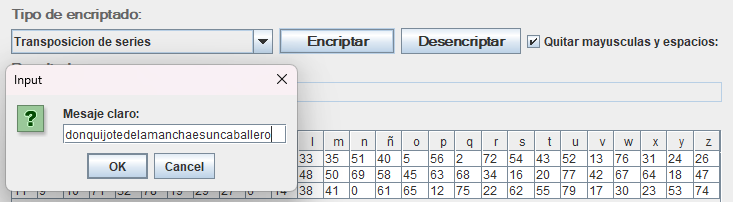
Es similar al anterior, pero en vez de usar una clave como criterio para cifrar sobre un texto plano se usan series de números.

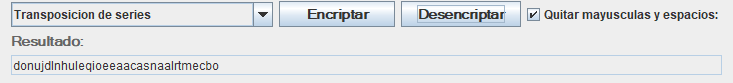
Para su implementación se definieron tres series excluyentes entre si:

1. Números primos
2. Números no primos pares
3. Números no primos impares

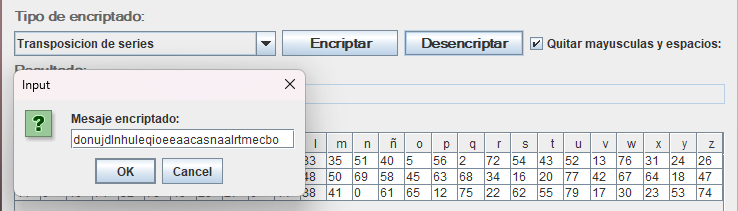
Luego se usan estas como índices para permutar los caracteres obteniendo el cifrado en el mismo orden descrito

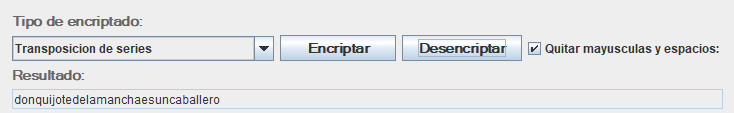
**Cifrado**





**Descifrado**

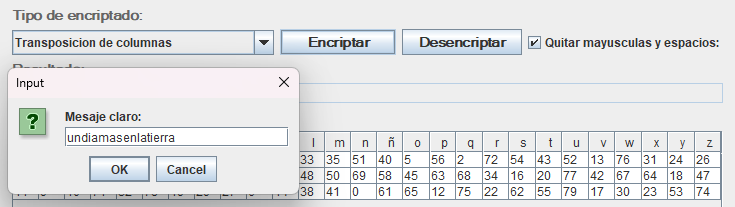
****

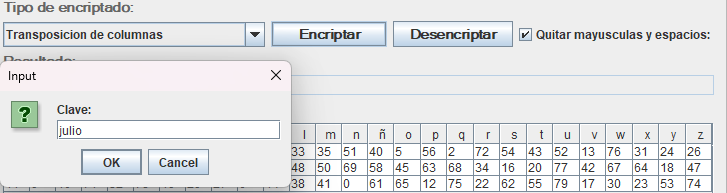
****

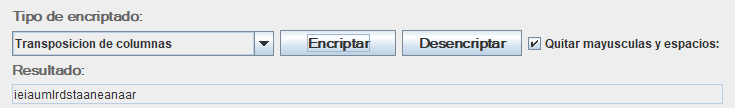
### Cifrado por transposición en columnas

En una transposición en columnas, el mensaje se escribe en filas de una longitud fija, y luego se lee de nuevo columna por columna, y las columnas se eligen en algún orden codificado.

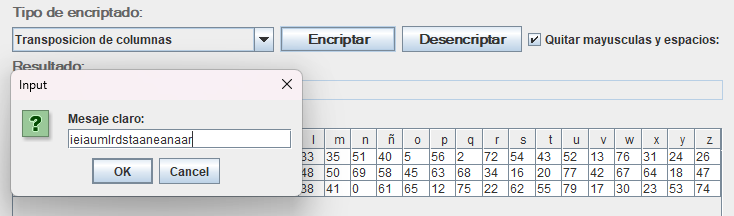
**Cifrado**

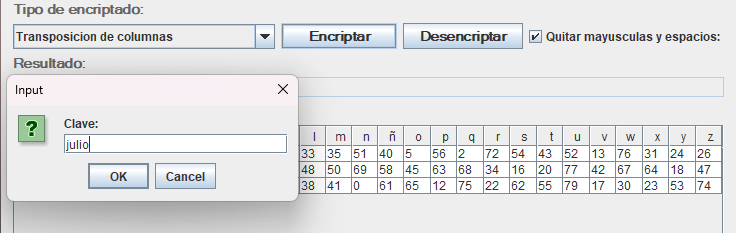
****

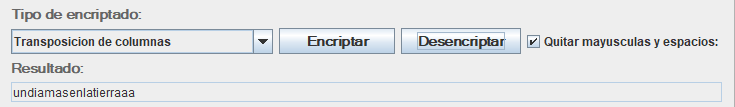
****

****

**Descifrado**







### Cifrado por transposición en filas

En una transposición en filas, el mensaje se escribe en columnas de una longitud fija, y luego se lee de nuevo fila por fila, se eligiendo en algún orden codificado.

**Cifrado**

Funciona de la misma manera que el anterior y devuelve los mimos resultados solo se diferencia en el algoritmo.

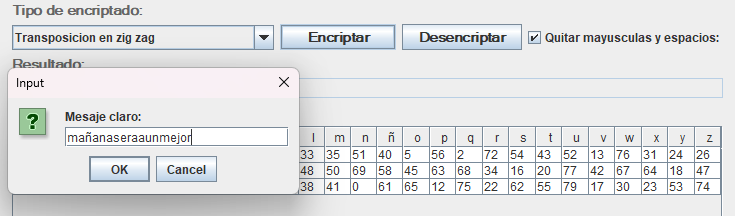
**Descifrado**

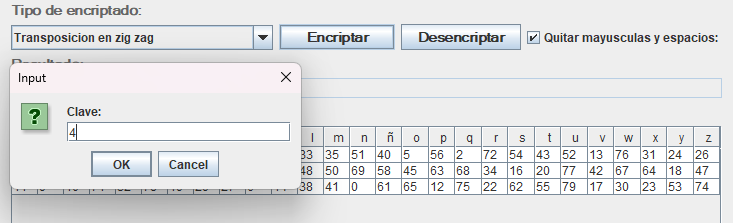
Funciona de la misma manera que el anterior y devuelve los mimos resultados solo se diferencia en el algoritmo.

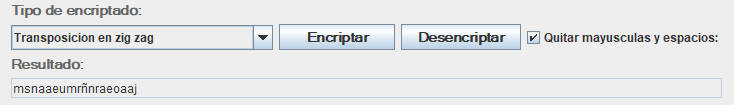
### Cifrado por transposición en zigzag

El cifrado en zigzag es una forma de cifrado de transposición que recibe su nombre de la forma en que está codificado. En el cifrado de la cerca de zig zag, el texto plano se escribe hacia comenzando hacia abajo en zigzag. A continuación, el mensaje se lee en filas.

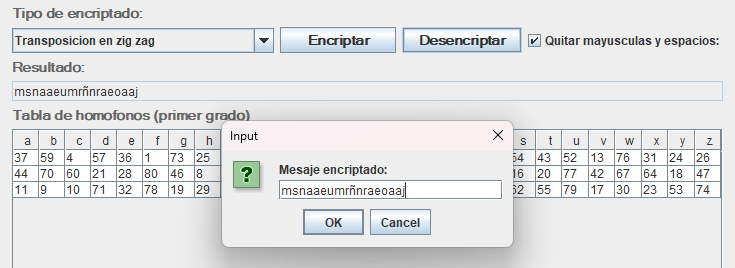
**Cifrado**

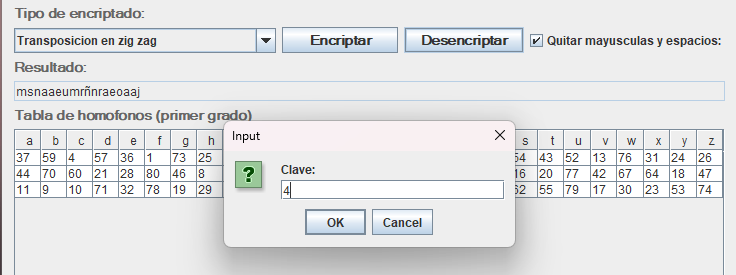
****

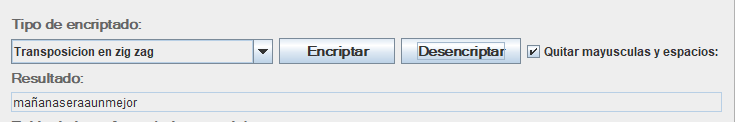
****

****

**Descifrado**







## Cifrado por sustitución

En criptografía, un cifrado de sustitución es un método de cifrado en el que las unidades de texto plano se reemplazan con el texto cifrado, de una manera definida, con la ayuda de una clave.

Además, dependiendo del método para realizar la sustitución podemos clasificarlas en:

* Mono alfabéticas
* Poli alfabéticas

### Cifrado por sustitución monoalfabetica

Es cuando para la sustitución de caracteres se usa un alfabeto, ósea para cada carácter existe un equivalente en otro alfabeto.

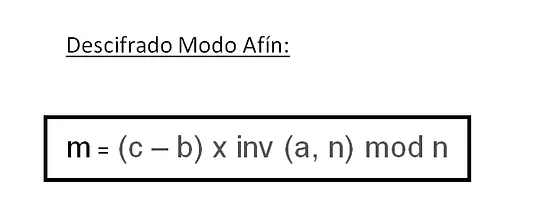
#### Por desplazamiento genérico

Es un tipo de cifrado por sustitución en el que cada símbolo del alfabeto en claro (el alfabeto del texto en claro) es sustituido por un símbolo del alfabeto cifrado (el alfabeto del texto cifrado) siendo el número de símbolos del alfabeto en claro igual que el número de símbolos del alfabeto cifrado. Para hallar el símbolo del alfabeto cifrado que sustituye a un determinado símbolo del alfabeto en claro, se usa una función matemática afín en aritmética modular.

Para cifrar:



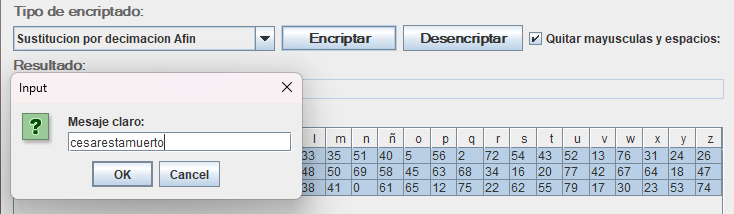
Para decifrar:

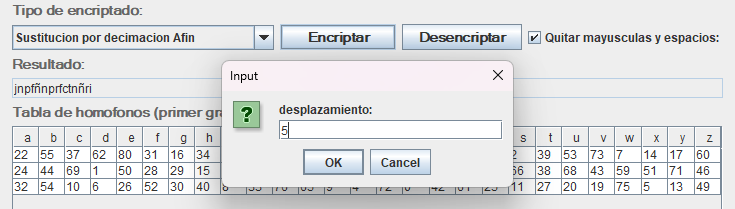


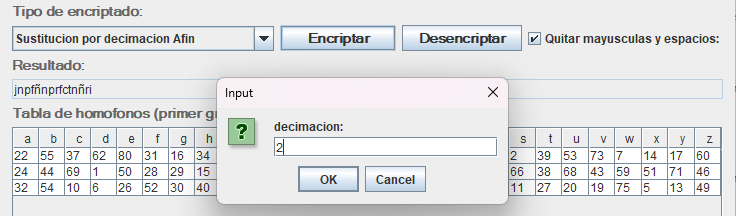
Además, en este caso podemos hacer notar casos especiales:

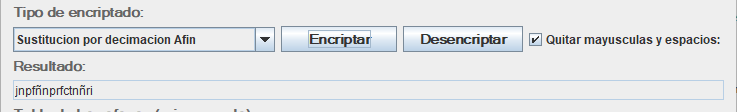
* Cifrado desplazamiento puro: cuando a = 1
* Cifrado por decimacion pura: cuando b = 0 y son comprimos(b, n)
* Cifrado afín: cuando a ≠ 1, b ≠ 0 y son comprimos(b, n)

**Cifrado**

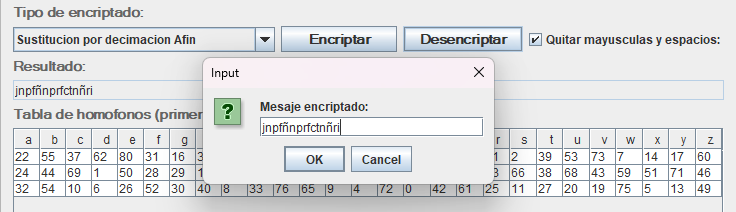
****

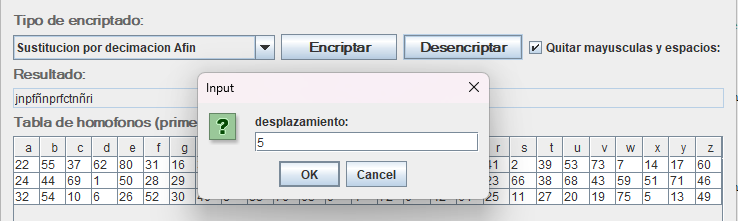
****

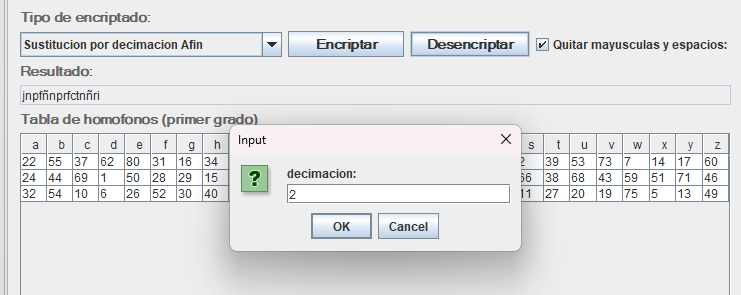
****

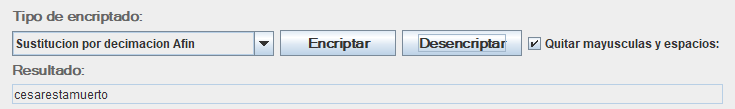
****

**Descifrado**









### Cifrado por sustitución polialfabetica

Es cuando para la sustitución de caracteres se usa más de un alfabeto, ósea para cada carácter existe una n equivalencia en otros muchos alfabetos.

#### Por periodos

En este caso para obtener el alfabeto se desplaza periódicamente por el alfabeto del texto plano generando una n cantidad de alfabetos periódicos. El mas famoso es el

Cifrado de Vigenère que usa una tabla, llamada tabla de Vigenère, que se usa como clave y intercepta el mensaje a cifrar con una clave repetida para obtener el mensaje cifrado.

Al usar alfabetos derivados obtenido por un criterio se puede llegar a expresar matemáticamente como:

Para cifrar:



Para descifrar:



Donde:

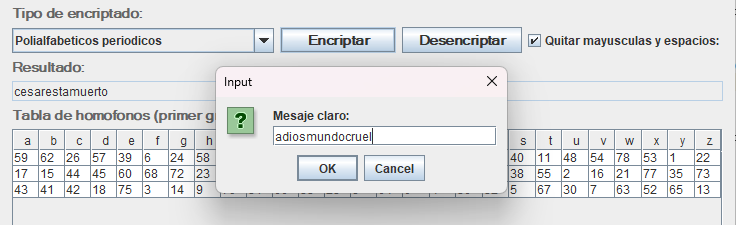
Xi = Es la posición de la letra del texto a cifrar en función de su alfabeto

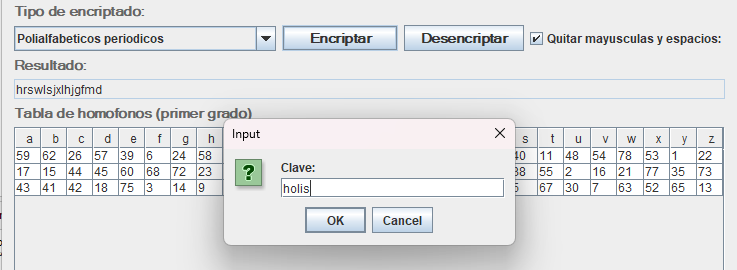
Ci = Es la posición de la letra del texto cifrado en función de su alfabeto

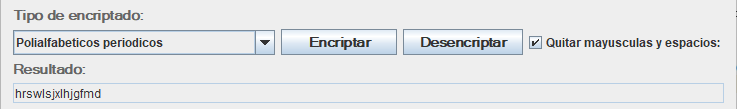
Ki = Es la posición de la letra de la clave para cifrar en función de su alfabeto

L = longitud del alfabeto usado

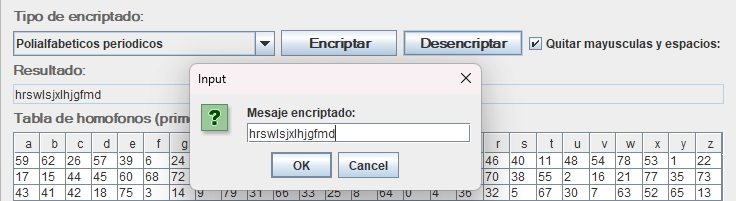
**Cifrado**

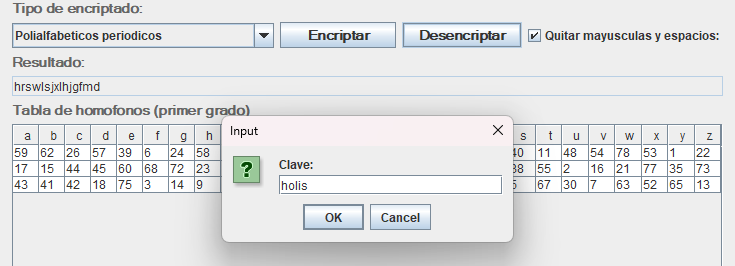
****

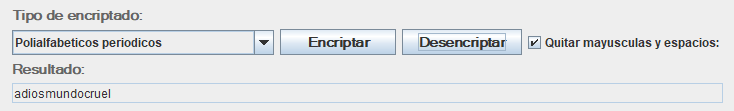
****

****

**Descifrado**





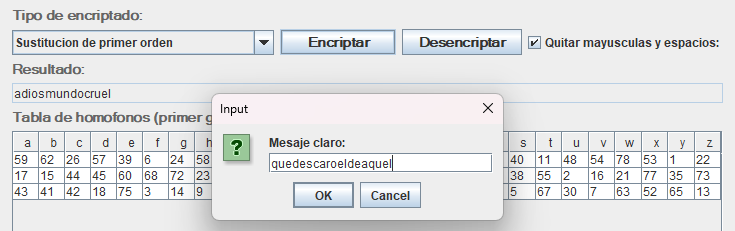


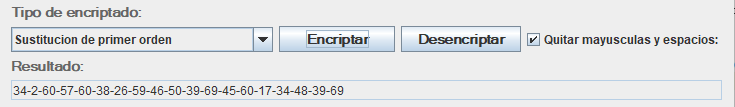
#### Por Homofonos de primer orden

Para este cifrado se usan homófonos, que vendrían a ser equivalentes normalmente numéricos para los caracteres en el alfabeto. Para este caso en particular se requiere de tener una tabla con n homófonos por carácter en el alfabeto.

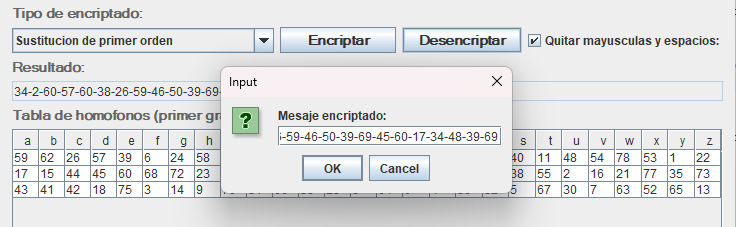
Para su implementación se usaron 3 homófonos por carácter resultando en una tabla del tamaño del alfabeto \* 3 que se rellenó de manera randomica.

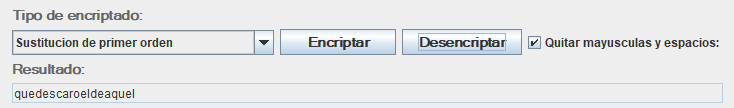
**Cifrado**

****

****

**Descifrado**

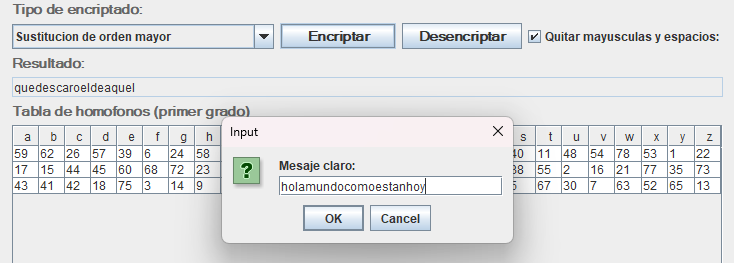


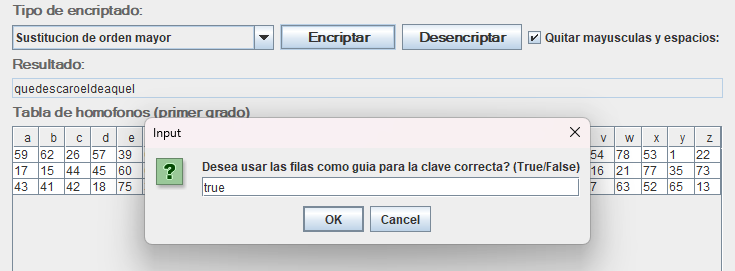


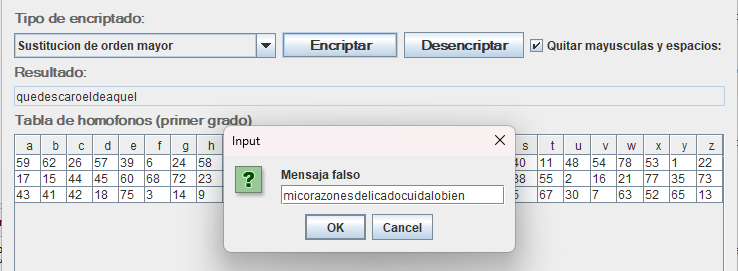
#### Por Homofonos de orden mayor

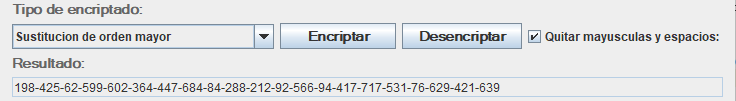
Similar al anterior, pero en este se hace uso de texto falso además del que se encripta por ello a la hora de implementar esto se forma una tabla cuyo orden sea el mismo que el del alfabeto y se intercepta las letras de texto correcto y el falso en función relacionando ya sea las filas o las columnas con los textos clase y claro.

**Cifrado**

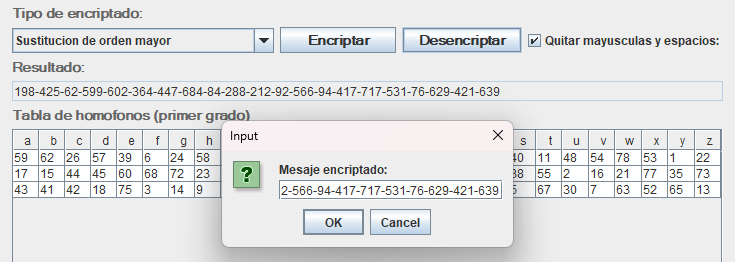
****

****

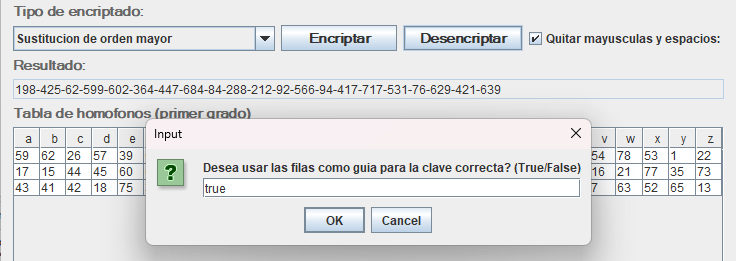
****

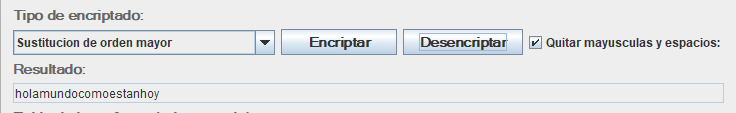
****

**Descifrado**



(mensaje correcto)





(mensaje falso)

