**Tarea Programada #1**

**Criptografía y tipos de criptografía**

**Manual de Usuario**

Samuel Garcés Castillo – 2022129139

Carlos Daniel Guzmán Ramírez – 2022437782

**Contenido**

1. **Introducción**
   1. Objetivo 3
   2. Requerimientos mínimos 3
2. **Navegación del sistema**
   1. Menú principal 4
   2. Menú secundario 4
   3. Validaciones 6
3. **Opciones del sistema**
   1. Cifrado César 8
   2. Cifrado por llave 8
   3. Sustitución Vigenére 9
   4. Sustitución XOR y llave 9
   5. Palabra inversa 10
   6. Mensaje inverso 10
   7. Cifrado telefónico 10
   8. Cifrado binario 11
   9. Terminar ­ 11
4. **Introducción**
   1. **Objetivo**

Otorgar soporte a los usuarios de la tarea programada #1 hecha durante el primer semestre del año 2022 en el TEC.

* 1. **Requerimientos mínimos**
     + Sistema operativo Windows 98 o Superior
     + Mínimo 64Mb en RAM
     + Un teclado
     + Versión de Python 3.10.2 o superior
     + Cualquier visualizador de código compatible con Python.

1. **Navegación del sistema**

**2.1. Menú principal**

Al inicializar el programa, se podrá visualizar un encabezado donde se indican los creadores del sistema, junto a sus respectivos códigos de estudiante.

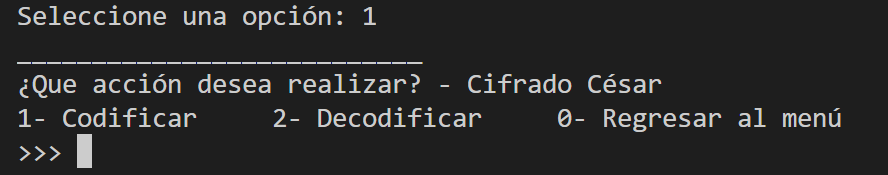
Posteriormente, se muestra el menú principal “Criptografía”, indicando las 9 posibles opciones a elegir: Cifrado César, Cifrado por llave, Sustitución vigenére, Sustitución XOR y llave, Palabra inversa, Mensaje inverso, Cifrado telefónico, Cifrado binario, y Terminar. Cada una de las anteriores serán explicada más adelante. Finalmente, en el pie del menú se muestra una consulta de entra de datos con la inscripción “Seleccione una opción:” donde se procederá a ingresar el numero respectivo a las opciones solicitadas.



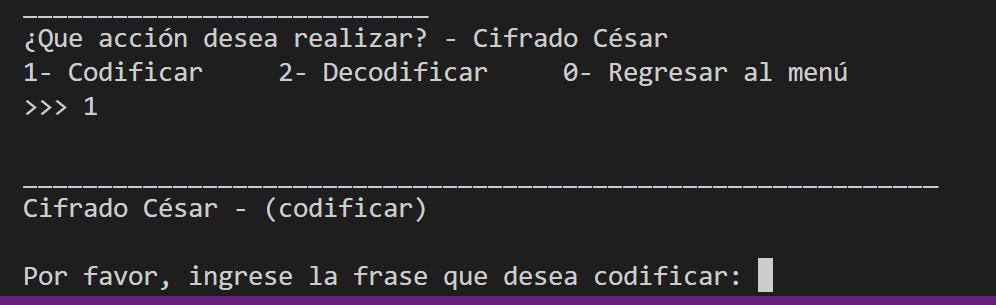
**2.2. Menú secundario**

Al seleccionar alguna de las opciones del menú, el sistema desplegará un menú secundario con el fin de identificar el tipo de acción que desea realizar con el sistema de cifrado correspondiente; ya sea codificar, seleccionando la opción 1, decodificar, seleccionando la opción 2, o ya sea que desee regresar al menú principal, seleccionando la opción 0. Sumado a esto, el menú muestra el tipo de cifrado que se trabajará, según las opciones del menú principal.

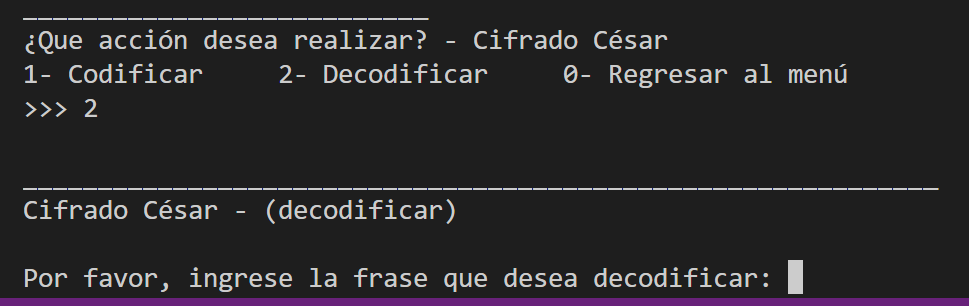
Interfaz básica:



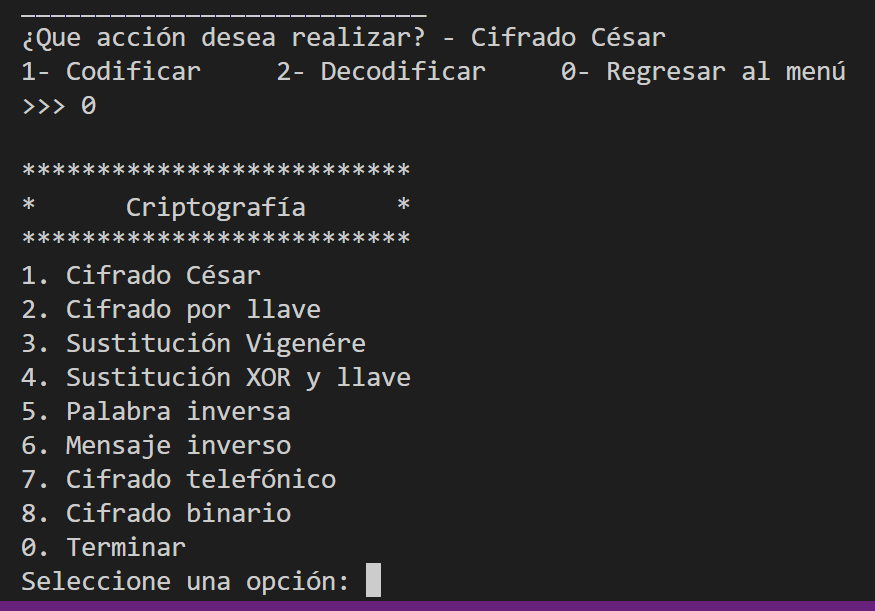
Caso 1:



Caso 2:



Caso 3:



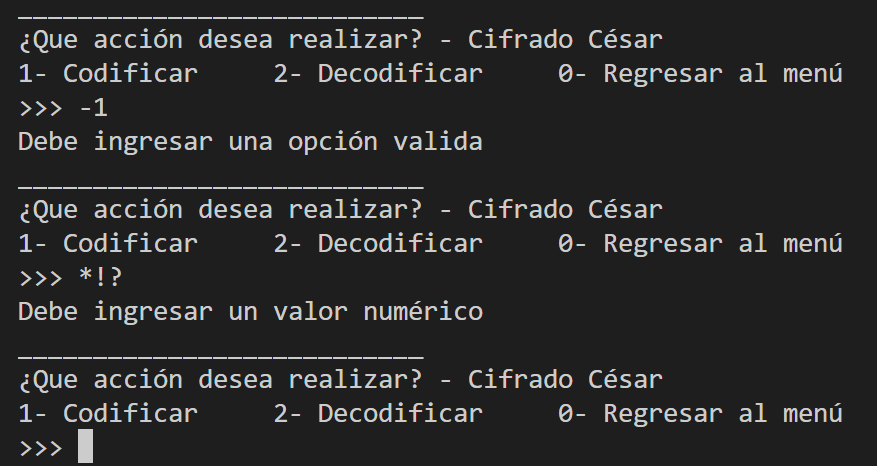
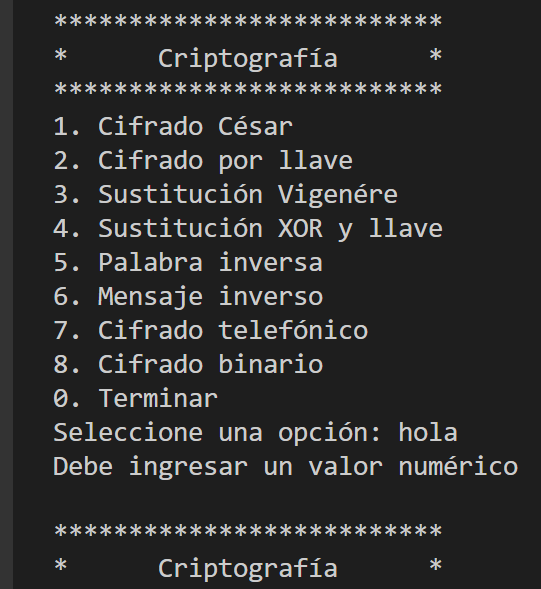
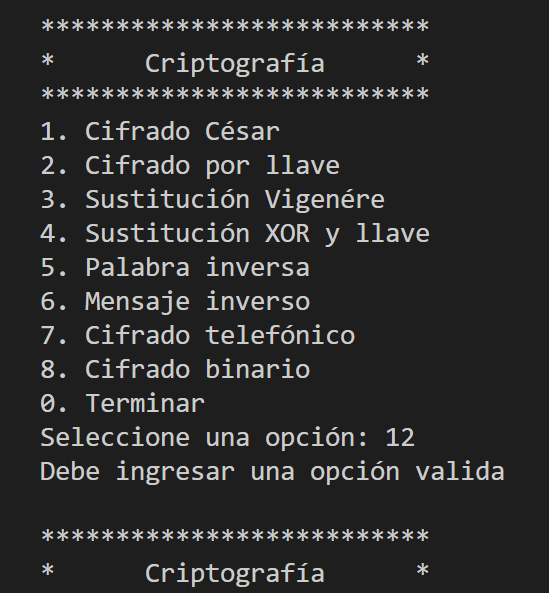
Una vez finalizada la acción correspondiente, el sistema regresará automáticamente al menú principal. Este proceso se repetirá hasta que el usuario indique que desea finalizar el procesamiento, seleccionando la opción 0, “Terminar”.

**2.3. Validaciones**

Para asegurar la robustez del sistema, se trabajó con una serie de validaciones principales que fueron aplicadas recursivamente a lo largo del código. Gracias a ello, se permitió contrarrestar numerosos tipos de errores, asegurando así la integridad de la aplicación. De la misma manera, estas repetirán la consulta de entrada de datos hasta que se realice el proceso de manera correcto. Entre las validaciones principales se encuentran:

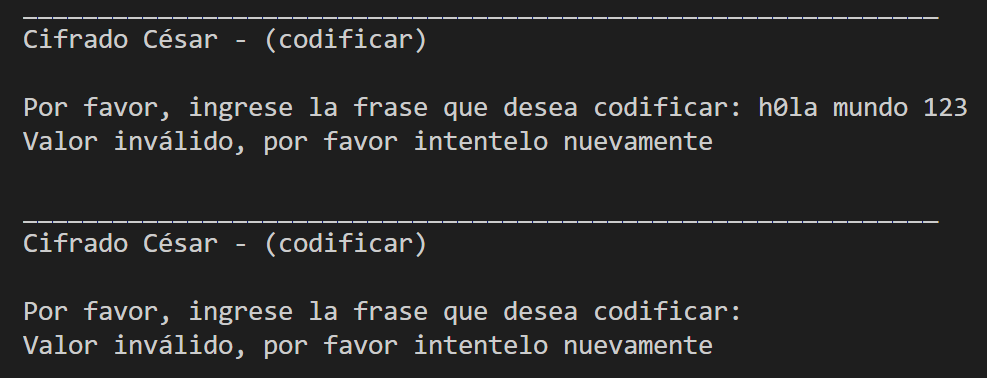
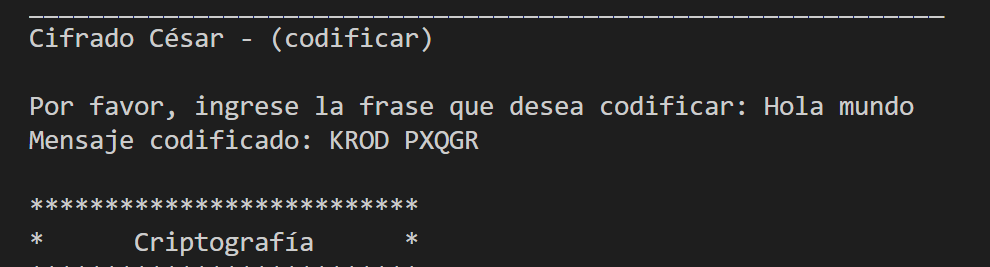
1. Validación del menú:

Asegura el ingreso correcto de las opciones dentro de los menús del sistema.



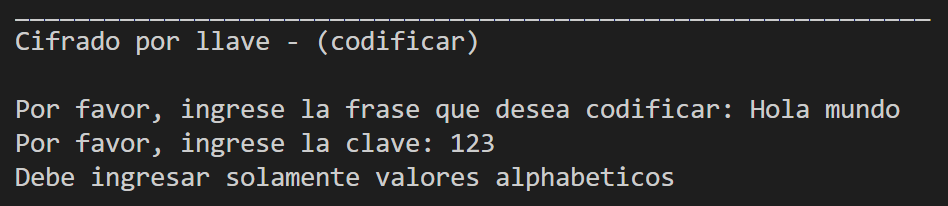
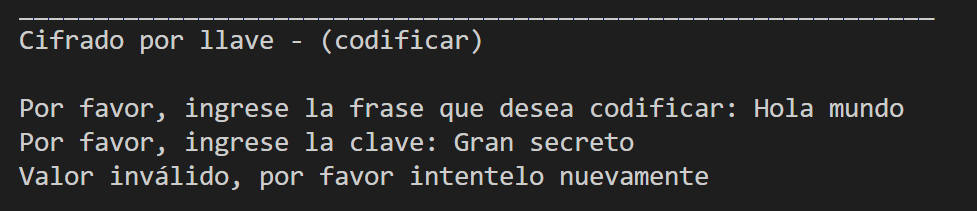
1. Validación de frases:

Asegura el ingreso correcto de frases largas al sistema, únicamente con valores alfabéticos y espacios en blanco. Este tipo de validación se utiliza en la gran mayoría de ingresos de frases a codificar o decodificar



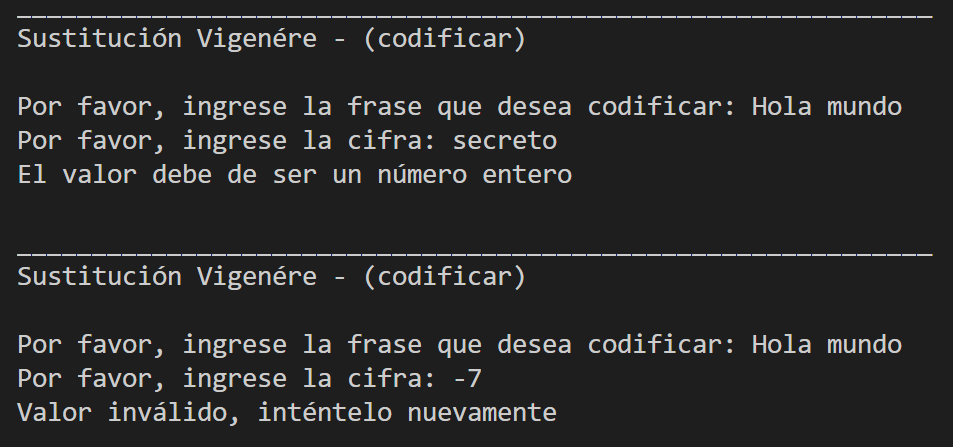
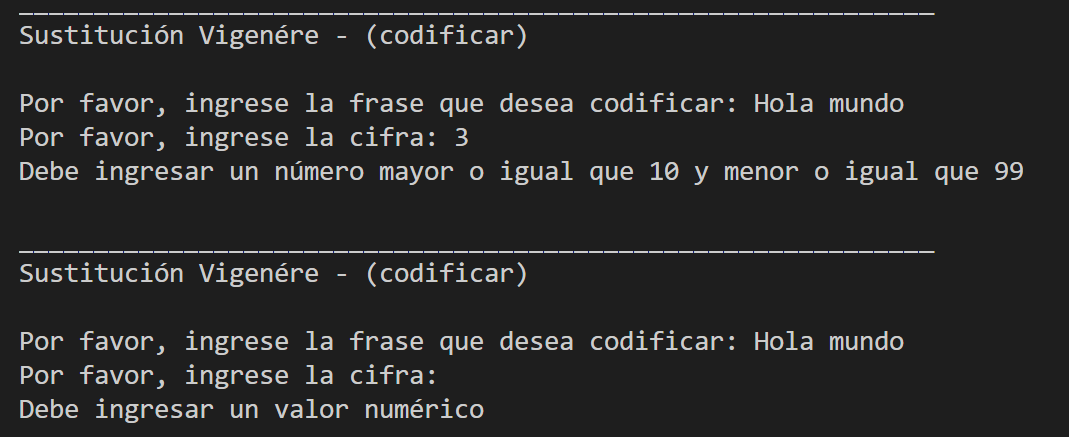
1. Validación de palabras:

Permite el ingreso únicamente de palabras alfabéticas, sin espacios en blanco. Este tipo de validación se utiliza en el ingreso de claves, dado que requieren de una sola palabra.



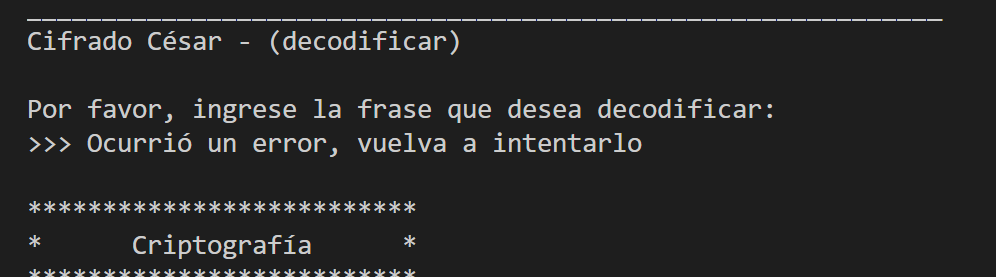
1. Validación numérica:

Permite validar el ingreso de datos numéricos dentro de un rengo determinado. Esta validación se utiliza al trabajar con datos numéricos, como en el caso de la “Codificación Vigenére”.



1. Validación de error desconocido:

Previene la caída del sistema ante la presencia de un error no contemplado bajo las anteriores validaciones.

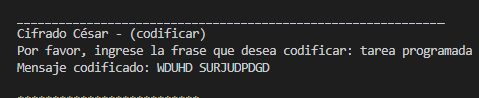


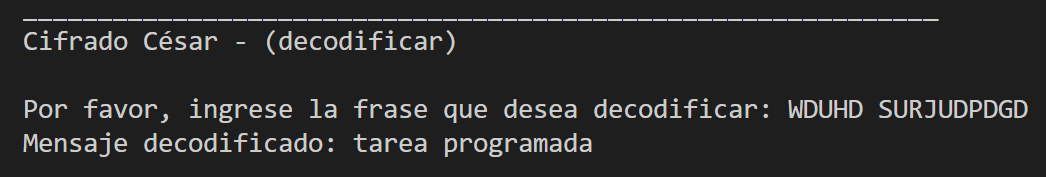
Estas validaciones aplican para toda entrada de datos solicita en el sistema, y su explicación anterior abarca cualquier escenario de prueba posible en los distintos métodos de cifrado presentes en este documento.

1. **Opciones del sistema**

**3.1. Cifrado César**

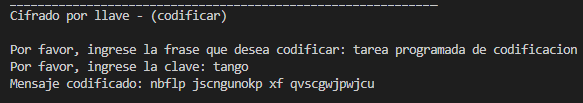
Al seleccionar esta opción, el usuario debe digitar la frase que desea codificar o decodificar, con el fin de ser procesada.

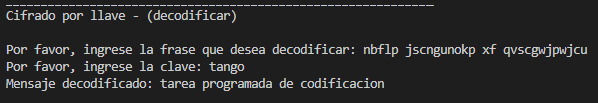


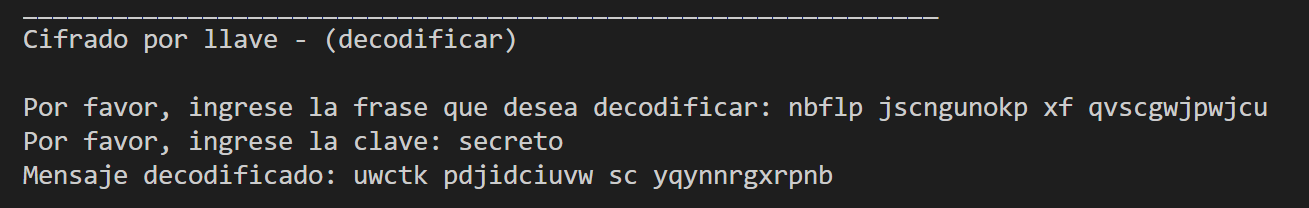


**3.2. Cifrado por llave**

En esta opción, el usuario debe digitar la frase a codificar o decodificar junto a una llave, la cual es una palabra especifica que se vincula a la frase trabajada, y permite su posterior decodificación.

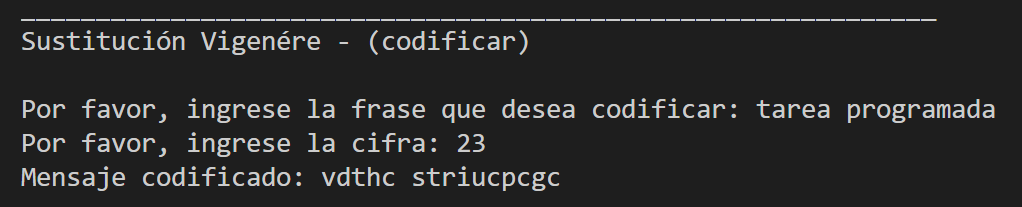


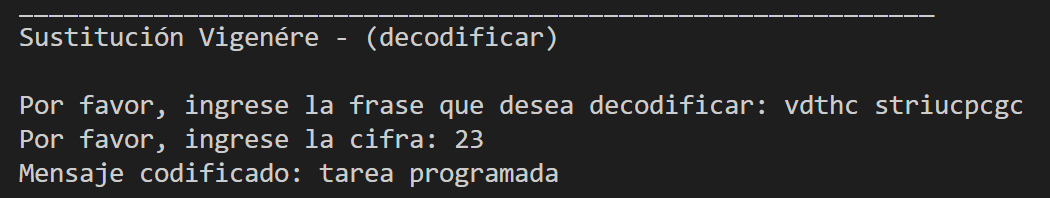


De no brindarse la llave correcta, la frase se decodificará de manera incorrecta

**3.3. Sustitución Vigenére**

En esta opción, el usuario debe digitar la frase y una cifra de 2 dígitos como llave para codificar o decodificar. La cifra ingresada puede ser cualquier número de exactamente 2 dígitos.

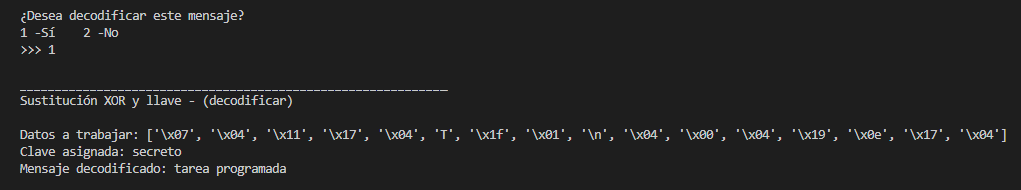


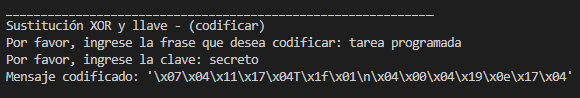


NOTA: Para visualizar un escenario de prueba incorrecto véase el apartado 2.3. Validaciones.

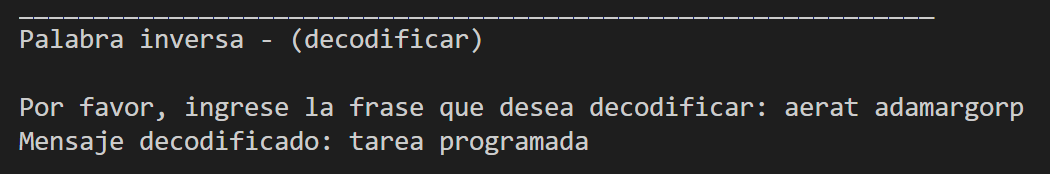
**3.4. Sustitución XOR y llave**

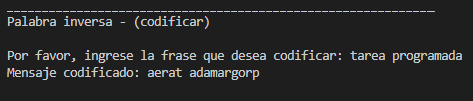
En esta opción, el usuario debe digitar la frase a trabajar, y una llave correspondiente para su codificación. El sistema codificará el mensaje aplicando el método XOR, e imprimiendo el valor ASCII correspondiente al resultado del proceso.

Una vez ingresado los datos, el sistema consulta al usuario si se desea decodificar dicho mensaje, en caso de respuesta afirmativa, se procede a decodificar el mensaje, indicando los datos con los cuales se trabaja.

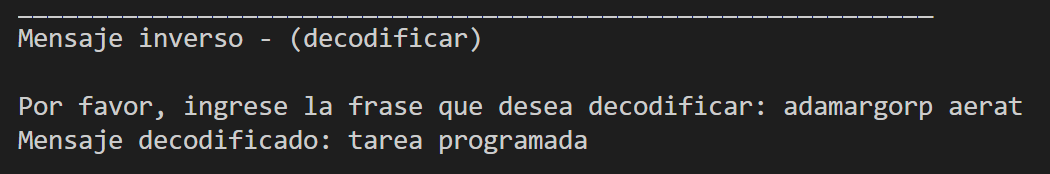
NOTA: La presente característica corresponde a la consulta explícita del cliente el día 24 de abril del 2022, a través de la plataforma *Telegram*.

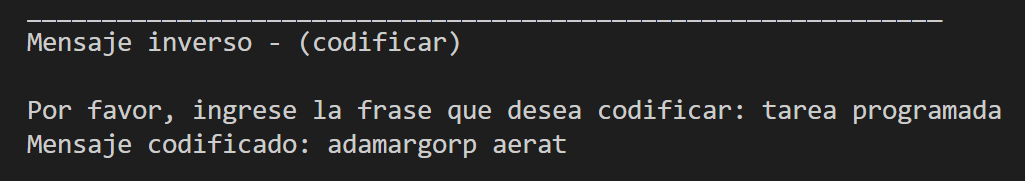
**3.5. Palabra inversa**

Esta opción permite codificar o decodificar la frase que se ingrese, invirtiendo las palabras individualmente de manera automática.



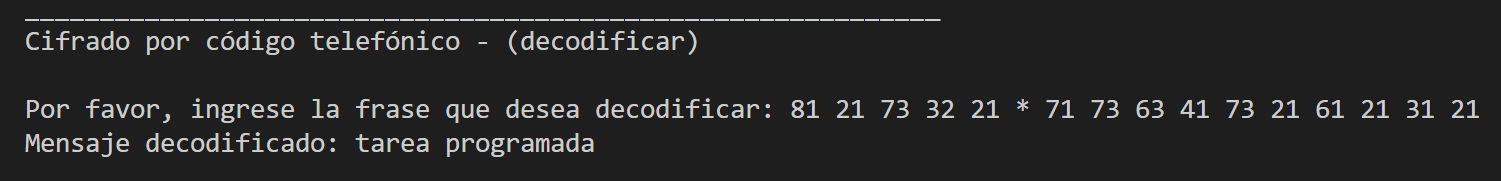
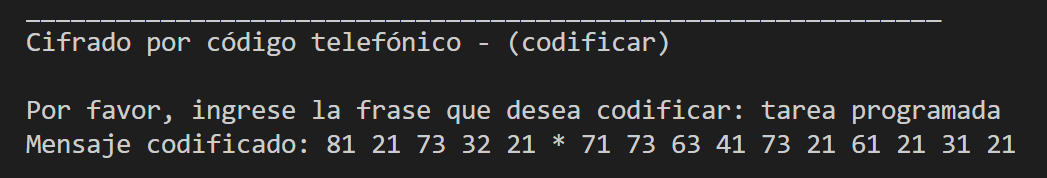
**3.6. Mensaje inverso**

Esta opción permite invertir la frase por completo, codificando o decodificando la información según lo requiera.



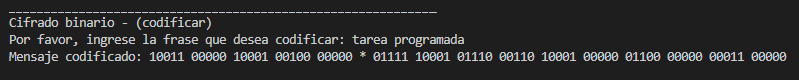
**3.7. Cifrado telefónico**

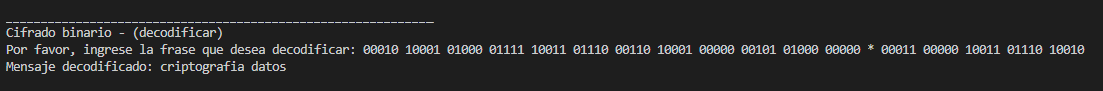
Esta opción permite codificar o decodificar un mensaje según se requiera, utilizando la lógica de las letras asignadas a los botones numéricos de un teléfono público:



**3.8. Cifrado binario**

Esta opción permite codificar y decodificar una frase brindando un código binario de 5 dígitos, correspondientes a todos los valores del alfabeto inglés.





**3.9. Terminar**

Por último, se encuentra la opción "Terminar”, la cual, como su nombre lo indica, permite finalizar la corrida del programa, cerrándolo y terminando todos sus procesos.

