Instituto Tecnológico de Costa Rica

Área Académica de Administración de Tecnologías de Información



Curso:

TI-1400 Introducción a la Programación

Primer Proyecto Programado

Tema:

Técnicas de Cifrado de Mensajes

Profesor:

Ing. Luis Pablo Soto Chaves

Estudiantes:

José Manuel Altamirano Salazar - 2020426159

Josué Brenes Alfaro - 2020054427

Fecha de Entrega:

10 de junio de 2020

**Índice**

[Introducción 3](#_Toc42508414)

[Estrategia Metodológica 5](#_Toc42508415)

[Asignación de roles y tareas 5](#_Toc42508416)

[Mecanismos de Seguimiento 6](#_Toc42508417)

[Reuniones y validación de avances 6](#_Toc42508418)

[Modalidad de Trabajo 7](#_Toc42508419)

[Cronograma de Trabajo 7](#_Toc42508420)

[Manual de Usuario 8](#_Toc42508421)

[Portada 8](#_Toc42508422)

[Introducción: 9](#_Toc42508423)

[Funcionalidad General: 10](#_Toc42508424)

[Requisitos del Programa 10](#_Toc42508425)

[Guía de Uso 13](#_Toc42508426)

[Funcionalidad dentro del programa: 14](#_Toc42508427)

[Opciones de Cifrado de Mensajes: 15](#_Toc42508428)

[1-Cifrados por sustitución: 15](#_Toc42508429)

[1.1. Cifrado Cesar: 15](#_Toc42508430)

[1.2. Cifrado por llave: 16](#_Toc42508431)

[1.3. Sustitución Vigenére: 18](#_Toc42508433)

[2.Cifrado RSA: 19](#_Toc42508434)

[3. Cifrado por Transposición 20](#_Toc42508435)

[3.1 Cifrado por palabra inversa: 20](#_Toc42508436)

[3.2. Cifrado mensaje inverso: 21](#_Toc42508437)

[4.Cifrado telefónico: 22](#_Toc42508438)

[Opciones de Descifrado de Mensajes: 25](#_Toc42508439)

[1-Cifrados por sustitución: 25](#_Toc42508440)

[1.1. Descifrado cesar: 25](#_Toc42508441)

[1.2. Descifrado por llave: 27](#_Toc42508442)

[1.3 Descifrado por Sustitución de Vigenére: 28](#_Toc42508443)

[2.Descifrado RSA: 30](#_Toc42508444)

[3. Cifrado por transposición 31](#_Toc42508445)

[3.1. Descifrada palabra inversa: 31](#_Toc42508446)

[3.2. Descifrado mensaje inverso: 32](#_Toc42508447)

[4.Descifrado telefónico: 33](#_Toc42508448)

[Pruebas de Funcionalidad 36](#_Toc42508449)

[Menú Principal 36](#_Toc42508450)

[Menú Cifrado 39](#_Toc42508451)

[Opción Cifrado César 45](#_Toc42508452)

[Opción Cifrado por Llave 47](#_Toc42508453)

[Opción Cifrado por Sustitución Vigenére 50](#_Toc42508454)

[Opción Cifrado RSA 53](#_Toc42508455)

[Opción Cifrado Palabra inversa 56](#_Toc42508456)

[Opción Cifrado Mensaje inverso 58](#_Toc42508457)

[Opción Cifrado Telefónico 60](#_Toc42508458)

[Opción Cifrado Binario 62](#_Toc42508459)

[Menú Descifrado 64](#_Toc42508460)

[Opción Descifrado César 69](#_Toc42508461)

[Opción Descifrado por Llave 71](#_Toc42508462)

[Opción Descifrado por Sustitución Vigenére 74](#_Toc42508463)

[Opción Descifrado RSA 77](#_Toc42508464)

[Opción Descifrado Palabra inversa 80](#_Toc42508465)

[Opción Descifrado Mensaje inverso 82](#_Toc42508466)

[Opción Descifrado Telefónico 84](#_Toc42508467)

[Opción Descifrado Binario 87](#_Toc42508468)

[Lecciones Aprendidas 89](#_Toc42508469)

[Bitácora de Trabajo 90](#_Toc42508470)

[Análisis de Resultados 91](#_Toc42508471)

[Objetivos Alcanzados 91](#_Toc42508472)

[Objetivos No Alcanzados 91](#_Toc42508473)

[Distribución del Trabajo 92](#_Toc42508474)

# Introducción

Desde las épocas antiguas se han buscado métodos de cómo ocultar un mensaje para que solo lo entienda la persona a la que va destinado. La criptografía se considera todo un arte, se ha usado en muchos campos como en la milicia y en la religión; hoy en día la criptografía se usa mucho en la programación con el objetivo de ocultar documentos o datos. Para la mayoría de estas codificaciones se utilizan algoritmos matemáticos, transposición de letras y números, o conversión de letras a números.

Existen muchos tipos de cifrado, algunos son muy conocidos y utilizados. En el día a día todos utilizamos la criptografía sin darnos cuenta, a partir de que esta ha sido implementada dentro de varios sistemas con los cuales solemos interactuar. Un ejemplo de esto se da cuando hacemos una transferencia de dinero, si los sistemas de banca no utilizaran los datos requeridos para realizar una transferencia, sería muy sencillo acceder a estas transferencias sin antes cifrar estos datos.

Otro ejemplo de la utilización de algoritmos de cifrado sucede cuando se hace una llamada o se envía un mensaje por internet y esta información se encuentra cifrada de extremo a extremo, para que nadie fuera de la llamada pueda ingresar o que alguien pueda leer lo que se envía en el mensaje.

En la actualidad la tecnología es una de las herramientas más utilizadas en el mundo tanto en las empresas, como en los gobiernos y demás instituciones. Al poseer tanta información procesada que se debe mantener segura, se van creando formas de ocultarla, a través de los sistemas de información. Hay secretos que se guardan por motivos varios, a veces es información que podría provocar caos en algún sector, o puede ser que una empresa llegue a la quiebra si personas externas entran a sabotear los sistemas de esta. Para ello es muy importante tener siempre un buen sistema de ciberseguridad.

En este proyecto se buscará desarrollar una solución basada en ocho tipos de cifrados sencillos. El software desarrollado le permitirá cifrar con estos ocho diferentes algoritmos, y descifrar aplicando el proceso inverso sobre los mensajes ya cifrados. de acuerdo de la opción que se haya escogido.

# Estrategia Metodológica

## Asignación de roles y tareas

Para la realización del proyecto, se determinó que la forma más conveniente de trabajar cada uno de sus elementos era a partir de la división de sus componentes en una serie de actividades. En ese sentido, se planteó que la división de estas como Actividades Generales o de Revisión, Actividades de Desarrollo de Código y Actividades de Documentación. Dentro de cada uno de estos apartados incluyen cada una de las tareas necesarias para poder completarlo, que además refieren a cada uno de los puntos a ser evaluados como parte del proyecto.

Ahora bien, con el fin de detallar un poco más la manera como serán estructuradas las tareas y roles, conviene mencionar algunas de las divisiones comprendidas por cada segmento. En el caso de las Actividades Generales, serán incluidas aquellas tareas que comprendan labores comunes a todos los miembros del equipo de trabajo. Algunas de estas incluyen el registro de los integrantes del grupo, las revisiones y reuniones periódicas sobre el desarrollo de los otros apartados, y al culminar el proyecto, la evaluación del trabajo realizado. Para este bloque la asignación de las tareas se da de forma proporcionada en su mayoría, incluyendo a todos los miembros del equipo para su realización.

Por otra parte, entre las tareas comprendidas por el segmento de Actividades de Desarrollo de Código, pueden hallarse todas las tareas de codificación de los algoritmos de cifrado requeridos, la validación y asignación de las restricciones de cada sección y la estructuración de los menús y opciones de navegación requeridas para el uso del programa principal. En este caso, la asignación de las tareas se da forma equitativa, asignando de forma combinada la codificación de los algoritmos de cifrado y descifrado. Considerando lo anterior, en caso de que a un integrante le corresponda el desarrollo proceso de cifrado de un algoritmo, al otro integrante le corresponderá desarrollar el proceso contrario, de descifrado, para el mismo algoritmo.

Para terminar, en el caso de las Actividades de Documentación, corresponde incluir todas aquellas tareas que involucren el registro de pruebas y procesos, toma de decisiones, cambios o ajustes que deban realizarse, así como la elaboración del Manual de Usuario para el programa a desarrollar. Otras actividades que se incluyen en este apartado son la publicación de entradas periódicas en el blog de cada integrante del equipo y la elaboración del presente documento. La asignación de las tareas de este segmento se da tanto de forma conjunta como individual, esto de acuerdo con la naturaleza del trabajo que debe realizarse para cada una y del tiempo que podría tomar su realización.

## Mecanismos de Seguimiento

El seguimiento del proyecto se llevará a cabo a partir de dos mecanismos principalmente. El primero de estos refiere a la forma en cómo se buscará editar e integrar el código para su desarrollo y revisión. En este caso se hará uso de la herramienta GitHub, con la cual, por medio de la creación de un repositorio será posible almacenar los archivos de código fuente para que todos los integrantes del equipo puedan disponer de estos, realizar los cambios que sean necesarios y completar cada una de sus asignaciones de forma rápida y sencilla.

Junto al mecanismo mencionado, se dispone la aplicación GitHub Desktop, la cual permite sincronizar los archivos disponibles en el repositorio con una carpeta local en el equipo de cada integrante. Con esta función, es posible manejar un respaldo del desarrollo que se tenga hasta el momento. Adicionalmente la plataforma GitHub y su aplicación permiten la creación de “ramas” o subdivisiones del programa o código principal tantas veces como sea necesario, y de esta esta manera es posible trabajar de forma separada secciones del código que podrían afectar o intervenir las áreas en las que otro integrante esté trabajando.

Así mismo, la intención de utilizar esta herramienta es llevar un control adicional sobre las actividades que se estén desarrollando en un momento determinado, y que cuando estas sean completadas, sea posible llevar a cabo una integración del código desarrollado de forma separada sin mayor problema.

El segundo mecanismo por utilizar será la ubicación de la documentación externa al código del programa, dentro de una carpeta en la plataforma de Google Drive. Esta permitirá la creación y posteriormente la edición de los documentos de forma colaborativa y en ocasiones sincronizada.

La funcionalidad que ofrece esta herramienta sobre la edición paralela de los archivos de texto y hojas de cálculo proporciona la facilidad de editar los documentos de pruebas del programa o de seguimiento de las actividades de forma sencilla y segura, y que estos cambios puedan ser revisados por los demás integrantes, no solo sobre la forma en que se hicieron sino también de acuerdo con el momento en que se dieron.

Finalmente, la creación de la carpeta mencionada anteriormente habilitará un espacio para la colocación de todos los recursos, referencias y material de apoyo, utilizados tanto para la elaboración de los documentos, como para la codificación de la solución programada.

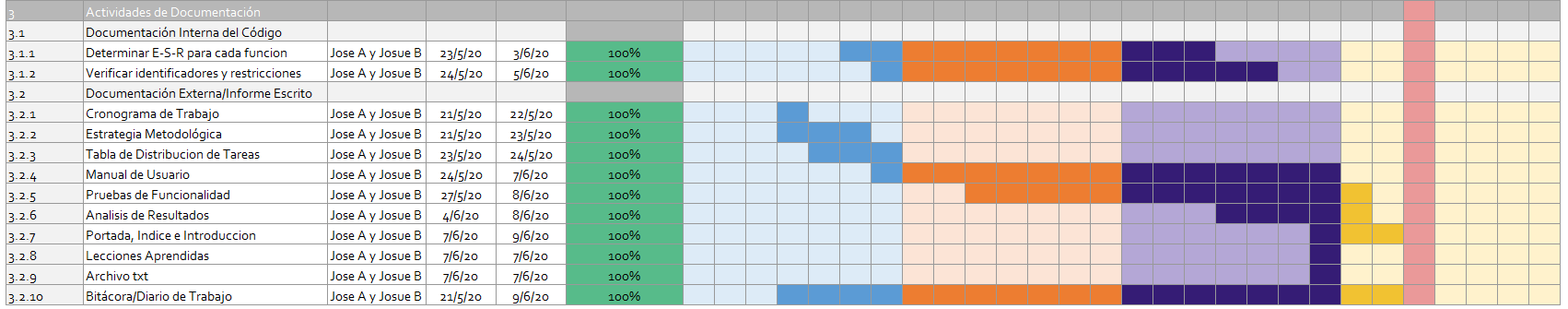
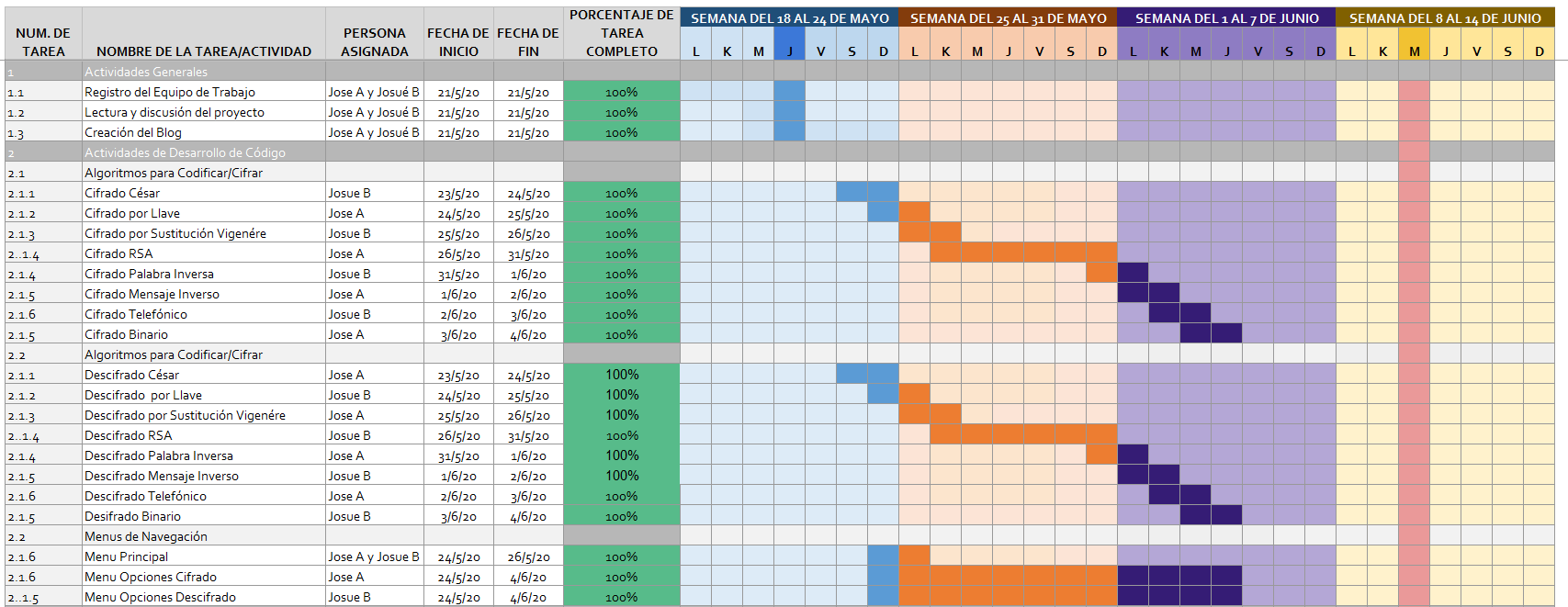
## Reuniones y validación de avances

En lo que respecta a las reuniones o sesiones de revisión del progreso del proyecto, se acordó que lo ideal sería realizar al menos dos sesiones semanales, los miércoles o jueves y sábado o domingo. De esta manera se dispondría del tiempo necesario para trabajar en su desarrollo y validar el estado de cada tarea, y en caso de fuese necesario, realizar las consultas correspondientes en los espacios destinados para este fin durante la semana.

## Modalidad de Trabajo

La modalidad de trabajo que será empleada tendrá un enfoque combinado, en el cual se tendrán sesiones de trabajo individuales y asincrónicas para las tareas que así lo requieran, así como sesiones grupales de forma sincrónica como es el caso de las reuniones o revisiones del progreso. Para las sesiones remotas se hará uso de plataformas de videoconferencias o videollamadas como lo son Zoom, Google Meet, Discord, entre otras.

# Cronograma de Trabajo



Enlace de acceso al cronograma en Google Drive para facilitar su lectura: <https://bit.ly/CronogramaProyecto1>

TI-1400 Introducción a la Programación

Primer Proyecto Programado

I Semestre, 2020

Integrantes:

Jose Altamirano Salazar - 2020426159

Josué Brenes Alfaro -2020054427

**Manual de Usuario del Programa de Técnicas de Cifrado de Mensajes**

# Manual de Usuario

## Portada

## Introducción:

Existen muchos tipos de cifrado, algunos son muy conocidos y utilizados. En software desarrollado presenta una solución basada en ocho tipos de cifrados sencillos. Este le permite a su usuario cifrar mensaje con estos algoritmos, y descifrar aplicando el proceso inverso sobre los mensajes ya cifrados, de acuerdo de la opción que se haya escogido.

El programa cuenta con un menú principal en el cual podrá elegir entre cifrar y descifrar, y luego, dependiendo de lo antes ya escogido, podrá visualizar los 8 tipos de cifrado o descifrado disponibles. Las opciones anteriores se despliegan dentro de un submenú para cada uno de los procesos.

Cada cifrado y descifrado tiene su propia funcionalidad ninguno es igual a otro, esto para que los códigos cifrados sean seguros. Hay cifrados en los cuales se pueden cifrar letras y números, otros sólo cifran caracteres específicos. Según lo anterior es importante considerar que, si el usuario cifrara un mensaje con una de las opciones de cifrado, solamente será posible descifrar este utilizando la función que corresponde al inverso del algoritmo utilizado para el cifrado.

Además, todos los cifrados tienen sus propias validaciones, las cuales guían al usuario sobre el uso del software y le indican los valores que debe ingresar para que el proceso de cifrado o descifrado funcione correctamente.

Algunos cifrados tienen un nivel de seguridad mayor en el cual tiene la aplicación de llaves. Estas llaves podrán ser escogida o se creará de manera aleatoria dependiendo del cifrado. En algunos de los algoritmos esta llave debe ser la misma que se utilizará para descifrar el mensaje. Si ingresamos valores que no corresponden, en el programa al momento de descifrar el mensaje solicitado retornará algo diferente en lugar del mensaje previamente cifrado.

Al ingresar a un tipo de cifrado o descifrado deberá completar todo lo solicitado, y una vez devuelto el resultado, podrá regresar al menú principal o si se desea escoger otra opción del menú y proceder a cifrar un nuevo mensaje. Los procesos de cifrado y descifrado pueden ser ejecutados las veces que sea necesario o que el usuario requiera que se realicen. Permitiendo acceder a las distintas funcionalidades del programa sin tener que ejecutarlo nuevamente desde el inicio.

## Funcionalidad General:

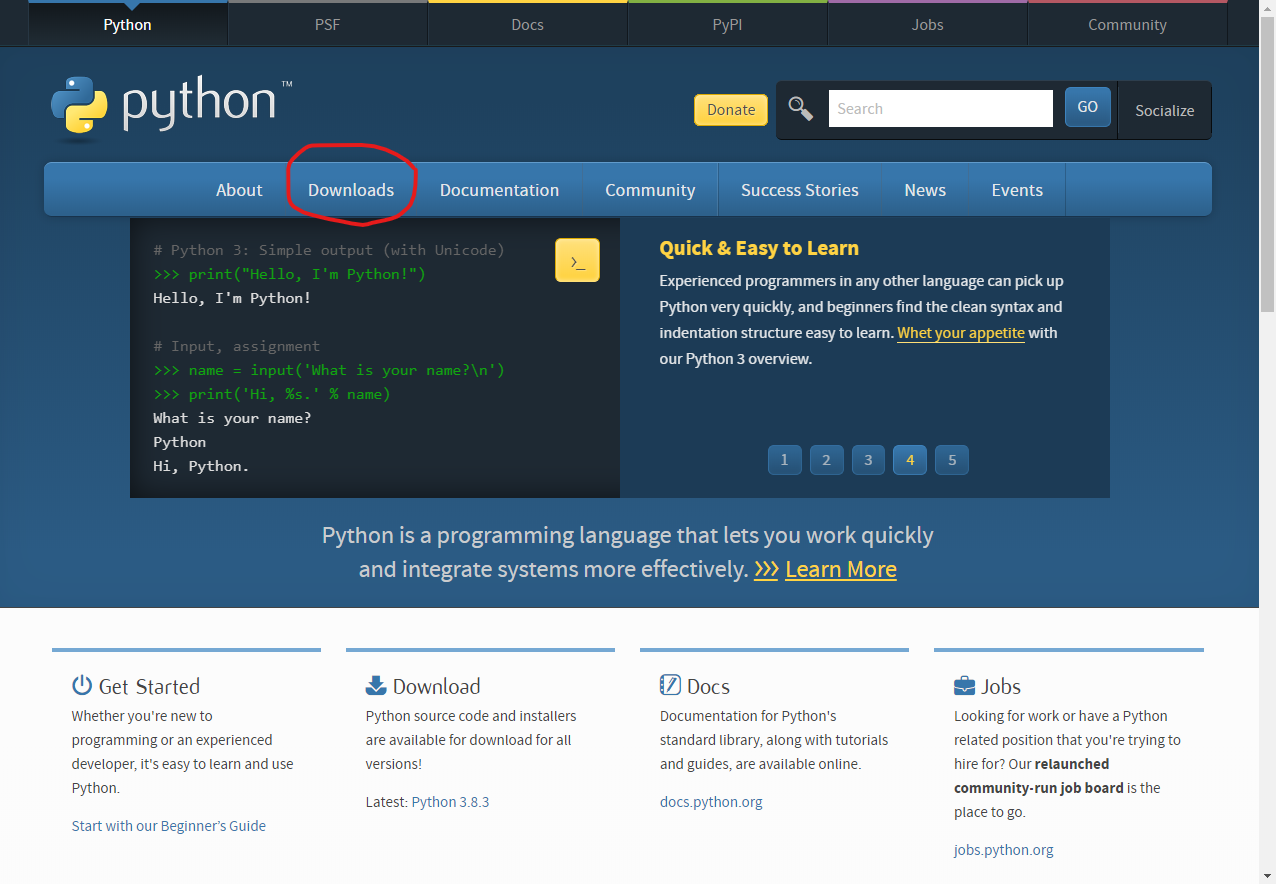
El sistema funciona de manera que el usuario elija entre las opciones de cifrar y descifrar en un menú principal. Luego hay dos menús secundarios, uno que contiene las opciones que hay en el sistema para cifrar el mensaje y en el otro encontrará las opciones para descifrarlo una vez ya cifrado. Hay una tercera opción en el menú principal para salir del programa.

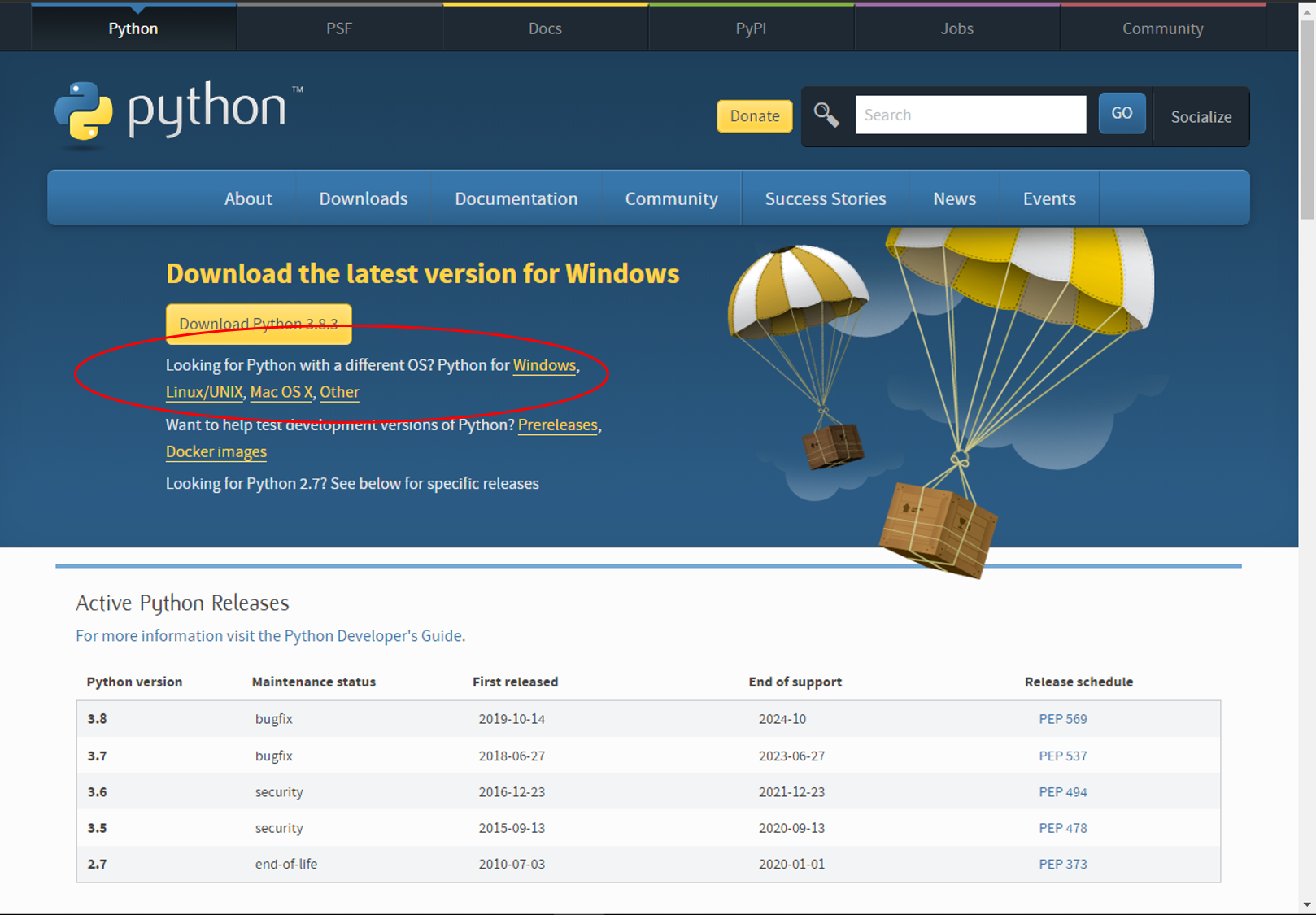
El usuario tiene la posibilidad de regresar de un menú secundario al principal. Si decide cifrar un mensaje, al ingresar a una de las ocho opciones de cifrado deberá ingresar lo solicitado y esperar al código cifrado. Si el menú es el de descifrado, la opción que se escoja debe corresponder a la opción de cifrado con la cual cifró el mensaje.

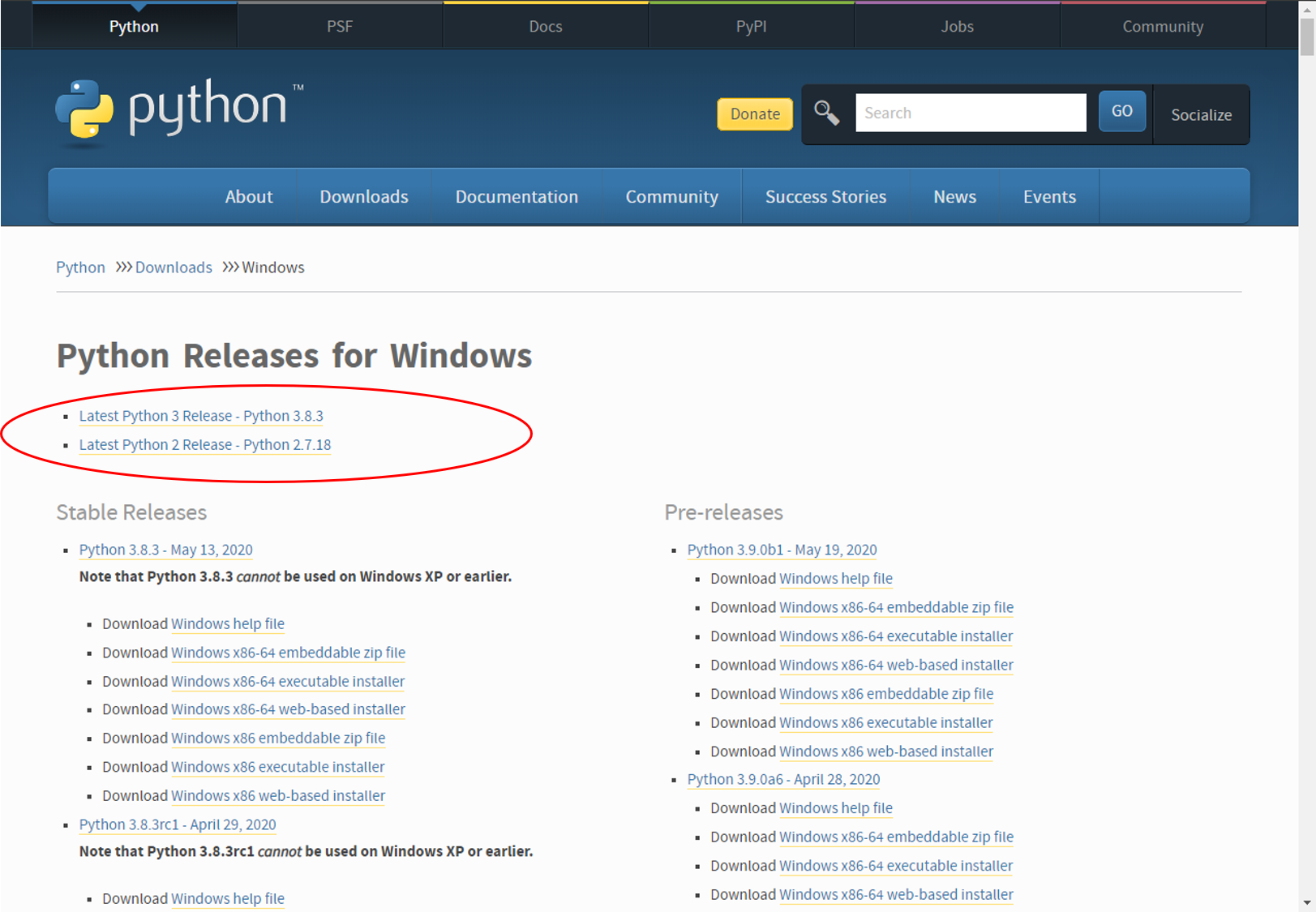
En caso de ingresar símbolos o cualquier elemento no permitido en cualquiera de los cifrados y descifrados, el programa le retornará un error. Si en algunas de las opciones de descifrado se ingresa un mensaje sin cifrar o cifrado con otro algoritmo, el resultado descifrar este retornará algo incoherente o sin sentido.

## Requisitos del Programa

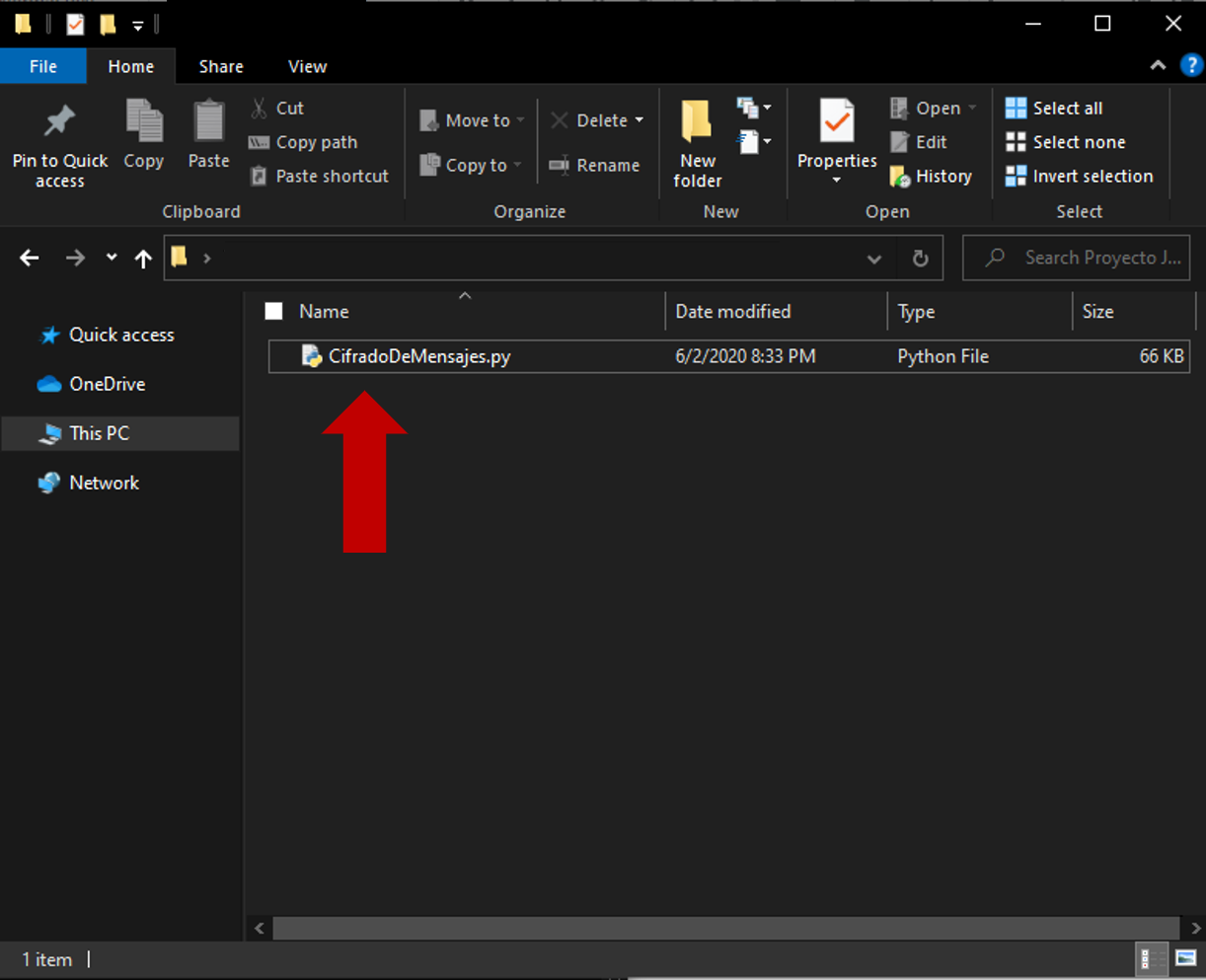
Para poder correr el programa debe tener un intérprete de Python. El programa se encuentra desarrollado bajo la versión 3.8, por lo cual es necesario descargar cualquier versión que iguale o supere a esta. Esta descarga se realiza por medio de la página oficial de Python ([https://www.python.org/](https://www.python.org/downloads/)). Al ingresar a esta, es necesario navegar a la opción de descargas en la barra de menú superior.



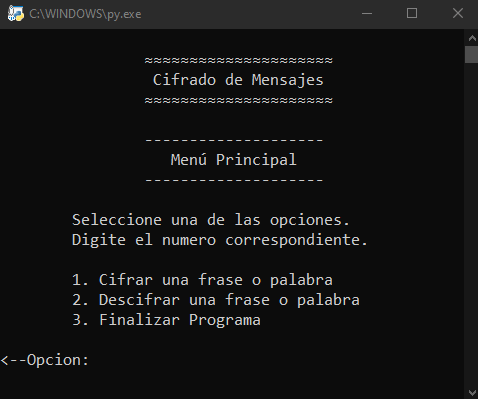
Al ingresar a esta sección, es necesario que seleccione el sistema operativo de su equipo para realizar la descarga apropiada.

En cualquiera de los casos debe seleccionar la opción que coincida o supera la versión 3.8. Generalmente se incluye en la parte superior de las descargas de cada sistema operativos, tal como se muestra en la siguiente imagen para el caso de Windows.

Una vez que el ejecutable de Python se haya descargado proceda a instalarlo. Cuando esta instalación haya finalizado, dirijase a la ubicación donde haya almacenado el archivo ejecutable del programa de cifrado de Mensajes.



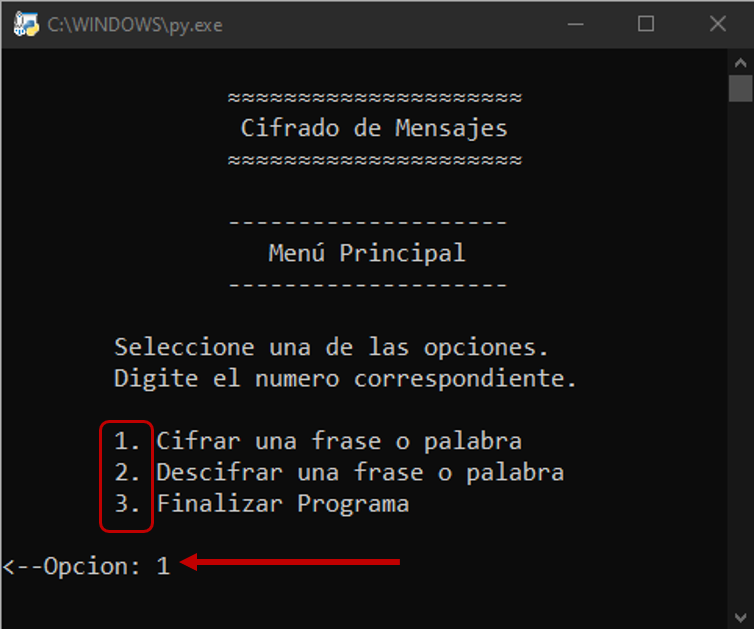
Al hacer doble clic sobre éste, se iniciará su ejecución. La siguiente imagen muestra este resultado dentro del SO Windows.



## 

## Guía de Uso

**Simbología del Programa:**

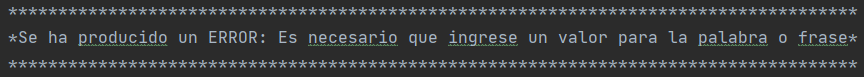
* Cada opción tiene un numero para poder ingresar a ella, para interactuar se deberá digitar el valor de la opción en los espacios designados para ingresar los valores
* En caso de ver una flecha apuntando a la izquierda (←) al inicio de la línea significa que se debe ingresar valores.



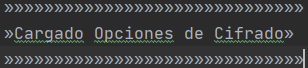
* En caso de ver una flecha apuntando a la derecha (→) al inicio de la línea significa que es una salida del programa.

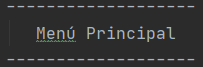
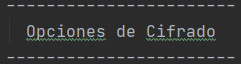


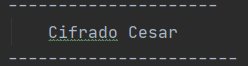
* Toda línea que está bordeada por un rectángulo de asteriscos (\*) son errores que emite el sistema por valores mal ingresados, por ejemplo:



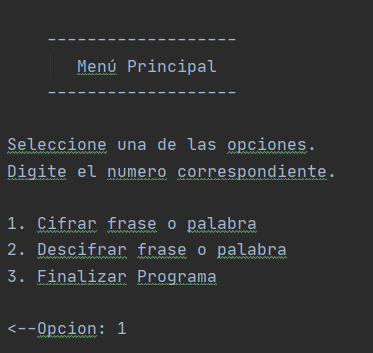
* Entre transiciones de menús se mencionan mensajes bordeados con el símbolo de doble flecha (»), por ejemplo:

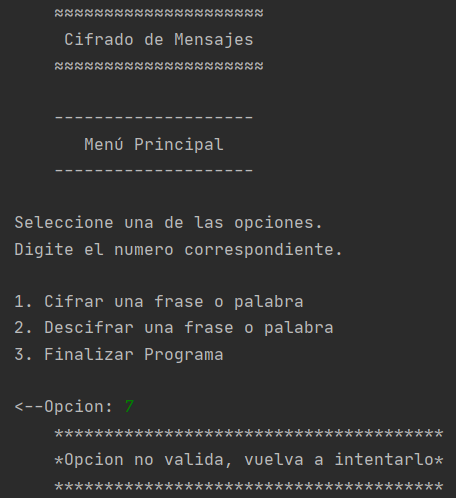


* Cada menú y sección tiene su propio encabezado, para darle al usuario la noción de la sección del programa en que se encuentra:

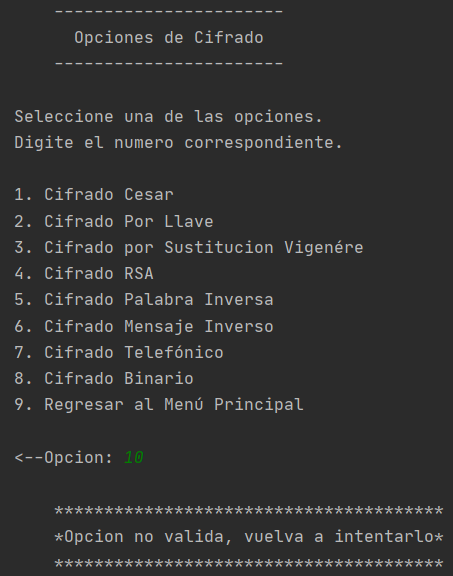


## Funcionalidad dentro del programa:

En el menú principal podrá seleccionar si desea cifrar (opción 1), descifrar (opción 2) o salir del programa (opción 3). La opción deseada debe ser ingresada en el espacio designado **(← opción:)**. En caso de colocar un número diferente de 1, 2 o 3 se mostrará un error hasta que se ingrese un valor correcto.:



### Opciones de Cifrado de Mensajes:

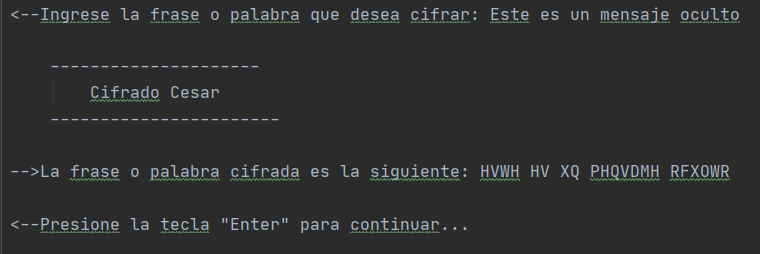
En caso de escoger la opción 1 (cifrado) del menú principal, tendrá en pantalla un menú secundario en el cual están todos los tipos de cifrados que tiene el sistema. Debe ingresar en el espacio indicado el número de cuál cifrado va a utilizar.



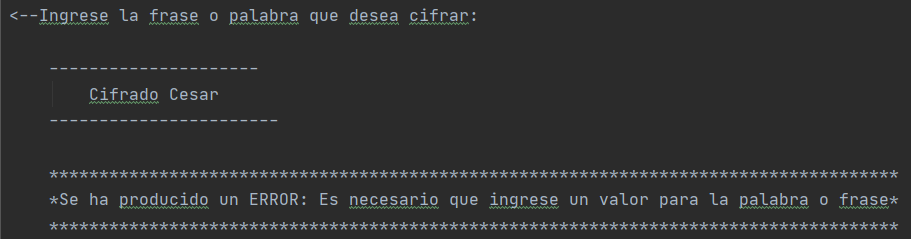
#### **1-Cifrados por sustitución:**

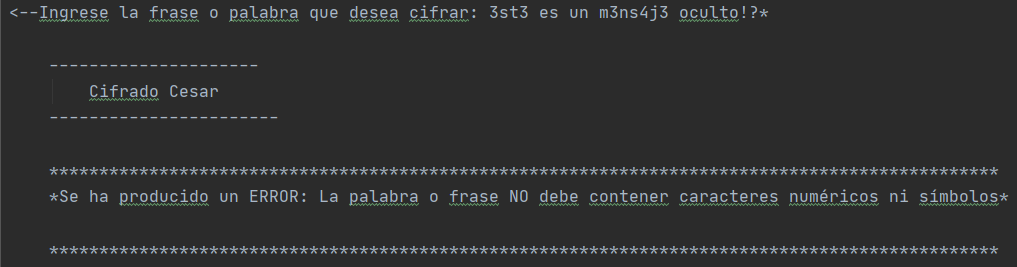
##### **1.1. Cifrado Cesar:**

Si elige la opción 1 del menú principal y opción **1** del menú secundario de cifrados se desplegará la pantalla el **cifrado césar**, deberá digitar palabras en el lugar destinado para ingresar valores, únicamente se pueden ingresar letras de lo contrario, el programa le mostrará un error. Luego de que el sistema le devuelva el mensaje cifrado deberá dar Enter para continuar y regresar al menú secundario de cifrados.



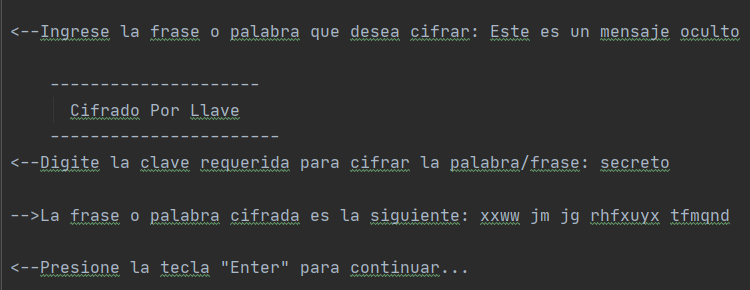
Posibles errores:



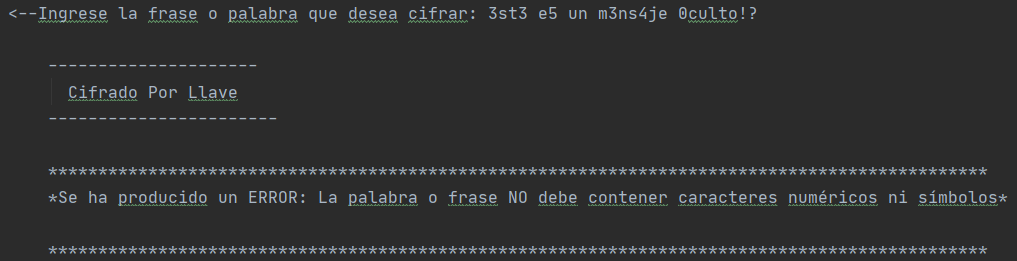


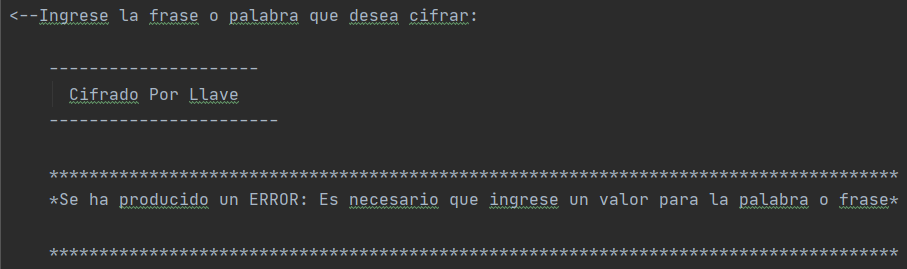
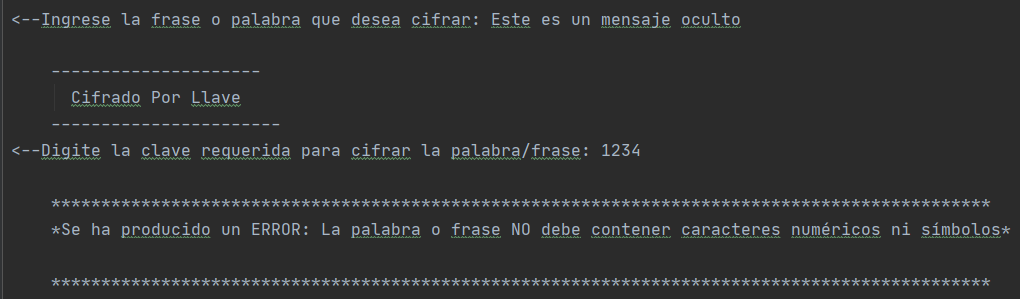
##### **1.2. Cifrado por llave:**

Si elige la opción 1 del menú principal y opción **2** del menú secundario de cifrados se desplegará la pantalla del **cifrado por llave**, deberá ingresar palabras en el lugar destinado para para este valor y además una llave, la cual le servirá a la hora que quiera descifrar el mensaje. Únicamente se pueden ingresar letras en ambas entradas, de lo contrario, el programa le mostrará un error. Luego que el sistema le devuelva el mensaje cifrado, deberá de dar Enter para regresar al menú secundario de cifrados.



Posibles errores:

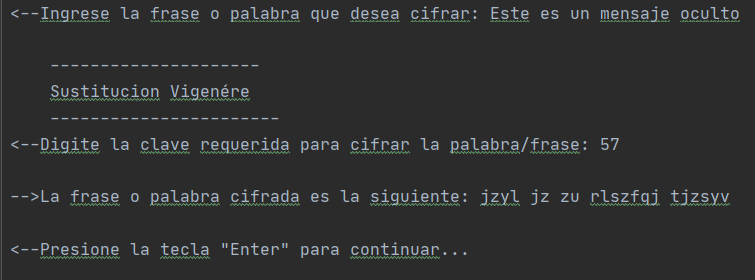


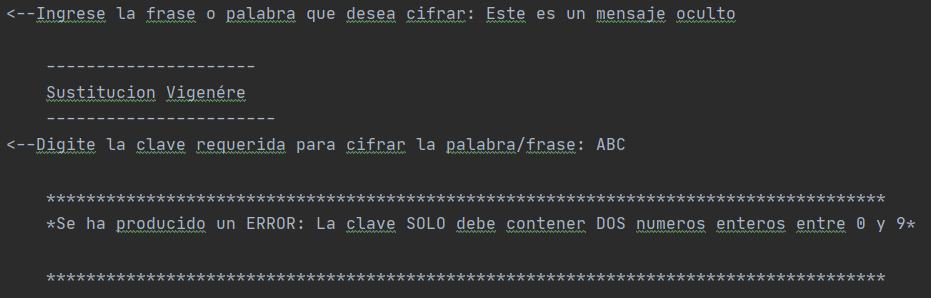


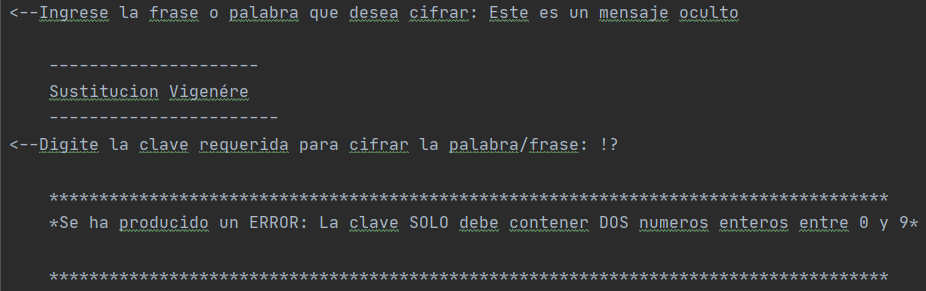


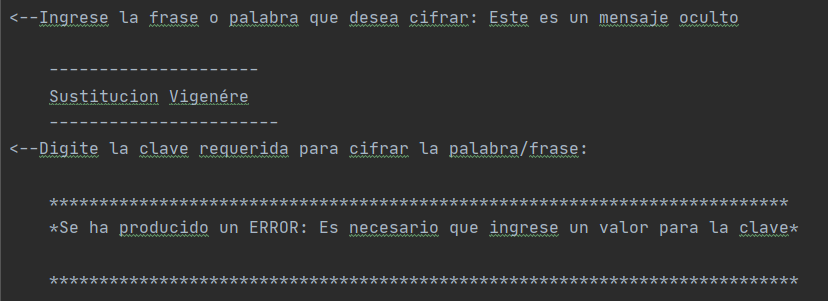
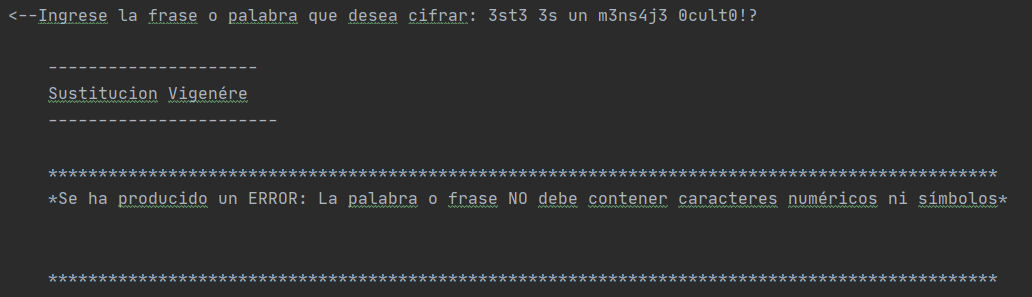
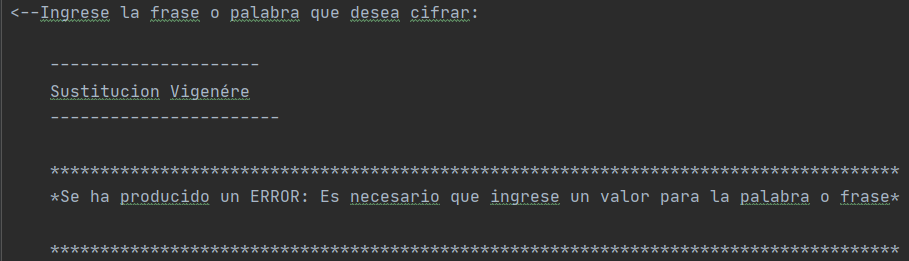
##### 

##### **1.3. Sustitución Vigenére:**

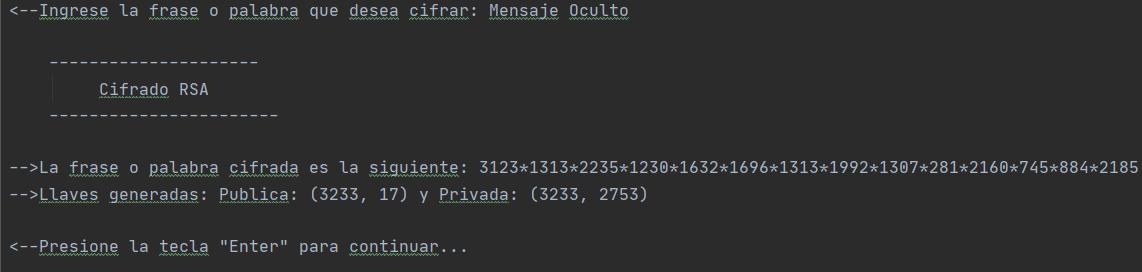
 Si elige la opción 1 del menú principal y opción **3** del menú secundario de cifrados se desplegará la pantalla del cifrado **Sustitución Vigenére**, deberá ingresar palabras en el primer espacio destinado para ingresar valores además una llave en el segundo espacio en la cual debe ingresar dos números como *por ejemplo* cincuenta y siete (57), la cual le servirá a la hora que quiera descifrar el mensaje. Únicamente se pueden ingresar letras en la primera entradas y números en la segunda (la llave), de lo contrario, el programa le mostrará un error. Luego que el sistema le devuelva el mensaje cifrado, deberá de dar Enter para regresar al menú secundario de cifrados.

Posibles errores:

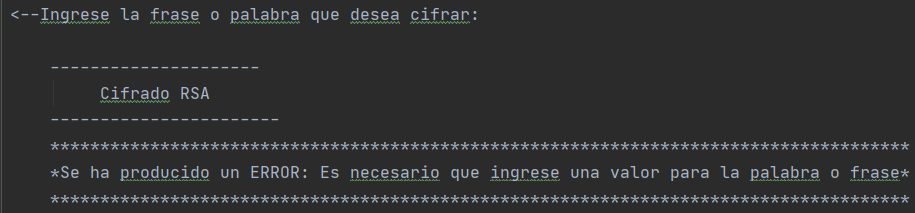


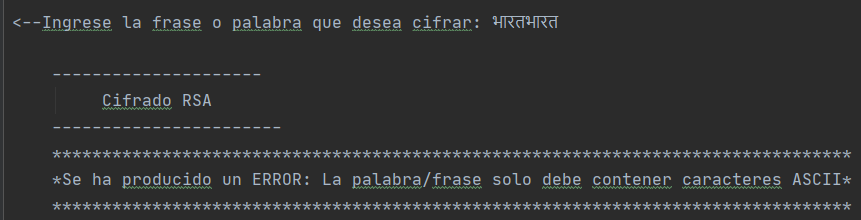


#### **2.Cifrado RSA:**

Si elige la opción 1 del menú principal y opción **4** del menú secundario de cifrados se desplegará la pantalla el **cifrado RSA**, deberá ingresar palabras en el lugar destinado para ingresar valores, únicamente se pueden ingresar letras, de lo contrario, el programa le mostrará un error. Luego de que el sistema le devuelva el mensaje cifrado y las llaves pública y privada. deberá dar Enter para continuar y regresar al menú secundario de cifrados.

Posibles errores:



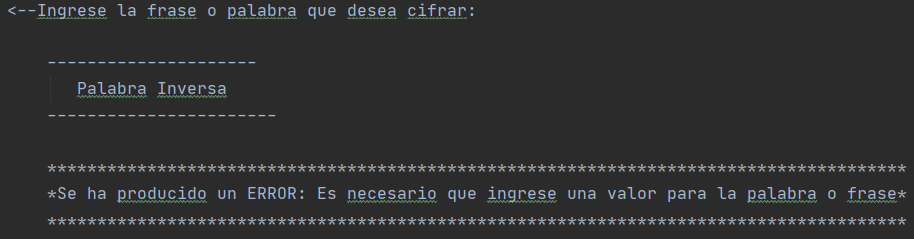


#### **3. Cifrado por Transposición**

##### **3.1 Cifrado por palabra inversa:**

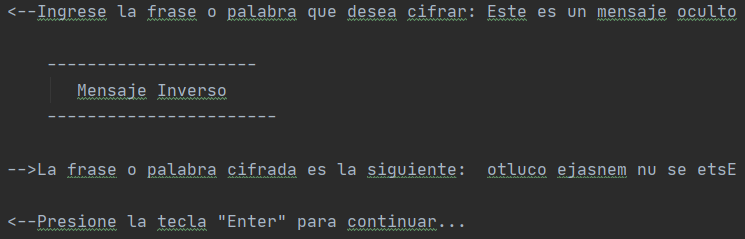
Si elige la opción 1 del menú principal y opción **5** del menú secundario de cifrados se desplegará la pantalla el **cifrado por palabra inversa**, deberá ingresar palabras en el lugar destinado para ingresar valores, únicamente se pueden ingresar letras de lo contrario, el programa le mostrará un error. Luego de que el sistema le devuelva el mensaje cifrado deberá dar Enter para continuar y regresar al menú secundario de cifrados.



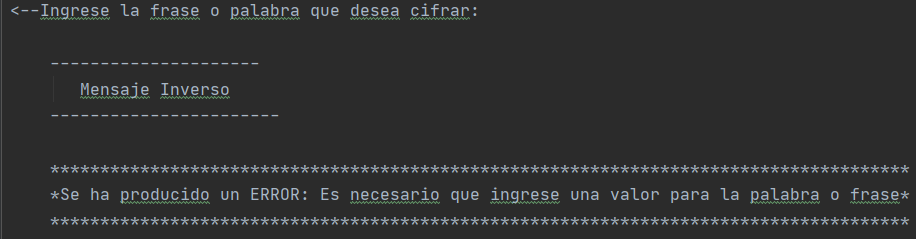
Posibles errores:

##### **3.2. Cifrado mensaje inverso:**

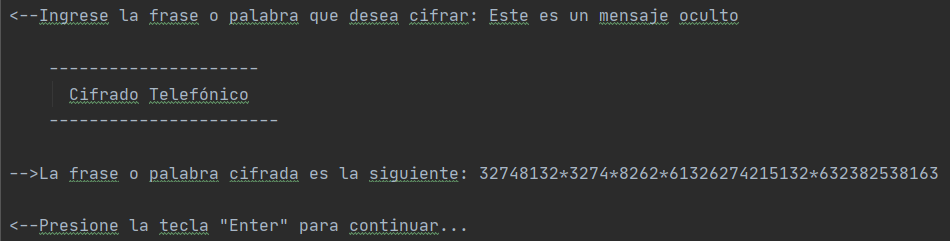
Si elige la opción 1 del menú principal y opción **6** del menú secundario de cifrados se desplegará la pantalla el **cifrado mensaje inverso**, deberá ingresar palabras en el lugar destinado para ingresar valores, únicamente se pueden ingresar letras de lo contrario, el programa le mostrará un error. Luego de que el sistema le devuelva el mensaje cifrado deberá dar Enter para continuar y regresar al menú secundario de cifrados.

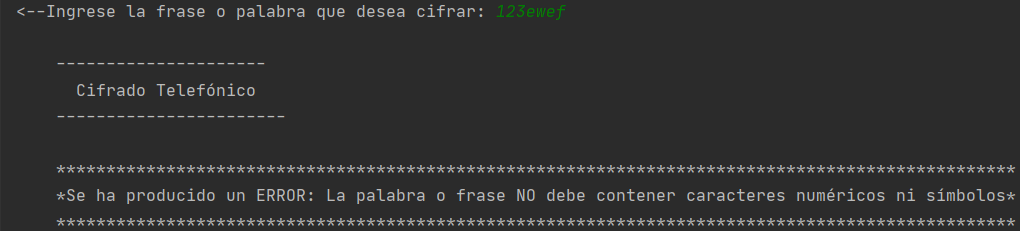
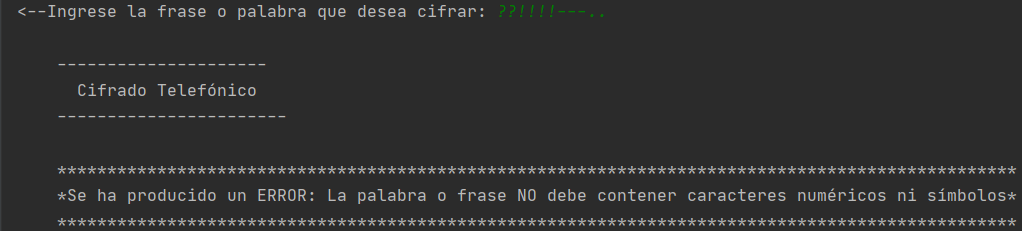
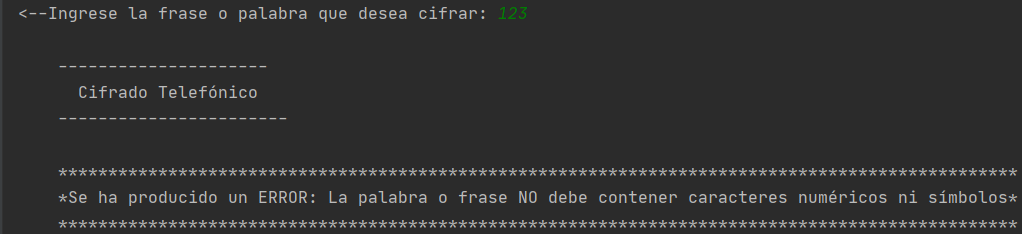


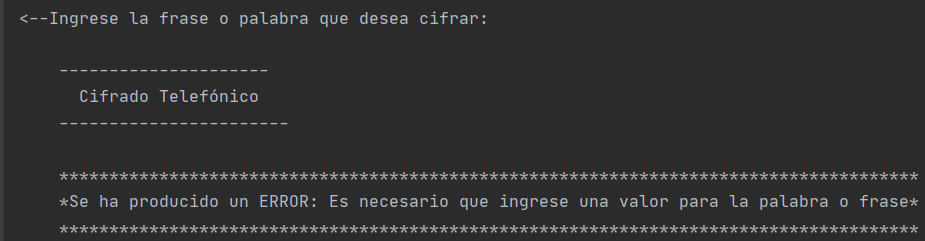
Posibles errores:



#### **4.Cifrado telefónico:**

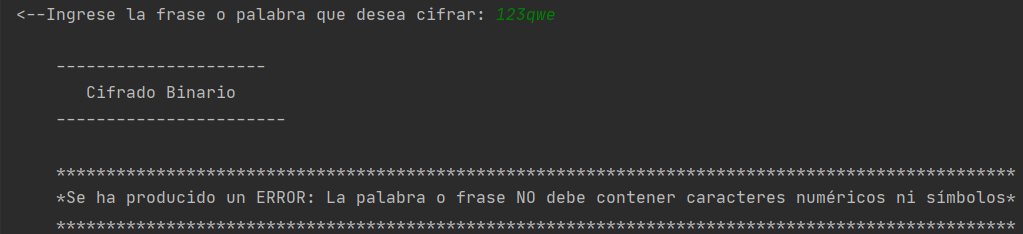
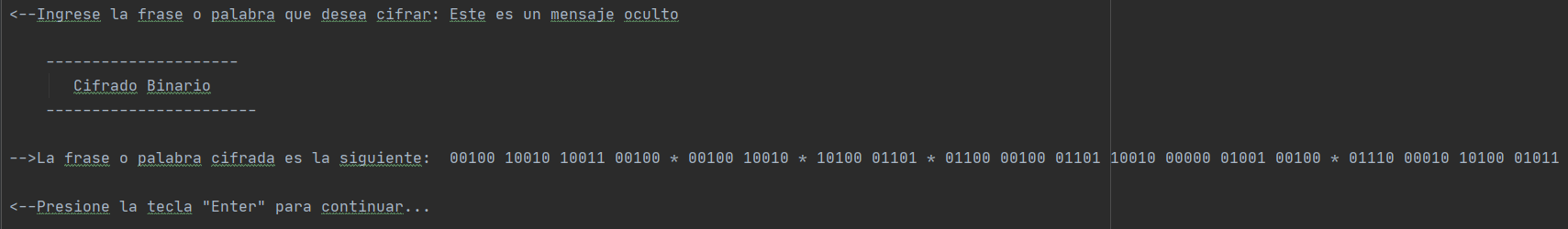
Si elige la opción 1 del menú principal y opción **7** del menú secundario de cifrados se desplegará la pantalla el **cifrado telefónico**, deberá ingresar palabras en el lugar destinado para ingresar valores, únicamente se pueden ingresar letras de lo contrario, el programa le mostrará un error. Luego de que el sistema le devuelva el mensaje cifrado deberá dar Enter para continuar y regresar al menú secundario de cifrados.

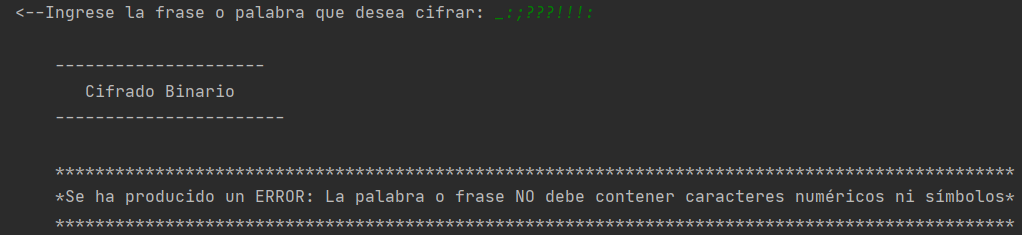
Posibles errores:

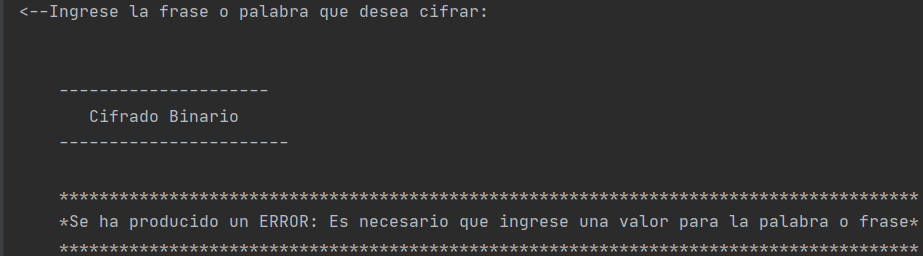


**5.Cifrado binario:**

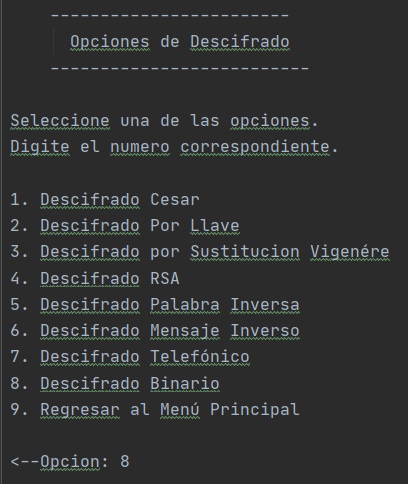
Si elige la opción 1 del menú principal y opción **8** del menú secundario de cifrados se desplegará la pantalla el **cifrado binario**, deberá ingresar palabras en el lugar destinado para ingresar valores, únicamente se pueden ingresar letras de lo contrario, el programa le mostrará un error. Luego de que el sistema le devuelva el mensaje cifrado deberá dar Enter para continuar y regresar al menú secundario de cifrados.

Posibles errores





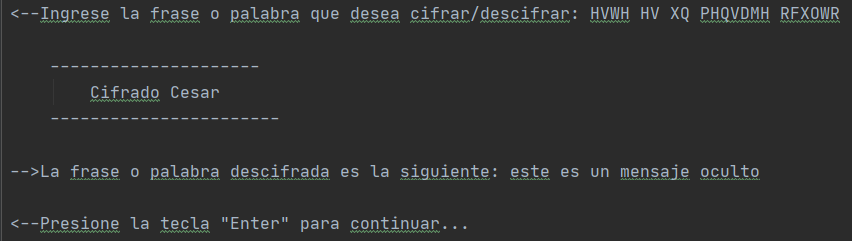
### Opciones de Descifrado de Mensajes:

En caso de escoger la opción 2 (descifrado) en el menú principal, tendrá en pantalla un menú secundario en el cual están todos los tipos de descifrados que tiene el sistema. Debe ingresar en el espacio indicado el número de cual descifrado va a utilizar.

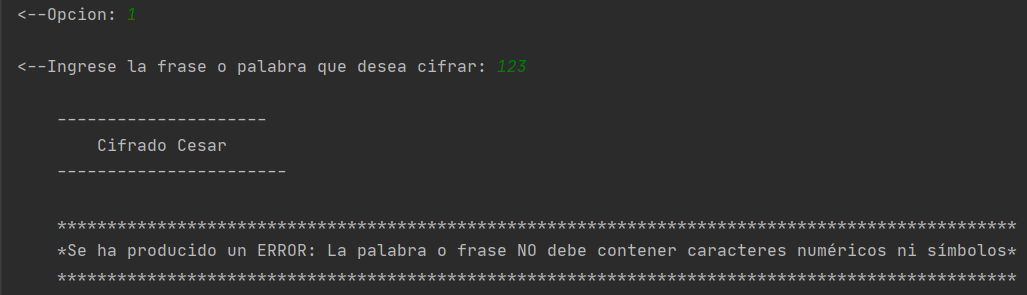
#### **1-Cifrados por sustitución:**

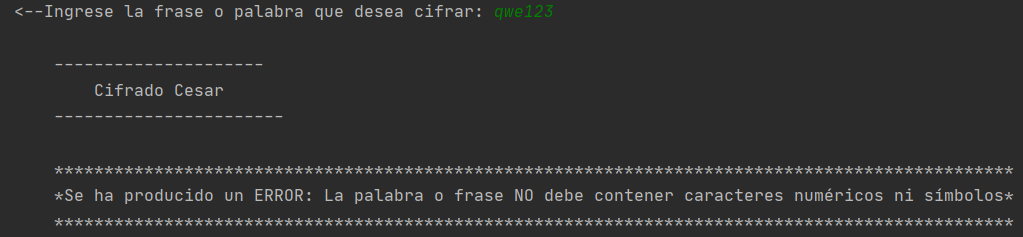
##### **Descifrado cesar:**

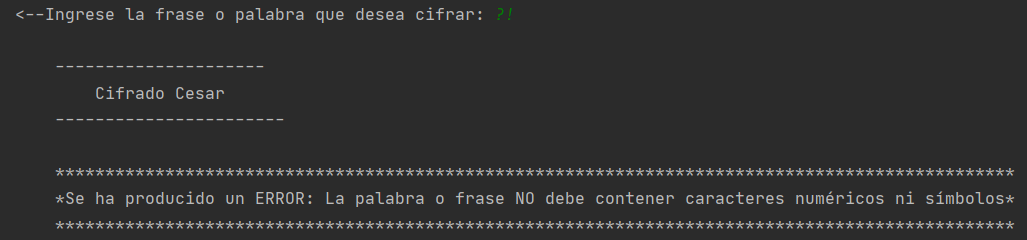
Si elige la opción 2 del menú principal y opción **1** del menú secundario de descifrados se desplegará la pantalla el **descifrado cesar**, deberá ingresar el mensaje cifrado en el lugar destinado para ingresar valores, únicamente se pueden ingresar letras de lo contrario, el programa le mostrará un error. Luego de que el sistema le devuelva el mensaje descifrado deberá dar Enter para continuar y regresar al menú secundario de cifrados.

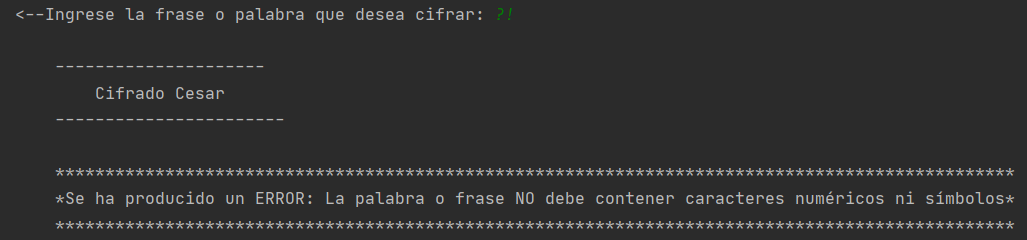


Posibles errores:



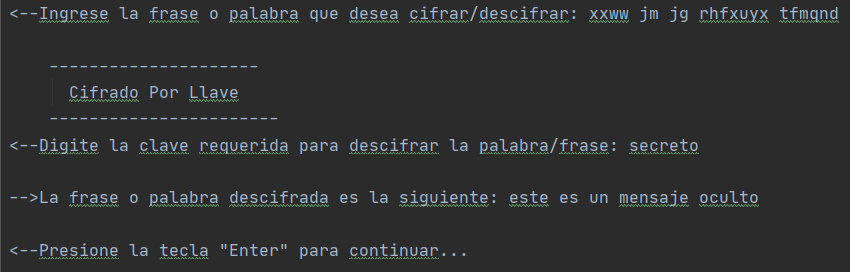


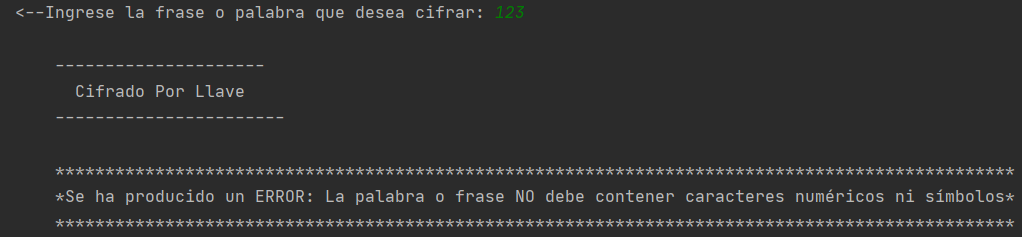
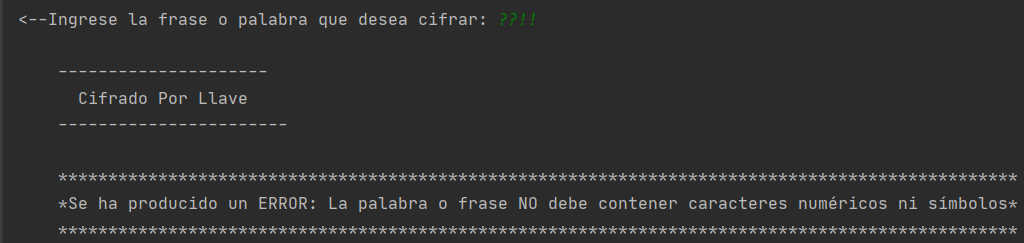


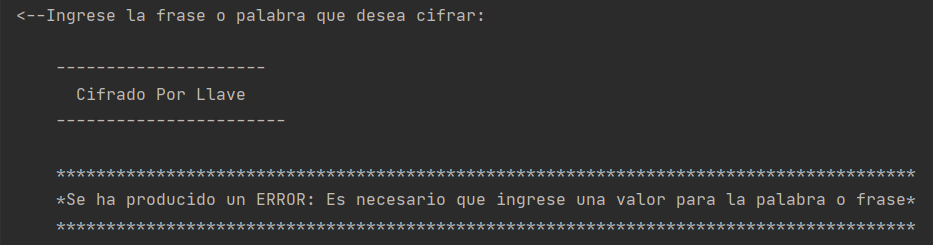


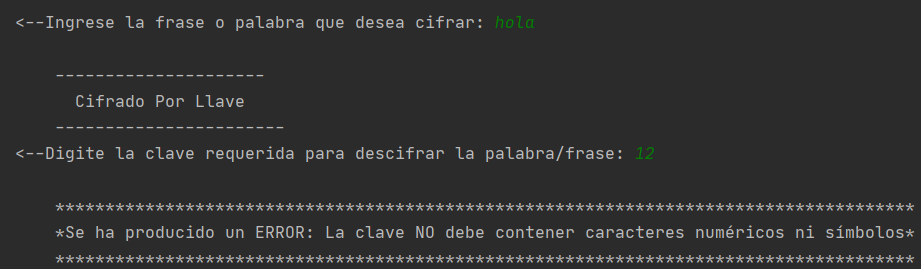
#### 

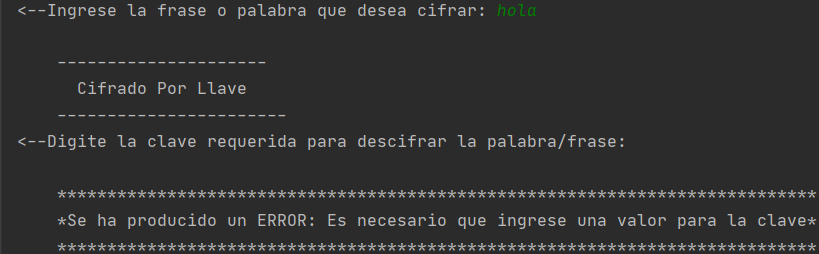
##### **Descifrado por llave:**

Si elige la opción 2 del menú principal y opción **2** del menú secundario de descifrados se desplegará la pantalla el **descifrado por llave**, deberá ingresar el mensaje cifrado y la llave usada para cifrar en el lugar destinado para ingresar valores, únicamente se pueden ingresar letras en ambas entradas, de lo contrario, el programa le mostrará un error. Luego de que el sistema le devuelva el mensaje descifrado deberá dar Enter para continuar y regresar al menú secundario de cifrados.

Posibles errores:

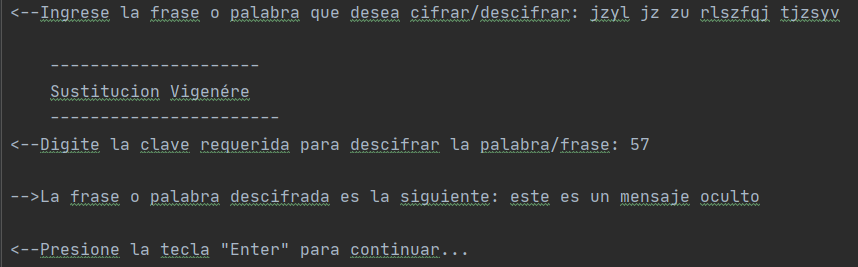




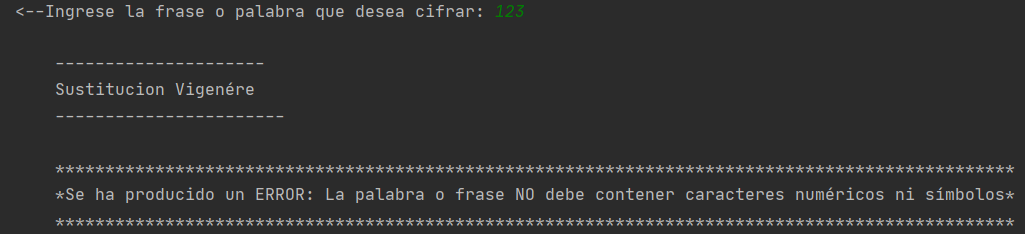


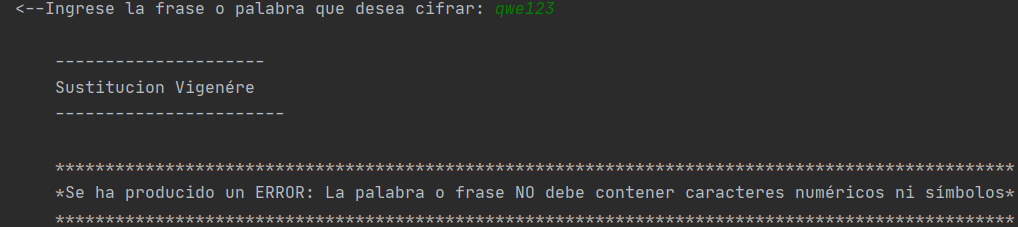
##### **1.3 Descifrado por Sustitución de Vigenére:**

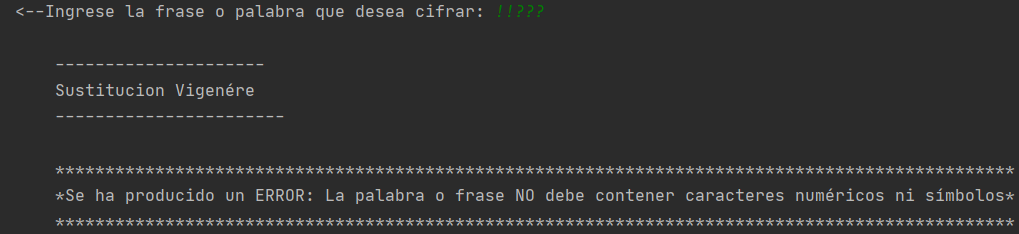
Si elige la opción 2 del menú principal y opción **3** del menú secundario de descifrados se desplegará la pantalla el **descifrado sustitución de vigenére**, deberá ingresar el mensaje cifrado y la llave usada para cifrar, en el lugar destinado para ingresar valores, en la primera entrada solo se debe ingresar letras y en la segunda solo dos números, de lo contrario, el programa le mostrará un error. Luego de que el sistema le devuelva el mensaje descifrado deberá dar Enter para continuar y regresar al menú secundario de cifrados.

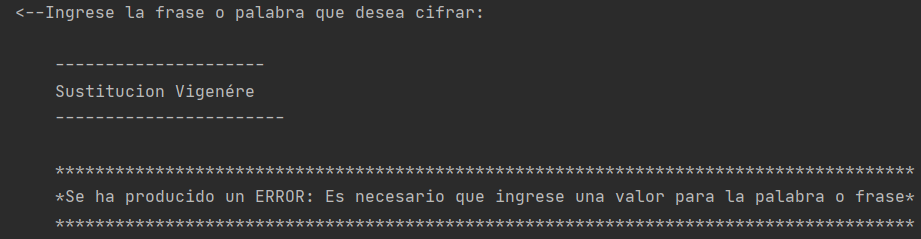


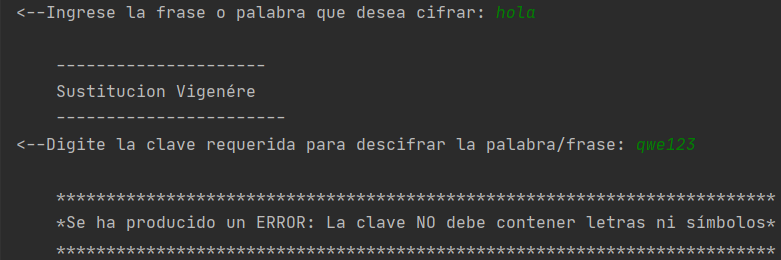
Posibilidad de errores:

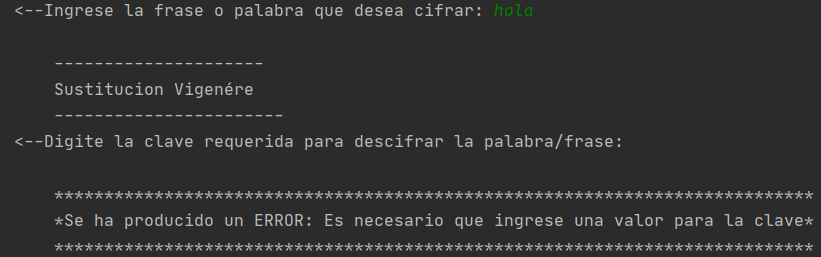






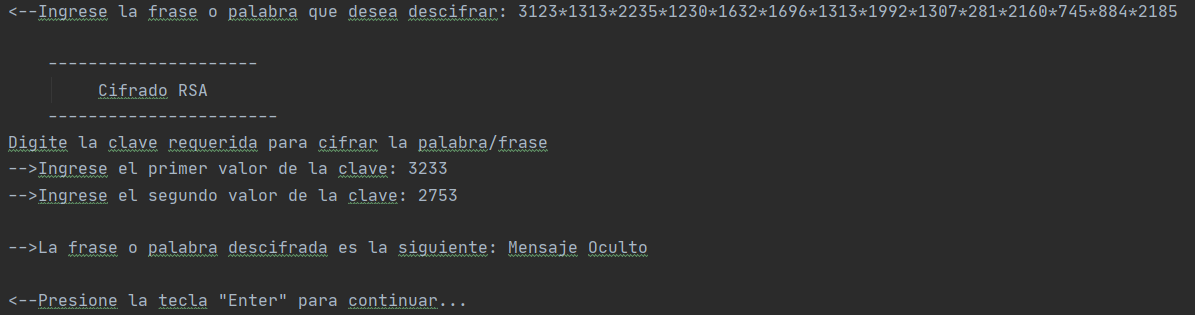




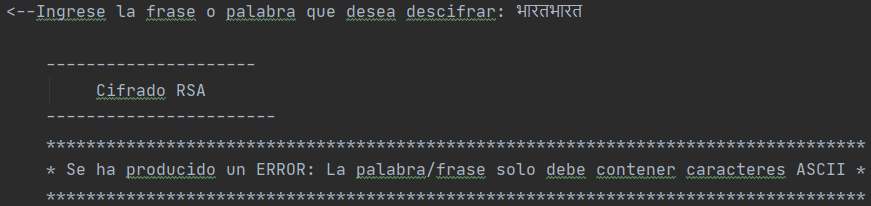


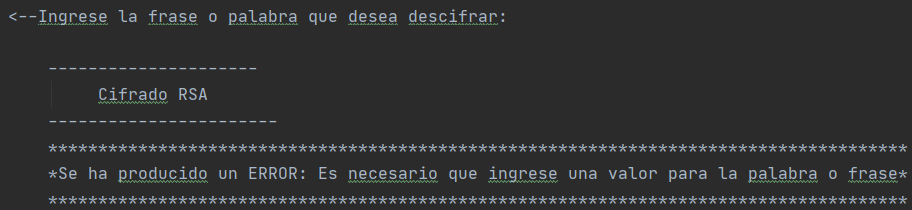
#### **2.Descifrado RSA:**

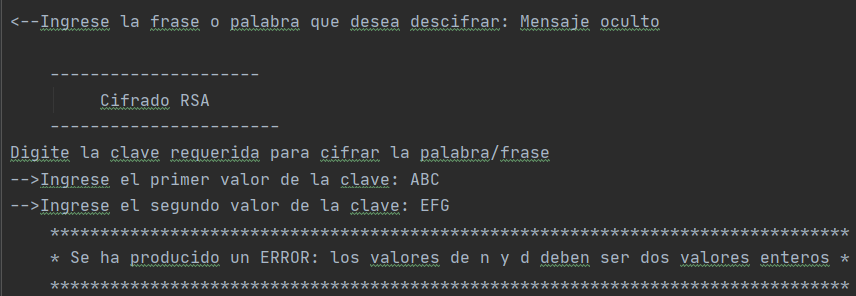
Si elige la opción 2 del menú principal y opción **4** del menú secundario de descifrados se desplegará la pantalla el **descifrado RSA**, deberá ingresar el mensaje cifrado y las dos partes de la clave privada, en el lugar destinado para ingresar valores, en la primera entrada solo se debe ingresar números y asteriscos (\*) y en la segunda y tercera solo números, de lo contrario, el programa le mostrará un error. Luego de que el sistema le devuelva el mensaje descifrado deberá dar Enter para continuar y regresar al menú secundario de cifrados.



Posibilidad de errores:



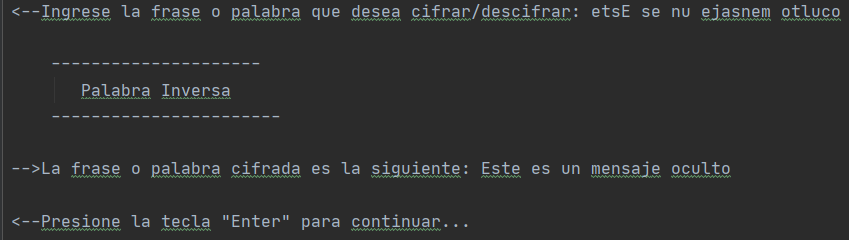


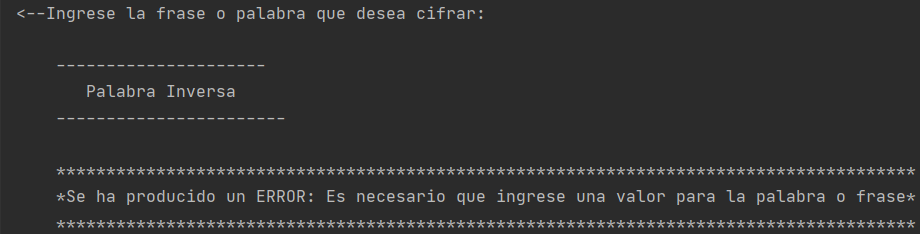


#### **3. Cifrado por transposición**

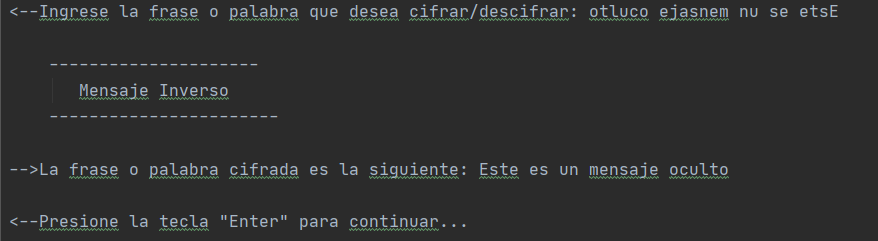
##### **3.1. Descifrada palabra inversa:**

Si elige la opción 2 del menú principal y opción **5** del menú secundario de descifrados se desplegará la pantalla la descifrada palabra inversa, deberá ingresar el mensaje cifrado en el lugar destinado para ingresar valores, únicamente se pueden ingresar letras de lo contrario, el programa le mostrará un error. Luego de que el sistema le devuelva el mensaje descifrado deberá dar Enter para continuar y regresar al menú secundario de cifrados.

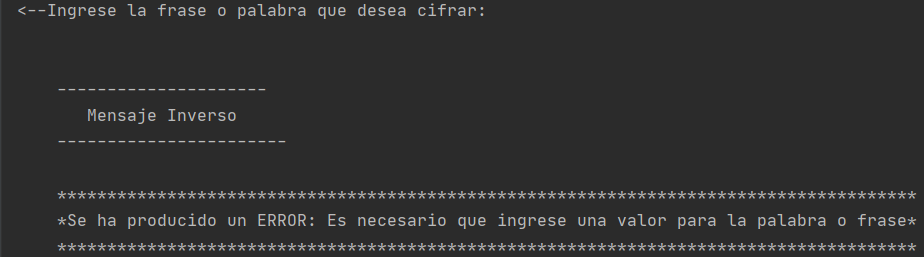


Posibilidad de errores:

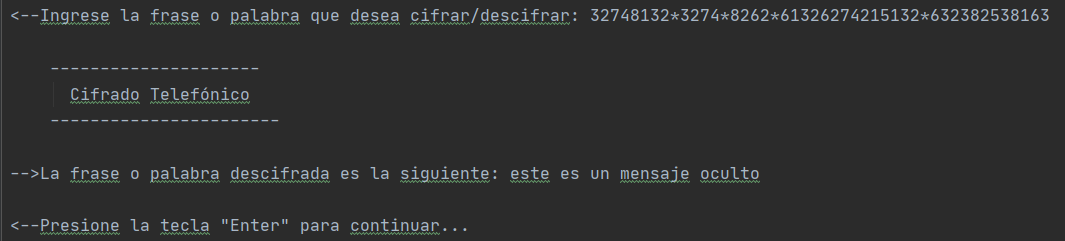
##### **3.2. Descifrado mensaje inverso:**

Si elige la opción 2 del menú principal y opción 6 del menú secundario de descifrados se desplegará la pantalla el descifrado mensaje inverso, deberá ingresar el mensaje cifrado en el lugar destinado para ingresar valores, únicamente se pueden ingresar letras de lo contrario, el programa le mostrará un error. Luego de que el sistema le devuelva el mensaje descifrado deberá dar Enter para continuar y regresar al menú secundario de cifrados.

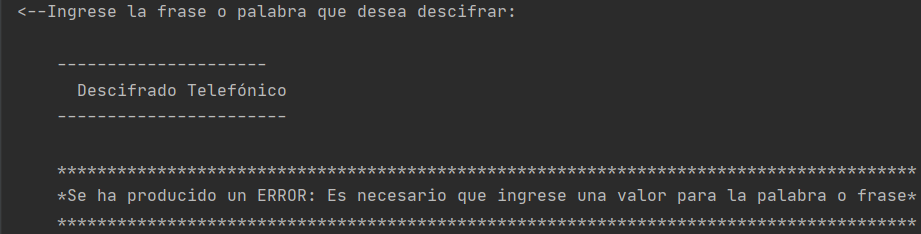
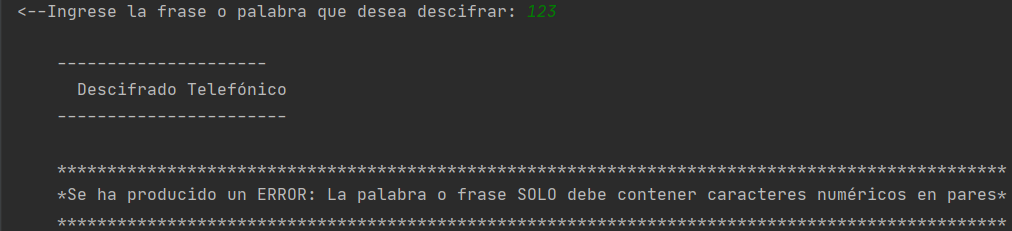
Posibilidad de errores:

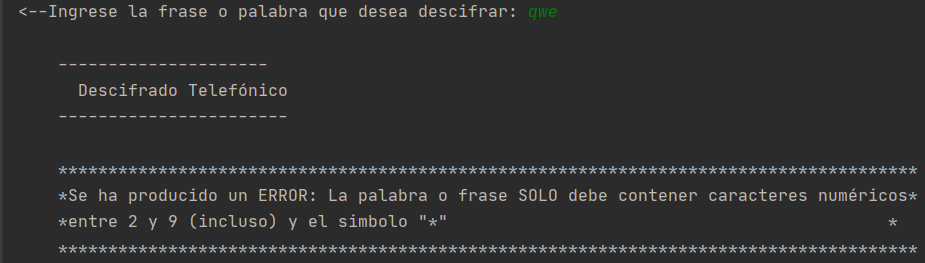


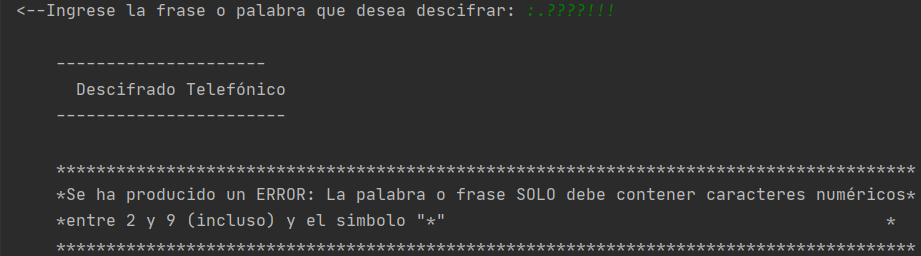
#### **4.Descifrado telefónico:**

Si elige la opción 2 del menú principal y opción **7** del menú secundario de descifrados se desplegará la pantalla el **descifrado telefónico**, deberá ingresar el mensaje cifrado en el lugar destinado para ingresar valores, únicamente se pueden ingresar números y asteriscos (\*) de lo contrario, el programa le mostrará un error. Luego de que el sistema le devuelva el mensaje descifrado deberá dar Enter para continuar y regresar al menú secundario de cifrados.

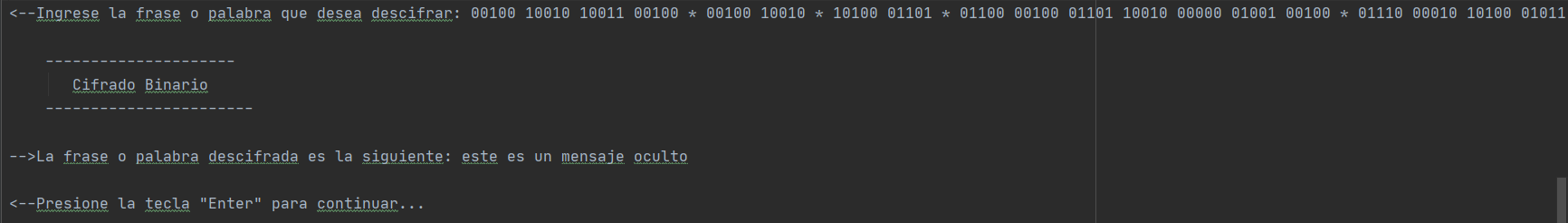
Posibilidad de errores:



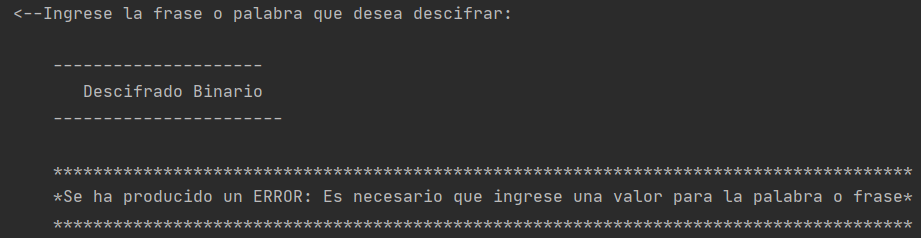


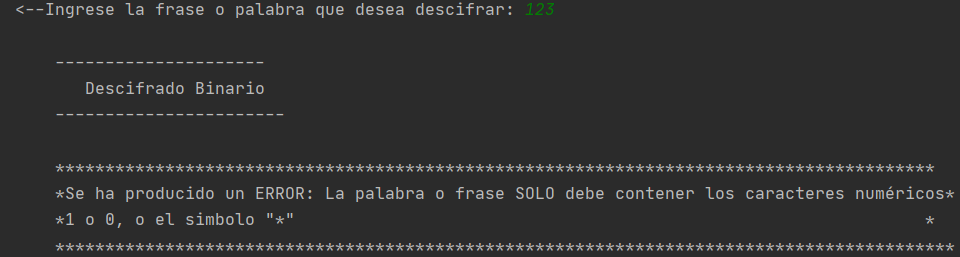


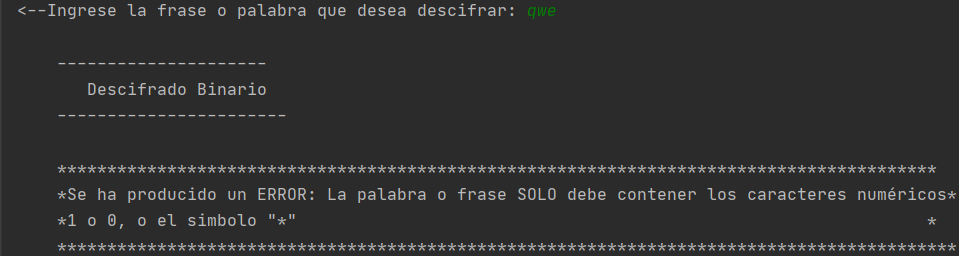
**5.Descifrado binario:**

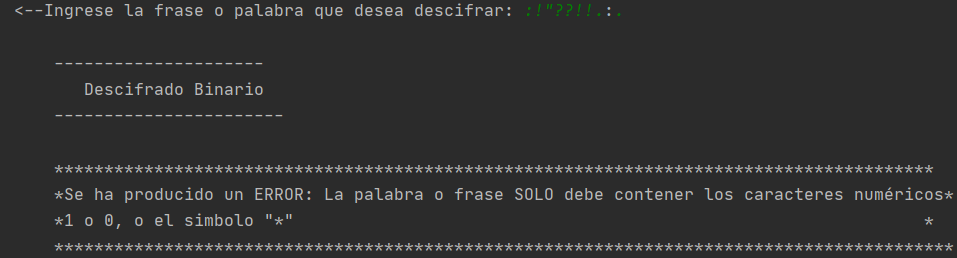
Si elige la opción 2 del menú principal y opción **7** del menú secundario de descifrados se desplegará la pantalla el **descifrado telefónico**, deberá ingresar el mensaje cifrado en el lugar destinado para ingresar valores, únicamente se pueden ingresar números y asteriscos (\*) de lo contrario, el programa le mostrará un error. Luego de que el sistema le devuelva el mensaje descifrado deberá dar Enter para continuar y regresar al menú secundario de cifrados.

Posibles errores:









# 

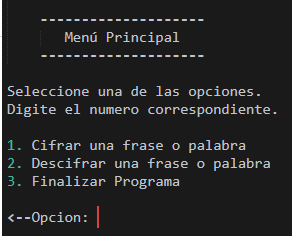
# Pruebas de Funcionalidad

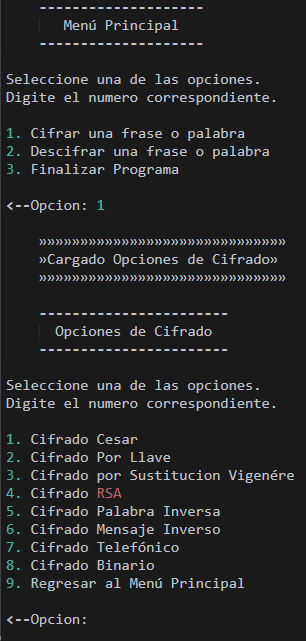
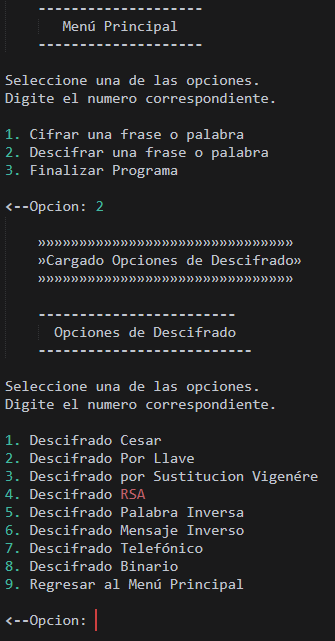
En esta sección detallan cada una las funcionalidades implementadas dentro del programa de “Técnicas de Cifrado de Mensajes”. Para cada opción se especifican las posibles entradas o valores que se requiera sean ingresados, las restricciones que rigen sobre cada una de estas entradas, el manejo de errores en caso valores no permitidos o no válidos y las salidas o valores retornados por cada una de las funciones utilizadas.

Cada funcionalidad será descrita de acuerdo con la distribución propuesta dentro de los menús de navegación internos al software. De esta manera podrán estructurarse las descripciones de las diferentes secciones, al hacer énfasis sobre el flujo normal, o acertado, y el flujo errado, o con la validación de las restricciones, para cada una de estas.

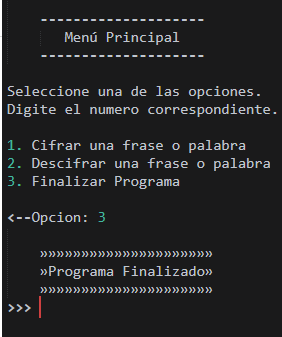
## Menú Principal

Dentro del Menú de Navegación Principal se requiere que el usuario seleccione una de las opciones que este le muestra. Para seleccionarla, es necesario que ingrese el valor numérico que antecede a cada una de estas (ver Imagen).

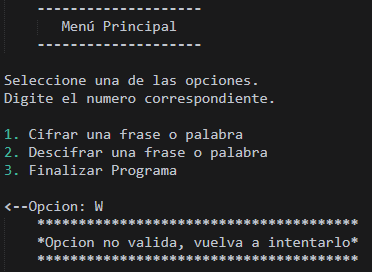
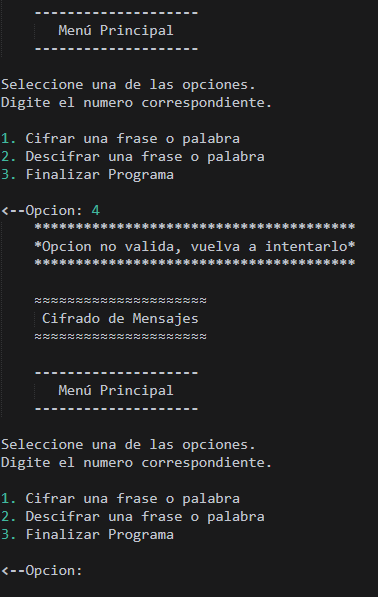
Inmediatamente después del despliegue de las opciones se dispone de un “input” o espacio para que se ingrese el valor de la opción deseada. En este caso, dicho valor podría ser 1, 2 o 3. Dentro del flujo normal del programa en caso de que se seleccione la opción 1 o la opción 2, lo que corresponde es que se carguen los menús con las opciones de cifrado y descifrado respectivamente. El resultado de la selección de ambas opciones mencionadas se detalla en las siguientes imágenes.



La otra opción posible, dentro del flujo acertado del programa, es el número 3. En caso de que el usuario ingrese este valor se, el programa será finalizado. Este proceso puede observarse en la siguiente imagen.

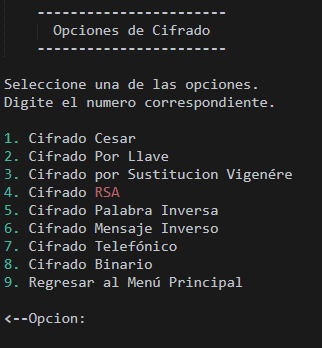


Ahora bien, dado el caso que se ingrese un valor no válido, el cual podría ser un valor numérico distinto de los 1, 2 o 3, algún símbolo o letra, o la combinación de alguno de los anteriores. De acuerdo con las validaciones implementadas dentro de esta función, se desplegará el mensaje “Opción no valida, vuelva a intentarlo”. Luego de que se muestre este mensaje, se volverá a desplegar el Menú Principal con la posibilidad de seleccionar nuevamente una opción. Este proceso puede observarse en las siguientes imágenes.

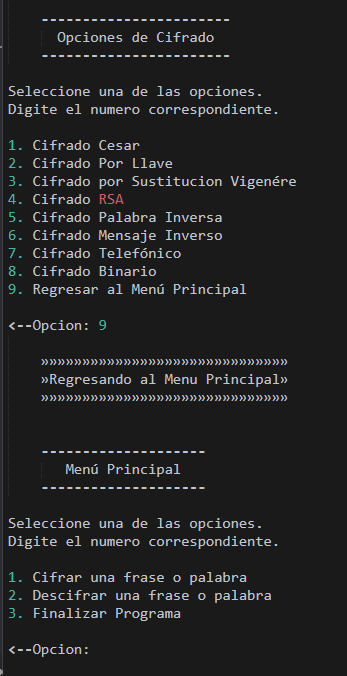


## Menú Cifrado

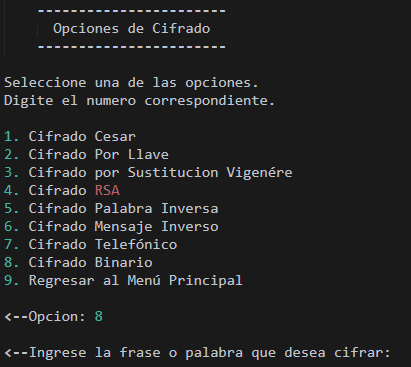
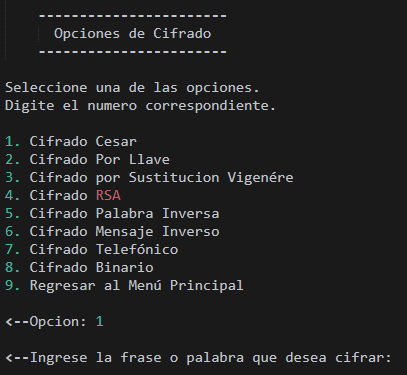
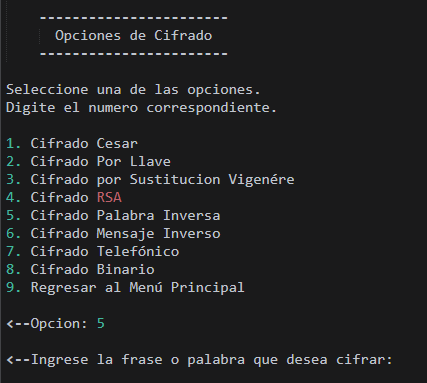
La interacción con el Menú de Cifrado o de Opciones de Cifrado sucede de la misma forma en que con el Menú de Navegación Principal. Se requiere que el usuario seleccione una de las opciones que este le muestra. Para seleccionarla, es necesario que ingrese el valor numérico que antecede a cada una de estas (ver Imagen).



En este caso las opciones desplegadas refieren a cada uno de los algoritmos de cifrado disponibles dentro del programa. Los valores válidos para ser ingresados en esta sección son valores numéricos entre 1 y 9. A diferencia del menú principal, en la última de las opciones se cuenta con la funcionalidad no de finalizar del programa, sino de regresar al Menú Principal.

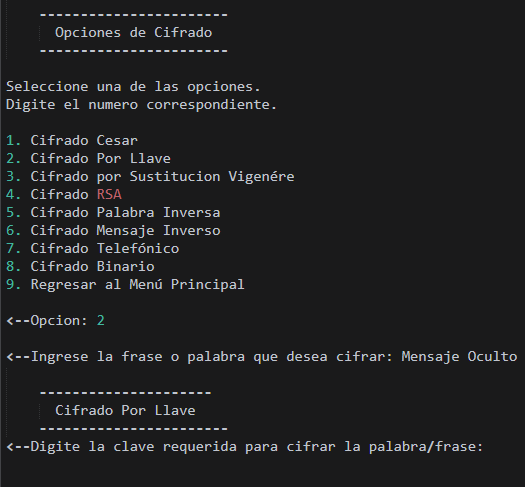


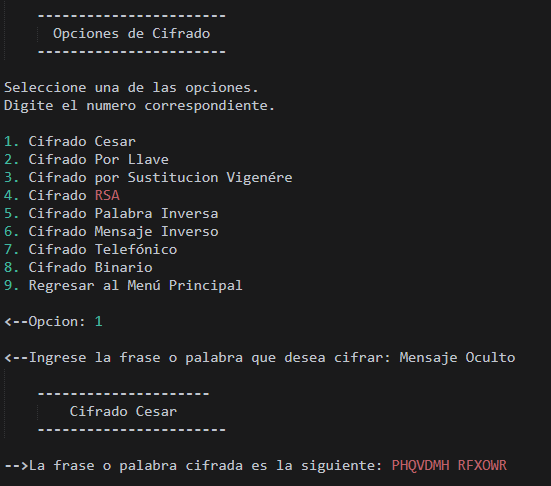
En caso de que se seleccione alguna de las opciones válidas, se desplegará el espacio para que el usuario ingrese la frase que desea convertir a partir del algoritmo seleccionado. Como ejemplo de este proceso se incluyen capturas de la selección de las opciones 1, 5, y 8. El detalle del ingreso a cada sección, se mostrará en la sección que corresponda a cada opción de cifrado.



Seguidamente, luego de haber ingresado la frase o palabra a cifrar, de acuerdo con la opción seleccionada se solicitará que el usuario ingrese cualquier otro valor que sea necesario para el correcto funcionamiento del algoritmo. De no ser necesario otra entrada por parte del usuario, el programa desplegará el resultado del proceso de cifrado del algoritmo.

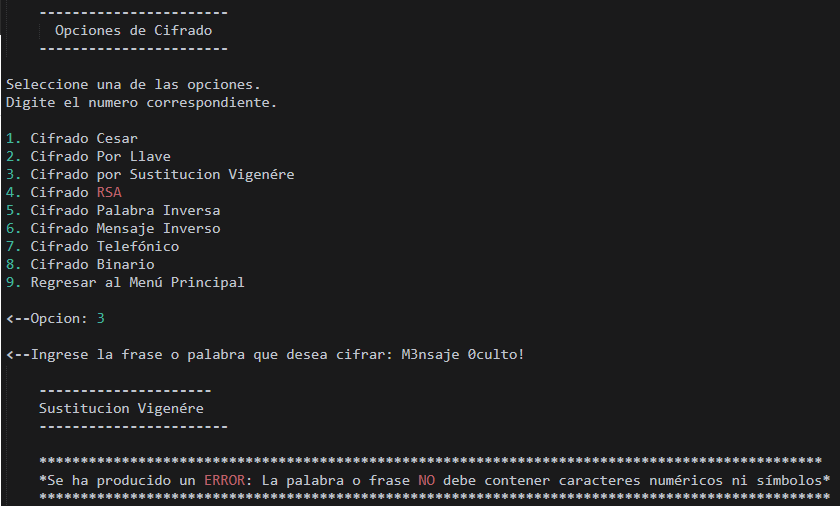
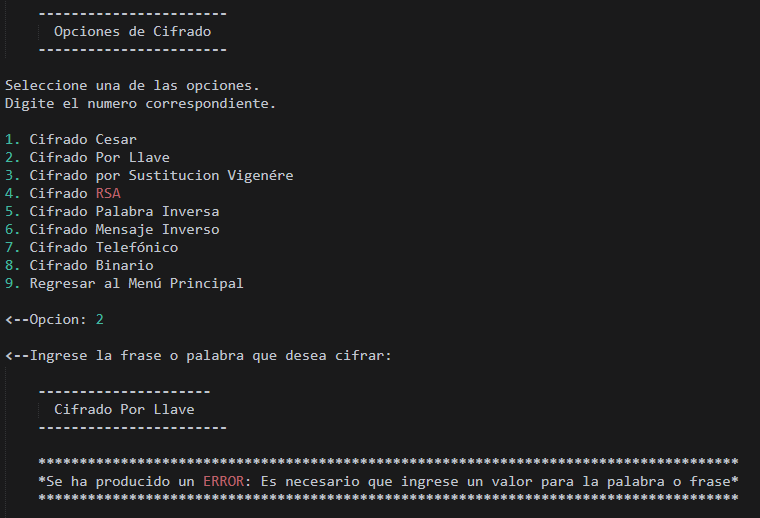
De acuerdo con lo anterior, un ejemplo se da en la opción de cifrado 2, para la cual es necesario que es usuario ingrese una clave para proceder con el cifrado de la frase. Esta se detalla en la siguiente imagen.

Para el caso que no se requiere ingresar un valor adicional a la frase, puede tomarse como ejemplo la selección del algoritmo de cifrado 1.



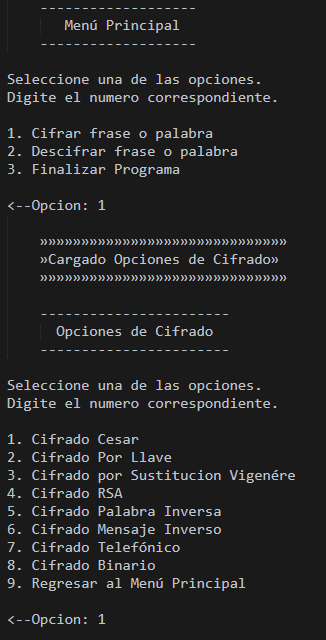
Al igual que en la selección de opciones de los menús, para el ingreso de la frase o palabra que el usuario requiera cifrar, se cuenta con proceso de validación. Este proceso puede variar de acuerdo con el algoritmo seleccionado. Para efectos del menú de opciones de cifrado se sigue la misma estructura para las diferentes opciones: se despliega el espacio para que el usuario ingrese la palabra o frase, y en caso de que su entrada no sea válida, se desplegará un mensaje indicando la razón por la cual esta entrada no es válida.

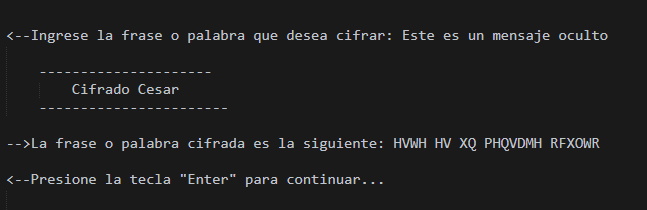
Como ejemplo para los procesos anteriormente mencionados se incluyen capturas de las opciones 2, 3 y 7, para cuales en caso de que se incumplan las restricciones de la entrada de la frase, se despliega el mensaje correspondiente.



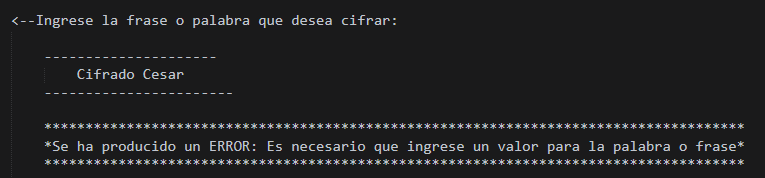


### Opción Cifrado César

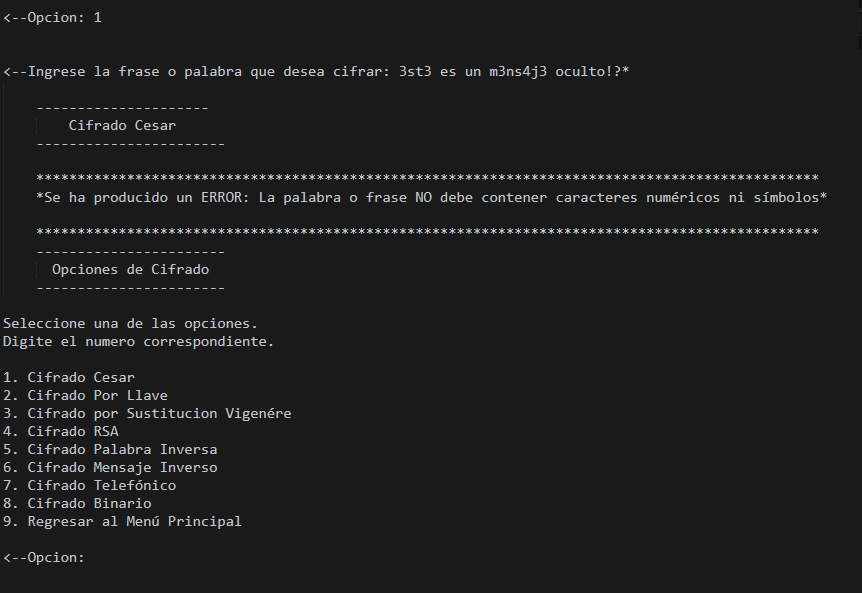
Para ingresar a esta opción es necesario seleccionar la opción 1 en el Menú Principal, y la opción 1 en el Menú de Opciones de Cifrado.

Luego de seleccionar ambas opciones el programa deberá desplegar el espacio para que el usuario ingrese la frase que desea convertir a partir del cifrado César. Para los valores aceptados dentro de este algoritmo se tiene que son permitidos los siguientes caracteres del alfabeto: a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, z y los espacios en blanco. En caso de que la entrada del usuario sea la correcta, se mostrará el título de la sección, seguido del resultado de realizar la conversión mediante el algoritmo seleccionado. Este proceso puede observarse en la siguiente imagen.

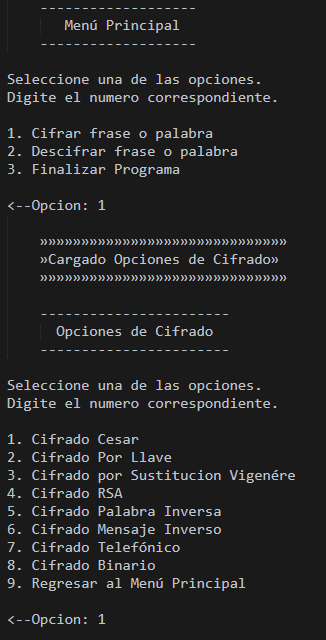
Si la entrada del usuario no es correcta, o incluye algún valor no válido para el algoritmo de cifrado César, el programa le retornará un mensaje indicando la razón por la cual no es válido es valor ingresado. En primera instancia, si no ingresa ningún valor para la frase a cifrar le retornara el siguiente mensaje.

En caso de que haya ingresado un caracter no valido o se realice una combinación de caracteres válidos y no permitidos en su entrada, se mostrará el siguiente mensaje.

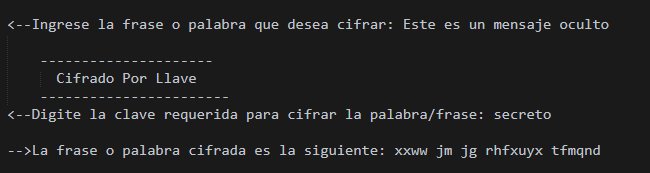


Para todos los casos mencionados sobre las posibles entradas de este algoritmo, erradas o válidas, luego de desplegar los mensajes correspondientes, se retornará al Menú de Opciones de Cifrado.

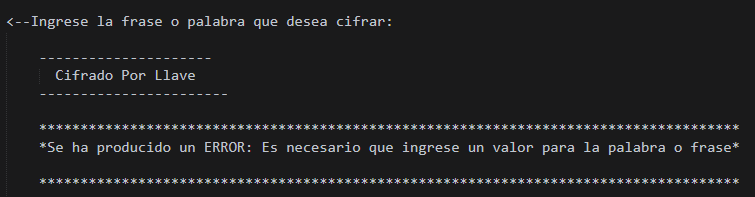
### Opción Cifrado por Llave

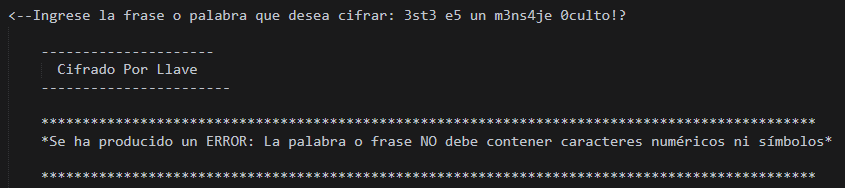
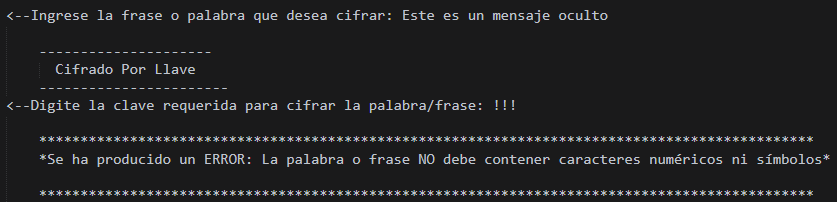
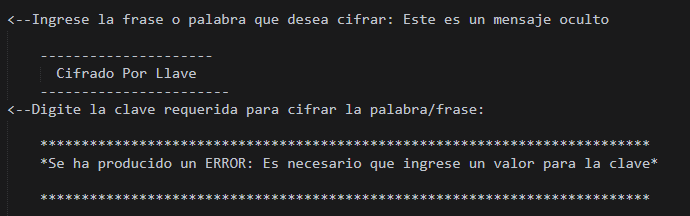
Para ingresar a esta opción es necesario seleccionar la opción 1 en el Menú Principal, y la opción 2 en el Menú de Opciones de Cifrado.

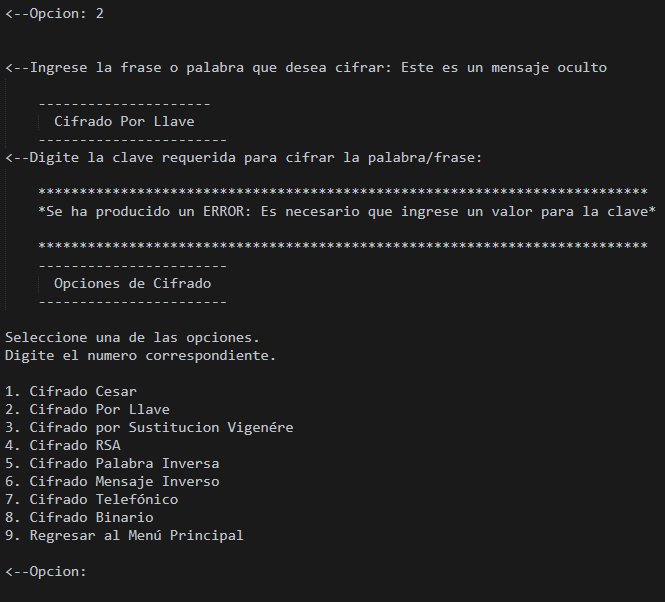
Luego de seleccionar ambas opciones el programa deberá desplegar el espacio para que el usuario ingrese la frase que desea convertir a partir del cifrado Por Llave. Para los valores aceptados para la frase dentro de este algoritmo, se tiene que son permitidos los siguientes caracteres del alfabeto: a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, z y los espacios en blanco. Para la clave se permiten los mismos valores, exceptuando el espacio.

En caso de que la entrada del usuario sea la correcta, se mostrará el título de la sección, seguido del resultado de realizar la conversión mediante el algoritmo seleccionado. Este proceso puede observarse en la siguiente imagen.

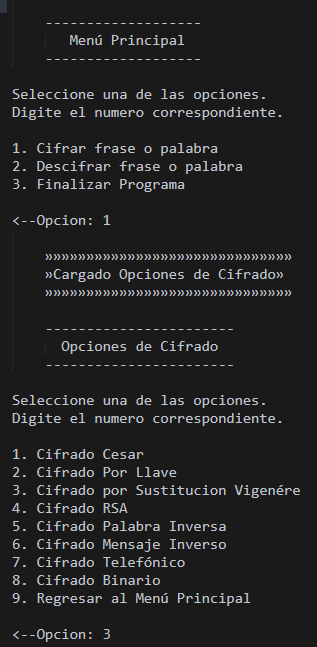
Si la entrada del usuario no es correcta, o incluye algún valor no válido para el algoritmo de cifrado Por Llave, el programa le retornará un mensaje indicando la razón por la cual no es válido es valor ingresado. En primera instancia, si no ingresa ningún valor para la frase a cifrar le retornara el siguiente mensaje.

En caso de que haya ingresado un caracter no valido o se realice una combinación de caracteres válidos y no permitidos en su entrada, se mostrará el siguiente mensaje.

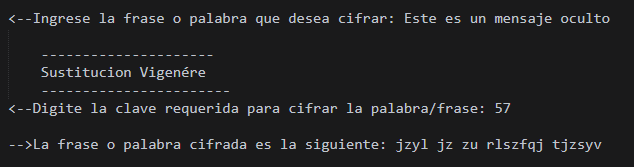
Para la palabra que será utilizada como la llave para este algoritmo de cifrado, si no se ingresa correctamente o se omite asignar un valor para esta, se desplegaran los mensajes correspondientes indicando razón por la cual la clave ingresada no es válida. Estas excepciones pueden observarse en las siguientes imágenes.

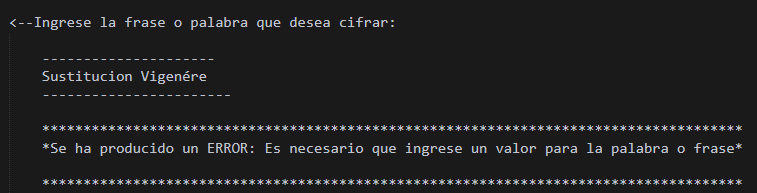
Para todos los casos mencionados sobre las posibles entradas de este algoritmo, erradas o válidas, luego de desplegar los mensajes correspondientes, se retornará al Menú de Opciones de Cifrado.

### Opción Cifrado por Sustitución Vigenére

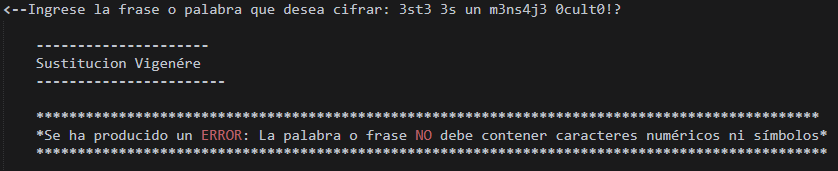
Para ingresar a esta opción es necesario seleccionar la opción 1 en el Menú Principal, y la opción 3 en el Menú de Opciones de Cifrado.

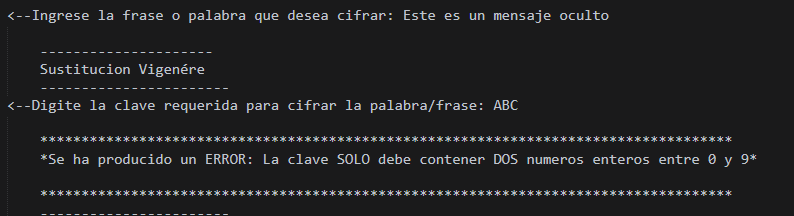
Luego de seleccionar ambas opciones el programa deberá desplegar el espacio para que el usuario ingrese la frase que desea convertir a partir del cifrado por Sustitución Vigenére. Para los valores aceptados para la frase dentro de este algoritmo, se tiene que son permitidos los siguientes caracteres del alfabeto: a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, z y espacios en blanco. Para la clave se permiten sólo dos valores numéricos enteros entre 1 y 9.

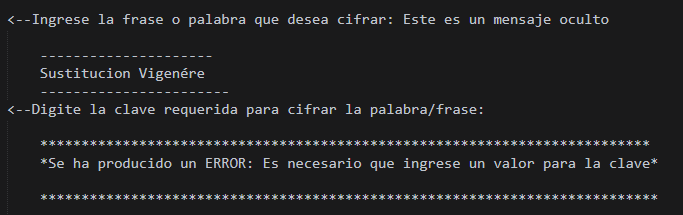
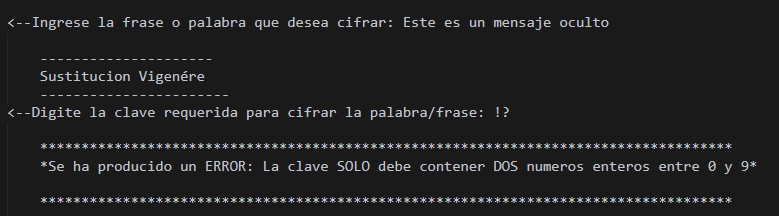
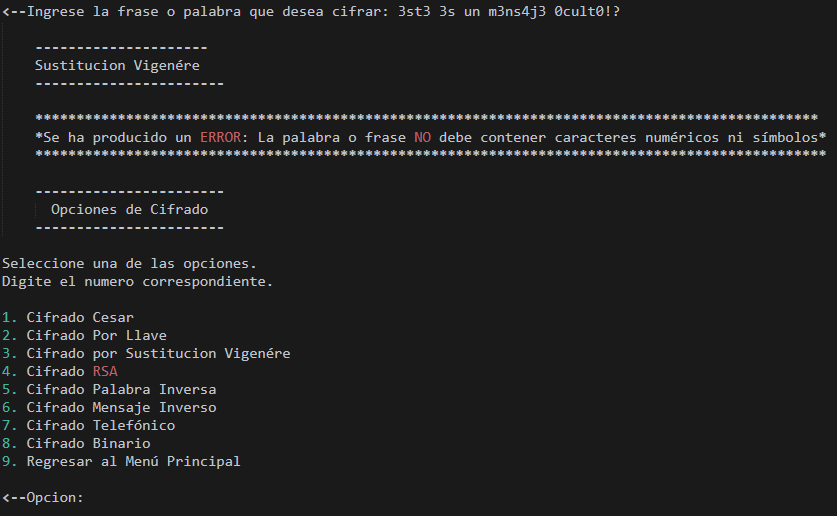
En caso de que la entrada del usuario sea la correcta, se mostrará el título de la sección, seguido del resultado de realizar la conversión mediante el algoritmo seleccionado. Este proceso puede observarse en la siguiente imagen.

Si la entrada del usuario no es correcta, o incluye algún valor no válido para el algoritmo de cifrado por Sustitución Vigenére, el programa le retornará un mensaje indicando la razón por la cual no es válido es valor ingresado. En primera instancia, si no ingresa ningún valor para la frase a cifrar le retornara el siguiente mensaje.

En caso de que haya ingresado un caracter no valido o se realice una combinación de caracteres válidos y no permitidos en su entrada, se mostrará el siguiente mensaje.

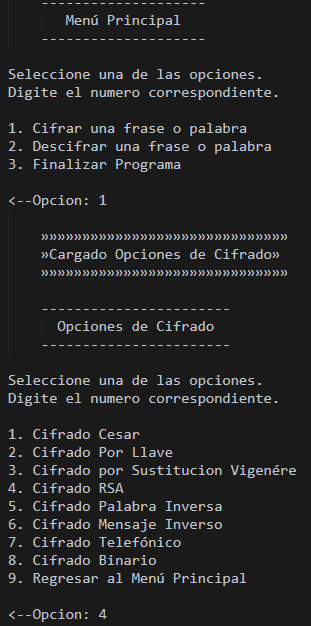


Para la clave que será utilizada para este algoritmo de cifrado, si no se ingresa correctamente o se omite asignar un valor para esta, se desplegaran los mensajes correspondientes indicando razón por la cual la clave ingresada no es válida. Estas excepciones pueden observarse en las siguientes imágenes.

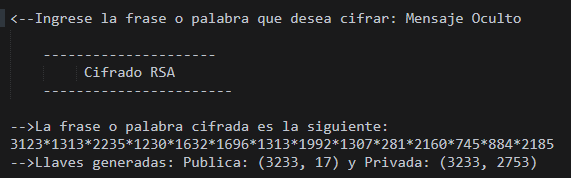
Para todos los casos mencionados sobre las posibles entradas de este algoritmo, erradas o válidas, luego de desplegar los mensajes correspondientes, se retornará al Menú de Opciones de Cifrado.

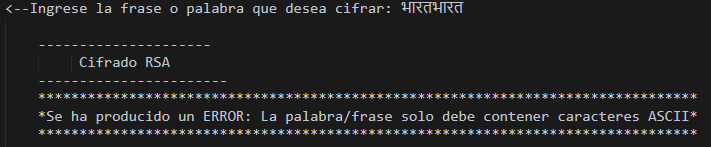
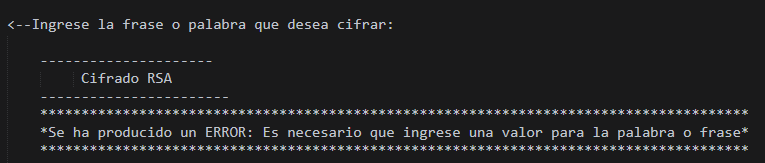
### Opción Cifrado RSA

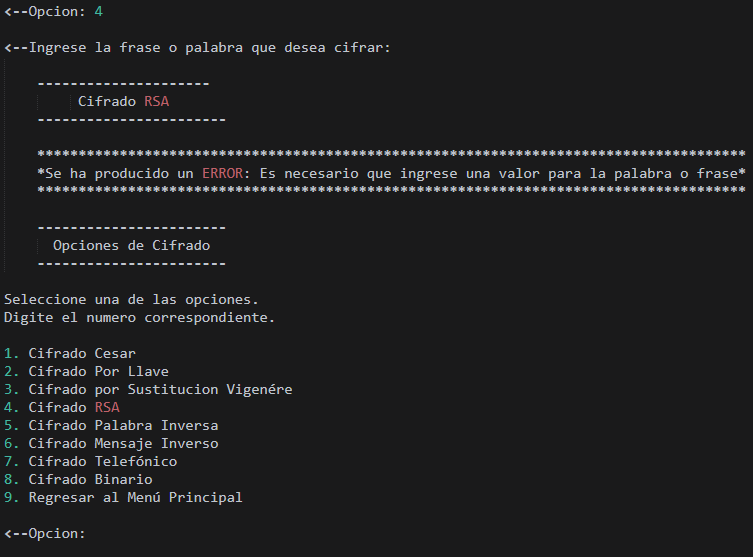
Para ingresar a esta opción es necesario seleccionar la opción 1 en el Menú Principal, y la opción 4 en el Menú de Opciones de Cifrado.

Luego de seleccionar ambas opciones el programa deberá desplegar el espacio para que el usuario ingrese la frase que desea convertir a partir del cifrado RSA (Rivest, Shamir y Adleman). Para los valores aceptados para la frase dentro de este algoritmo, se tiene que son permitidos cualquiera de los 256 caracteres comprendidos dentro del [código ASCII](https://www.ascii-code.com/). 

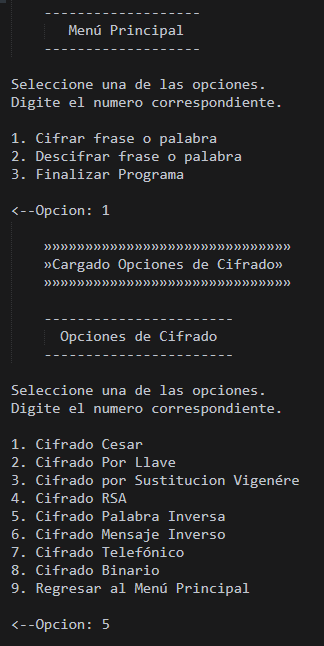
En caso de que la entrada del usuario sea la correcta, se mostrará el título de la sección, seguido del resultado de realizar la conversión mediante el algoritmo seleccionado y en la siguiente línea se incluyen los valores de ambas claves generadas por el algoritmo. Este proceso puede observarse en la siguiente imagen.

Si la entrada del usuario no es correcta, o incluye algún valor no válido para el algoritmo de cifrado RSA, el programa le retornará un mensaje indicando la razón por la cual no es válido es valor ingresado. En primera instancia, si no ingresa ningún valor para la frase a cifrar le retornara el siguiente mensaje.

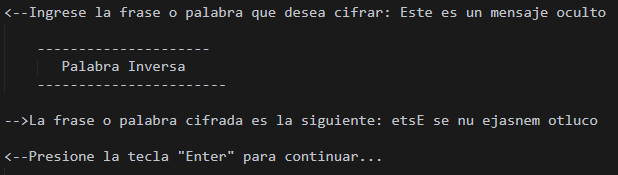
En caso de que haya ingresado un caracter no valido o se realice una combinación de caracteres válidos y no permitidos en su entrada, se mostrará el siguiente mensaje.

Para todos los casos mencionados sobre las posibles entradas de este algoritmo, erradas o válidas, luego de desplegar los mensajes correspondientes, se retornará al Menú de Opciones de Cifrado.

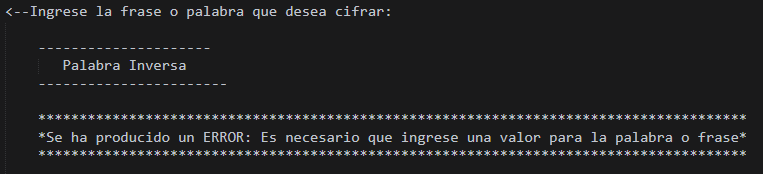
### Opción Cifrado Palabra inversa

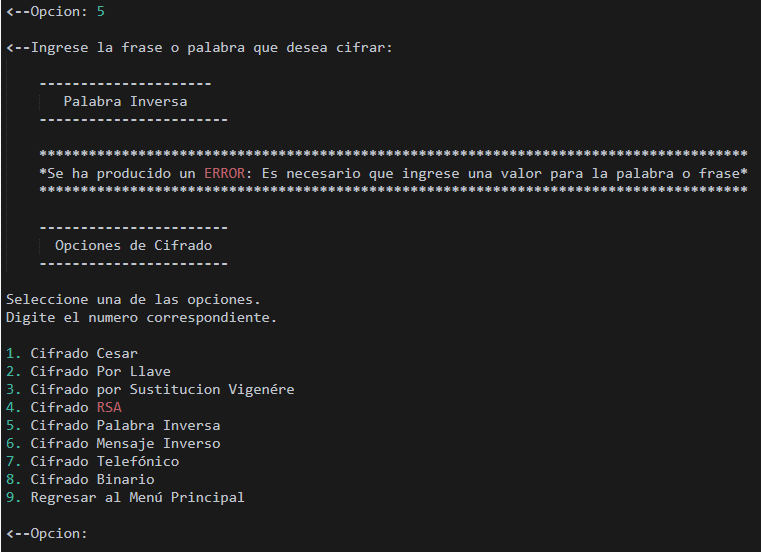
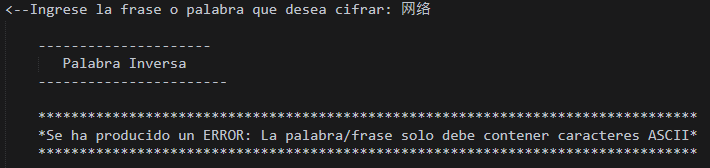
Para ingresar a esta opción es necesario seleccionar la opción 1 en el Menú Principal, y la opción 5 en el Menú de Opciones de Cifrado.

Luego de seleccionar ambas opciones el programa deberá desplegar el espacio para que el usuario ingrese la frase que desea convertir a partir del cifrado de Palabra Inversa. Para los valores aceptados alfabeto válido es cualquier símbolo, número o carácter.

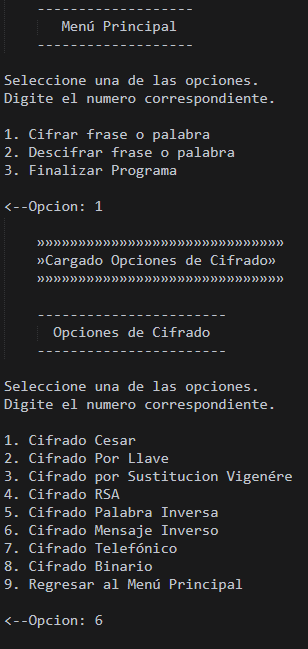
En caso de que la entrada del usuario sea la correcta, se mostrará el título de la sección, seguido del resultado de realizar la conversión mediante el algoritmo seleccionado Este proceso puede observarse en la siguiente imagen.

Si la entrada del usuario no es correcta, o incluye algún valor no válido para el algoritmo de cifrado de Palabra Inversa, el programa le retornará un mensaje indicando la razón por la cual no es válido es valor ingresado. En primera instancia, si no ingresa ningún valor para la frase a cifrar le retornara el siguiente mensaje.

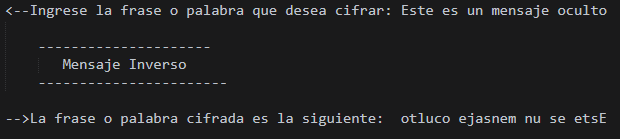
En caso de que haya ingresado un caracter no valido o se realice una combinación de caracteres válidos y no permitidos en su entrada, se mostrará el siguiente mensaje.

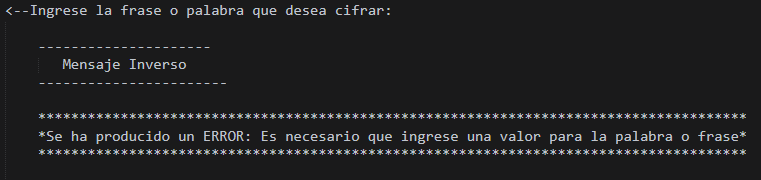
Para todos los casos mencionados sobre las posibles entradas de este algoritmo, erradas o válidas, luego de desplegar los mensajes correspondientes, se retornará al Menú de Opciones de Cifrado.

### Opción Cifrado Mensaje inverso

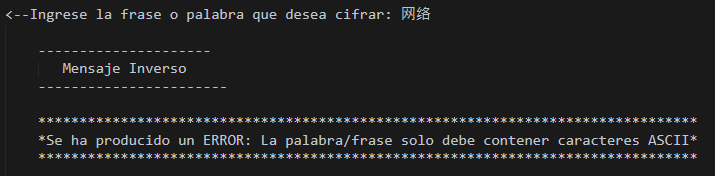
Para ingresar a esta opción es necesario seleccionar la opción 1 en el Menú Principal, y la opción 6 en el Menú de Opciones de Cifrado.

Luego de seleccionar ambas opciones el programa deberá desplegar el espacio para que el usuario ingrese la frase que desea convertir a partir del cifrado de Mensaje Inverso. Para los valores aceptados para la frase dentro de este algoritmo, se tiene que son permitidos cualquiera de los 256 caracteres comprendidos dentro del [código ASCII](https://www.ascii-code.com/).

En caso de que la entrada del usuario sea la correcta, se mostrará el título de la sección, seguido del resultado de realizar la conversión mediante el algoritmo seleccionado Este proceso puede observarse en la siguiente imagen.

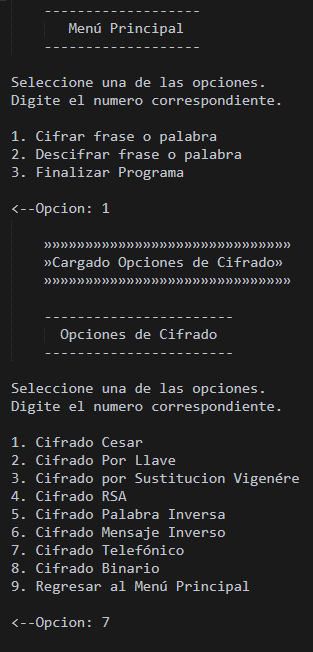
Si la entrada del usuario no es correcta, o incluye algún valor no válido para el algoritmo de cifrado de Mensaje Inverso, el programa le retornará un mensaje indicando la razón por la cual no es válido es valor ingresado. En primera instancia, si no ingresa ningún valor para la frase a cifrar le retornara el siguiente mensaje.

En caso de que haya ingresado un caracter no valido o se realice una combinación de caracteres válidos y no permitidos en su entrada, se mostrará el siguiente mensaje.

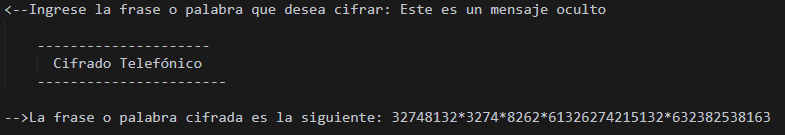


Para todos los casos mencionados sobre las posibles entradas de este algoritmo, erradas o válidas, luego de desplegar los mensajes correspondientes, se retornará al Menú de Opciones de Cifrado.

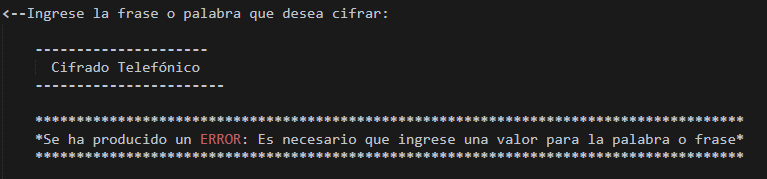
### Opción Cifrado Telefónico

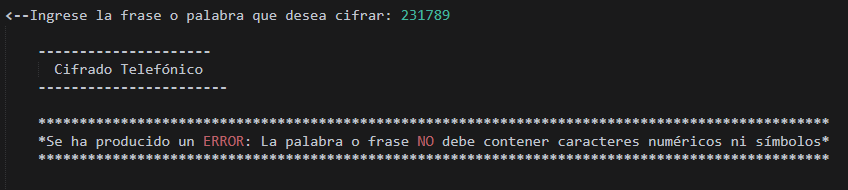
Para ingresar a esta opción es necesario seleccionar la opción 1 en el Menú Principal, y la opción 7 en el Menú de Opciones de Cifrado.

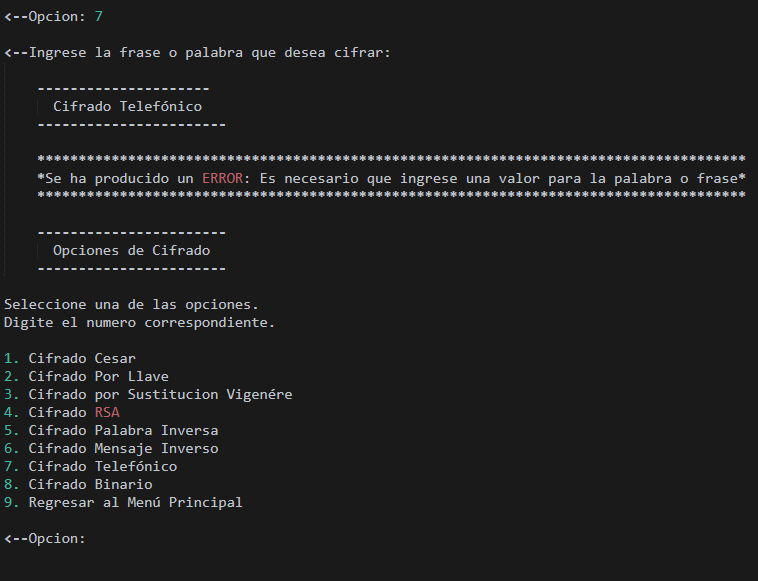
Luego de seleccionar ambas opciones el programa deberá desplegar el espacio para que el usuario ingrese la frase que desea convertir a partir del cifrado de Cifrado Telefónico. Para los valores aceptados para la frase dentro de este algoritmo, se tiene que son permitidos cualquiera de las letras que se muestran en la figura del teclado telefónico y los espacios en blanco.

En caso de que la entrada del usuario sea la correcta, se mostrará el título de la sección, seguido del resultado de realizar la conversión mediante el algoritmo seleccionado. Este proceso puede observarse en la siguiente imagen.

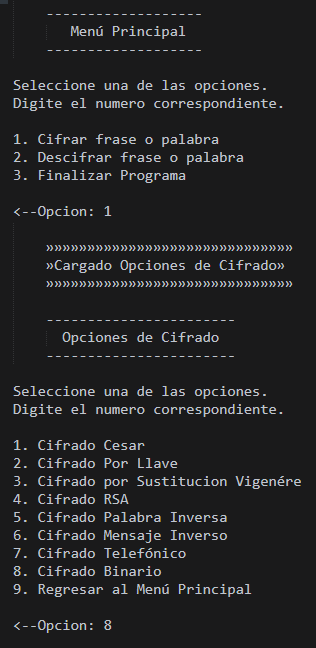
Si la entrada del usuario no es correcta, o incluye algún valor no válido para el algoritmo de cifrado de Cifrado Telefónico, el programa le retornará un mensaje indicando la razón por la cual no es válido es valor ingresado. En primera instancia, si no ingresa ningún valor para la frase a cifrar le retornara el siguiente mensaje.

En caso de que haya ingresado un caracter no valido o se realice una combinación de caracteres válidos y no permitidos en su entrada, se mostrará el siguiente mensaje.

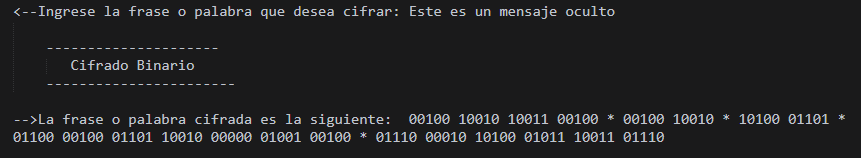
Para todos los casos mencionados sobre las posibles entradas de este algoritmo, erradas o válidas, luego de desplegar los mensajes correspondientes, se retornará al Menú de Opciones de Cifrado.



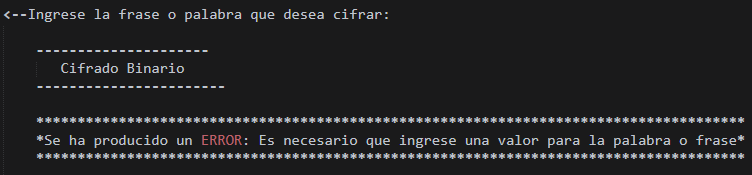
### Opción Cifrado Binario

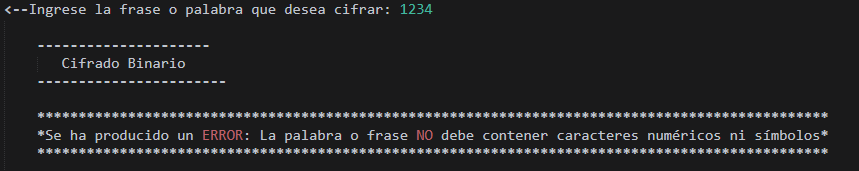
Para ingresar a esta opción es necesario seleccionar la opción 1 en el Menú Principal, y la opción 8 en el Menú de Opciones de Cifrado.

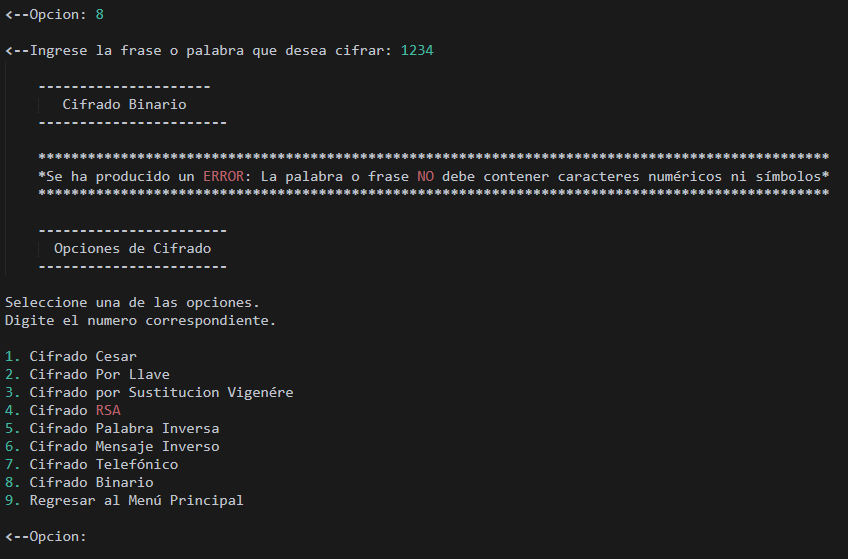
Luego de seleccionar ambas opciones el programa deberá desplegar el espacio para que el usuario ingrese la frase que desea convertir a partir del cifrado Binario. Para los valores aceptados para la frase dentro de este algoritmo, se tiene que se tiene que son permitidos los siguientes caracteres del alfabeto: a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, z y los espacios en blanco.

En caso de que la entrada del usuario sea la correcta, se mostrará el título de la sección, seguido del resultado de realizar la conversión mediante el algoritmo seleccionado Este proceso puede observarse en la siguiente imagen.

Si la entrada del usuario no es correcta, o incluye algún valor no válido para el algoritmo de cifrado Binario, el programa le retornará un mensaje indicando la razón por la cual no es válido es valor ingresado. En primera instancia, si no ingresa ningún valor para la frase a cifrar le retornara el siguiente mensaje.

En caso de que haya ingresado un caracter no valido o se realice una combinación de caracteres válidos y no permitidos en su entrada, se mostrará el siguiente mensaje.



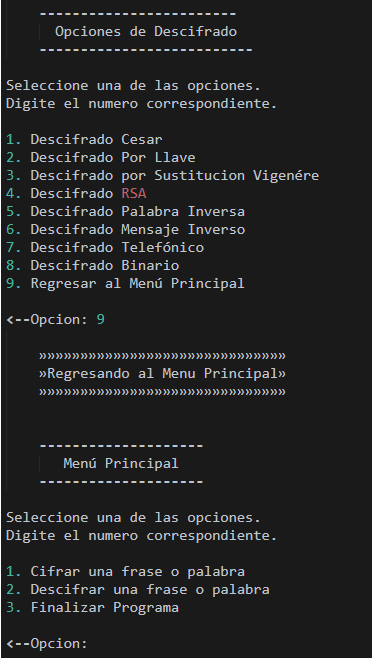
Para todos los casos mencionados sobre las posibles entradas de este algoritmo, erradas o válidas, luego de desplegar los mensajes correspondientes, se retornará al Menú de Opciones de Cifrado.

## Menú Descifrado

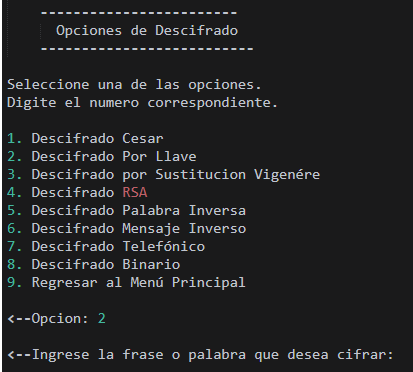
La interacción con el Menú de Descifrado o de Opciones de Descifrado sucede de la misma forma en que con el Menú de Navegación Principal y de Opciones de Cifrado. Se requiere que el usuario seleccione una de las opciones que este le muestra. Para seleccionarla, es necesario que ingrese el valor numérico que antecede a cada una de estas (ver Imagen).

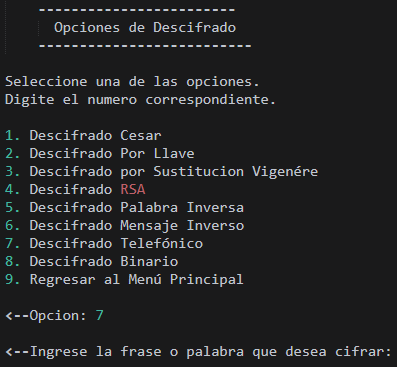


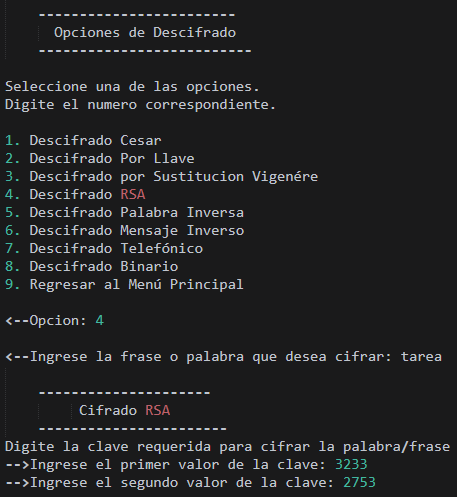
En este caso las opciones desplegadas refieren a cada uno de los algoritmos de descifrado disponibles dentro del programa. Los valores válidos para ser ingresados en esta sección son valores numéricos entre 1 y 9. A diferencia del menú principal, en la última de las opciones se cuenta con la funcionalidad no de finalizar del programa, sino de regresar al Menú Principal.



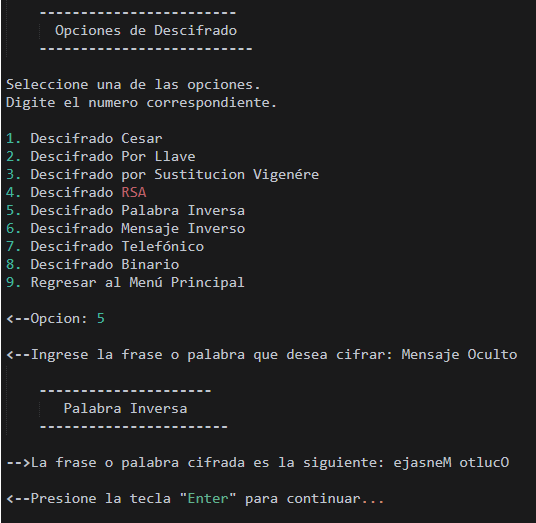
En caso de que se seleccione alguna de las opciones válidas, se desplegará el espacio para que el usuario ingrese la frase que desea convertir a partir del algoritmo seleccionado. Como ejemplo de este proceso se incluyen capturas de la selección de las opciones 2, 4, y 7. El detalle del ingreso a cada sección, se mostrará en la sección que corresponda a cada opción de descifrado.



Seguidamente, luego de haber ingresado la frase o palabra a descifrar, de acuerdo a la opción seleccionada se solicitará que el usuario ingrese cualquier otro valor que sea necesario para el correcto funcionamiento del algoritmo. De no ser necesario otra entrada por parte del usuario, el programa desplegará el resultado del proceso de cifrado del algoritmo.

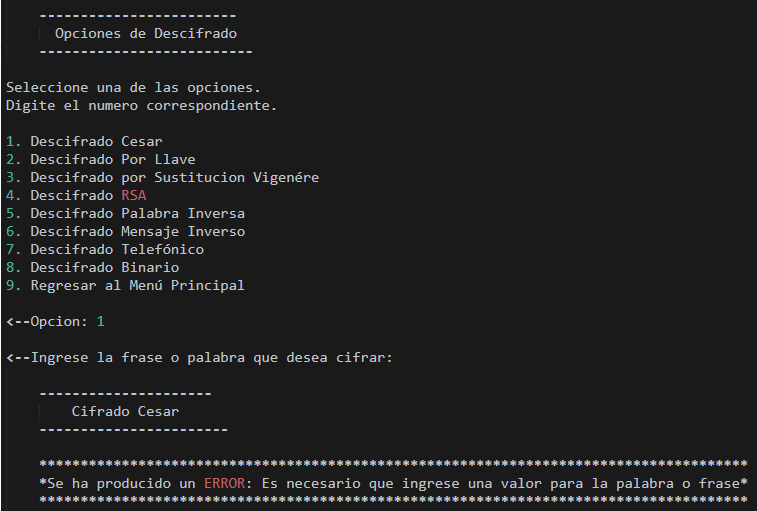
De acuerdo con lo anterior, un ejemplo se da en la opción de cifrado 4, para la cual es necesario que es usuario ingrese los valores de una de las llaves generadas en el proceso de cifrado para proceder con el descifrado de la frase. Esta se detalla en la siguiente imagen.

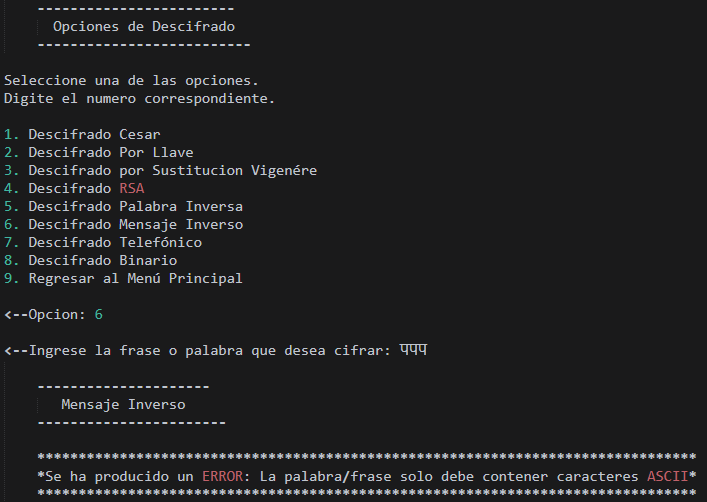
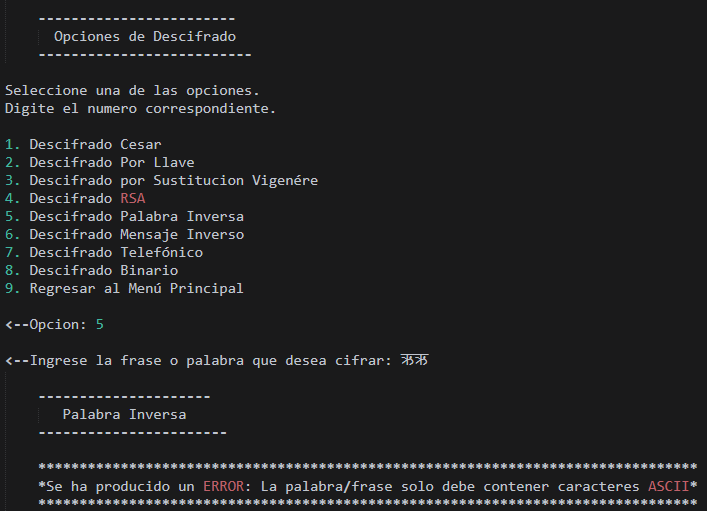
Para el caso que no se requiere ingresar un valor adicional a la frase, puede tomarse como ejemplo la selección del algoritmo de cifrado 5.



Al igual que en la selección de opciones de los menús, para el ingreso de la frase o palabra que el usuario requiera cifrar, se cuenta con proceso de validación. Este proceso puede variar de acuerdo con el algoritmo seleccionado. Para efectos del menú de opciones de descifrado se sigue la misma estructura para las diferentes opciones: se despliega el espacio para que el usuario ingrese la palabra o frase, y en caso de que su entrada no sea válida, se desplegará un mensaje indicando la razón por la cual esta entrada no es válida.

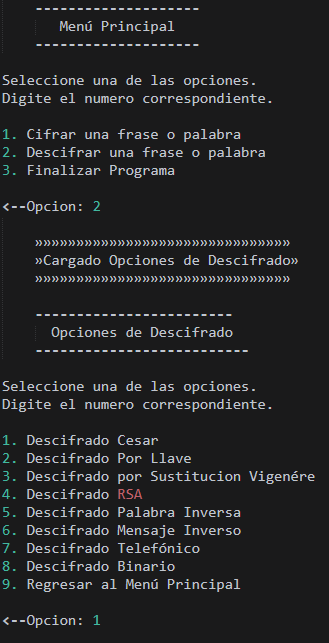
Como ejemplo para los procesos anteriormente mencionados se incluyen capturas de las opciones 1, 6 y 5, para cuales en caso de que se incumplan las restricciones de la entrada de la frase, se despliega el mensaje correspondiente.

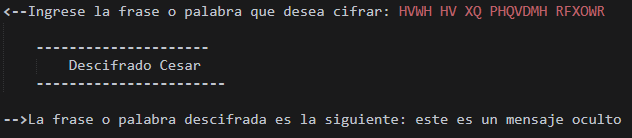




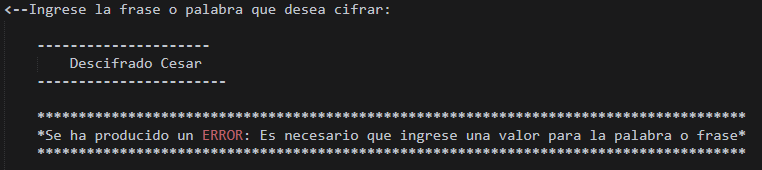
### Opción Descifrado César

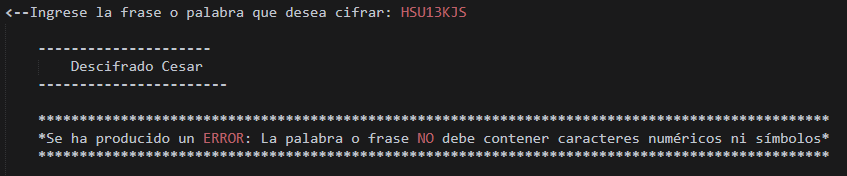
Para ingresar a esta opción es necesario seleccionar la opción 1 en el Menú Principal, y la opción 1 en el Menú de Opciones de Descifrado.

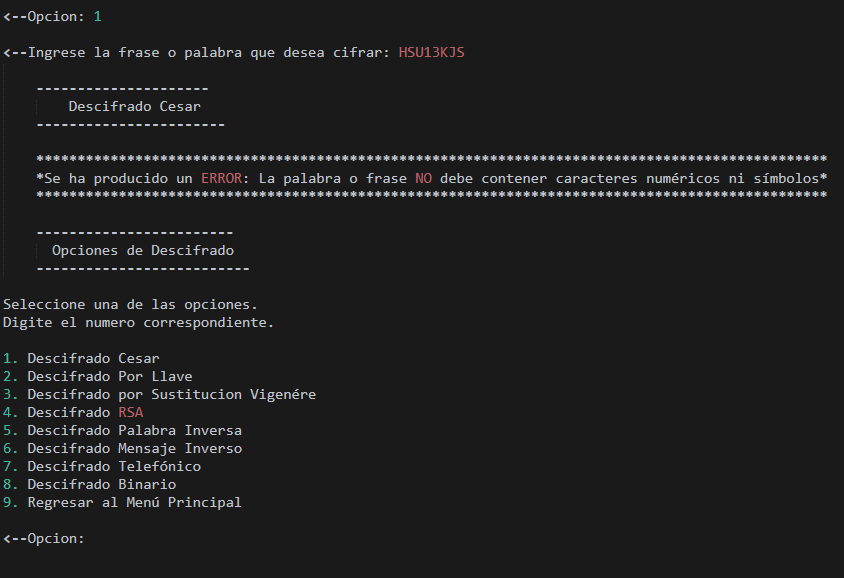


Luego de seleccionar ambas opciones el programa deberá desplegar el espacio para que el usuario ingrese la frase que desea convertir a partir del descifrado César. Para los valores aceptados dentro de este algoritmo se tiene que son permitidos los siguientes caracteres del alfabeto: a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, z y los espacios en blanco. En caso de que la entrada del usuario sea la correcta, se mostrará el título de la sección, seguido del resultado de realizar la conversión mediante el algoritmo seleccionado. Este proceso puede observarse en la siguiente imagen.

Si la entrada del usuario no es correcta, o incluye algún valor no válido para el algoritmo de descifrado César, el programa le retornará un mensaje indicando la razón por la cual no es válido es valor ingresado. En primera instancia, si no ingresa ningún valor para la frase a descifrar le retornara el siguiente mensaje.

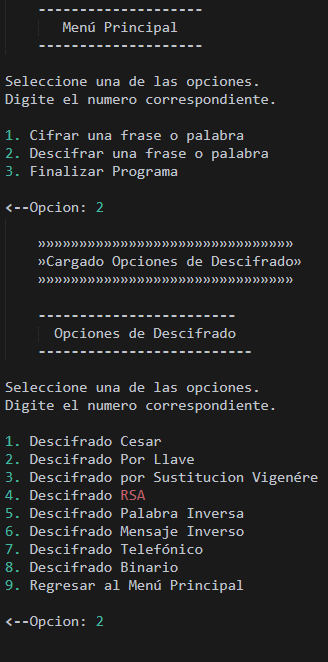
En caso de que haya ingresado un caracter no valido o se realice una combinación de caracteres válidos y no permitidos en su entrada, se mostrará el siguiente mensaje.



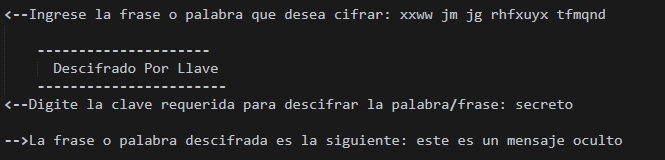
Para todos los casos mencionados sobre las posibles entradas de este algoritmo, erradas o válidas, luego de desplegar los mensajes correspondientes, se retornará al Menú de Opciones de Descifrado.

### Opción Descifrado por Llave

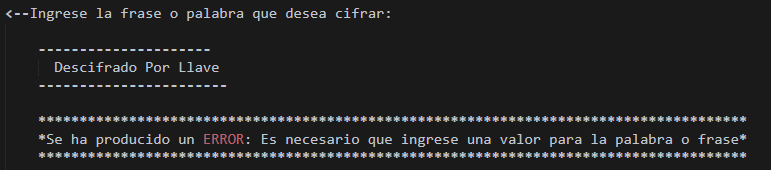
Para ingresar a esta opción es necesario seleccionar la opción 1 en el Menú Principal, y la opción 2 en el Menú de Opciones de Descifrado.



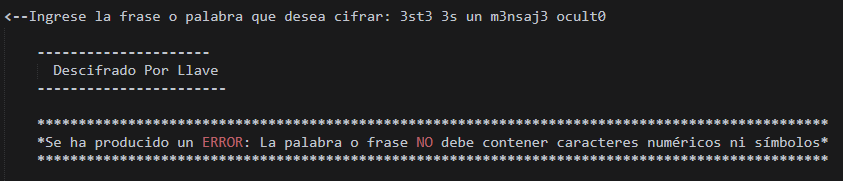
Luego de seleccionar ambas opciones el programa deberá desplegar el espacio para que el usuario ingrese la frase que desea convertir a partir del descifrado Por Llave. Para los valores aceptados para la frase dentro de este algoritmo, se tiene que son permitidos los siguientes caracteres del alfabeto: a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, z y los espacios en blanco. Para la clave se permiten los mismos valores, exceptuando el espacio.

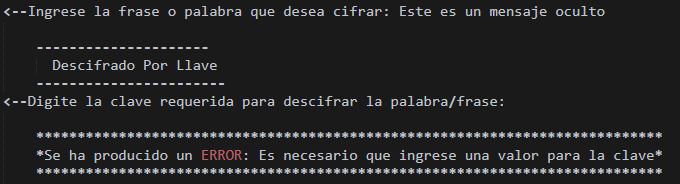
En caso de que la entrada del usuario sea la correcta, se mostrará el título de la sección, seguido del resultado de realizar la conversión mediante el algoritmo seleccionado. Este proceso puede observarse en la siguiente imagen.

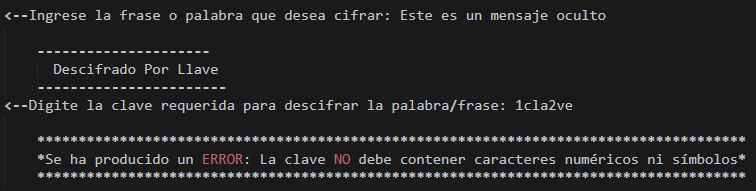
Si la entrada del usuario no es correcta, o incluye algún valor no válido para el algoritmo de descifrado Por Llave, el programa le retornará un mensaje indicando la razón por la cual no es válido es valor ingresado. En primera instancia, si no ingresa ningún valor para la frase a descifrar le retornará el siguiente mensaje.



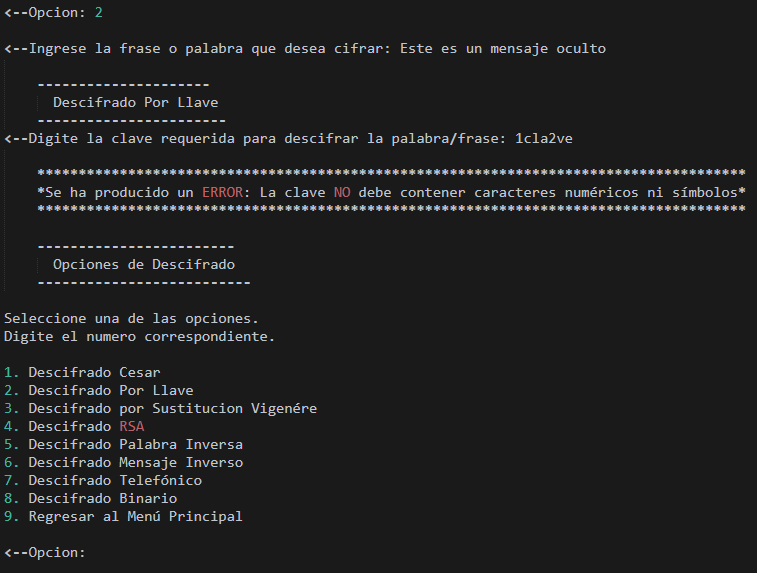
En caso de que haya ingresado un caracter no valido o se realice una combinación de caracteres válidos y no permitidos en su entrada, se mostrará el siguiente mensaje.



Para la palabra que será utilizada como la llave para este algoritmo de cifrado, si no se ingresa correctamente o se omite asignar un valor para esta, se desplegaran los mensajes correspondientes indicando razón por la cual la clave ingresada no es válida. Estas excepciones pueden observarse en las siguientes imágenes.



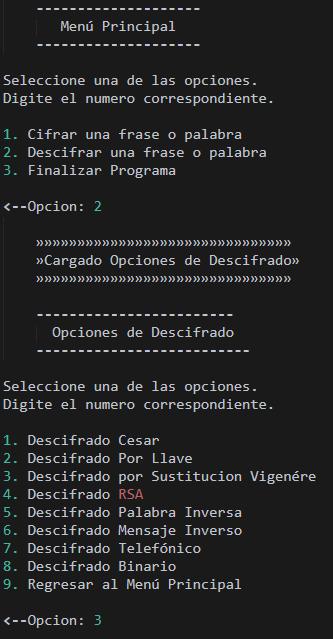
Para todos los casos mencionados sobre las posibles entradas de este algoritmo, erradas o válidas, luego de desplegar los mensajes correspondientes, se retornará al Menú de Opciones de Descifrado.



### 

### Opción Descifrado por Sustitución Vigenére

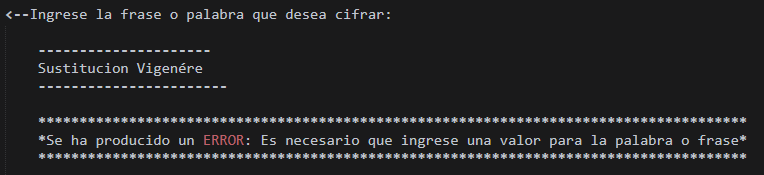
Para ingresar a esta opción es necesario seleccionar la opción 1 en el Menú Principal, y la opción 3 en el Menú de Opciones de Descifrado.



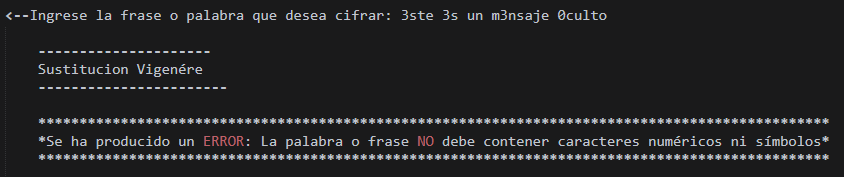
Luego de seleccionar ambas opciones el programa deberá desplegar el espacio para que el usuario ingrese la frase que desea convertir a partir del descifrado por Sustitución Vigenére. Para los valores aceptados para la frase dentro de este algoritmo, se tiene que son permitidos los siguientes caracteres del alfabeto: a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, z y espacios en blanco. Para la clave se permiten sólo dos valores numéricos enteros entre 1 y 9.

En caso de que la entrada del usuario sea la correcta, se mostrará el título de la sección, seguido del resultado de realizar la conversión mediante el algoritmo seleccionado. Este proceso puede observarse en la siguiente imagen.

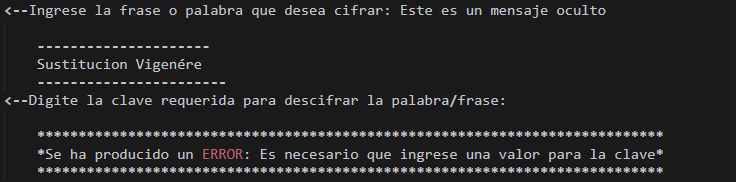
Si la entrada del usuario no es correcta, o incluye algún valor no válido para el algoritmo de descifrado por Sustitución Vigenére, el programa le retornará un mensaje indicando la razón por la cual no es válido es valor ingresado. En primera instancia, si no ingresa ningún valor para la frase a descifrar le retornara el siguiente mensaje.

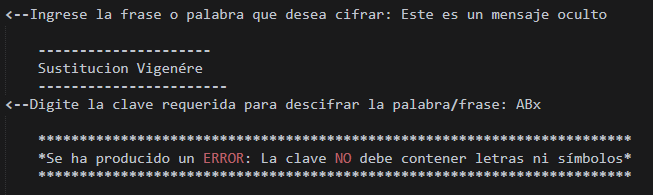


En caso de que haya ingresado un caracter no valido o se realice una combinación de caracteres válidos y no permitidos en su entrada, se mostrará el siguiente mensaje.

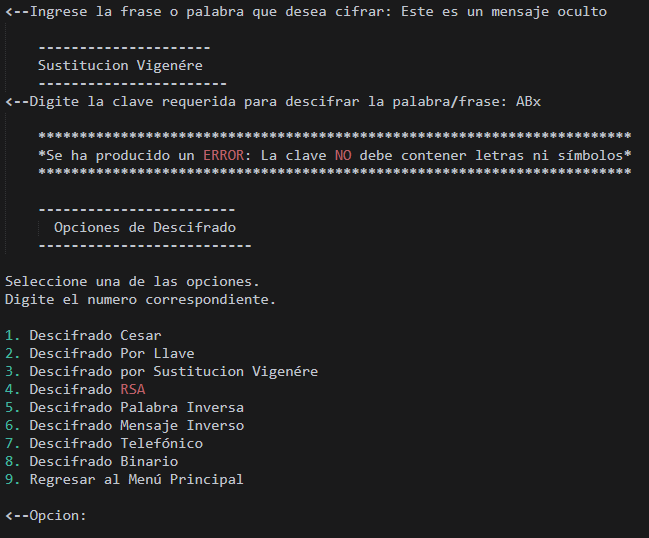


Para la clave que será utilizada por este algoritmo de cifrado, si no se ingresa correctamente o se omite asignar un valor para esta, se desplegaran los mensajes correspondientes indicando razón por la cual la clave ingresada no es válida. Estas excepciones pueden observarse en las siguientes imágenes.



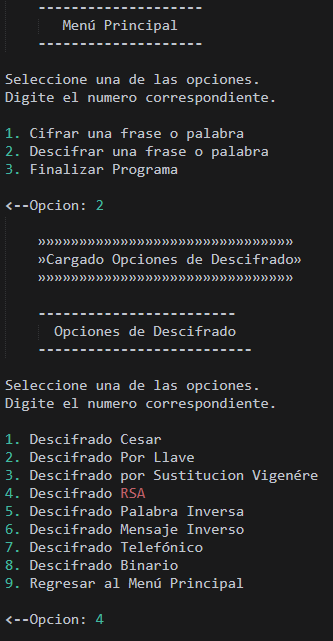


Para todos los casos mencionados sobre las posibles entradas de este algoritmo, erradas o válidas, luego de desplegar los mensajes correspondientes, se retornará al Menú de Opciones de Descifrado.



### Opción Descifrado RSA

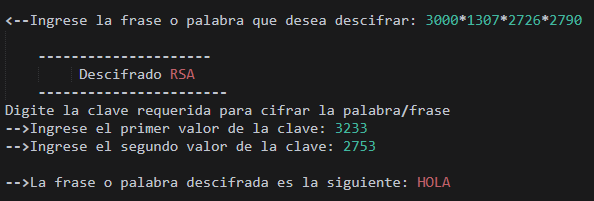
Para ingresar a esta opción es necesario seleccionar la opción 1 en el Menú Principal, y la opción 4 en el Menú de Opciones de Descifrado.

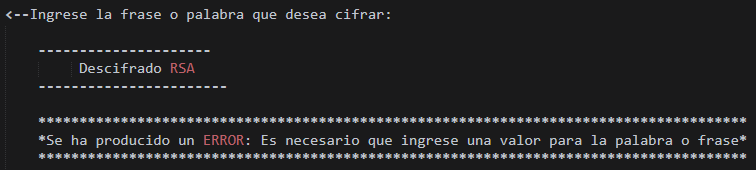


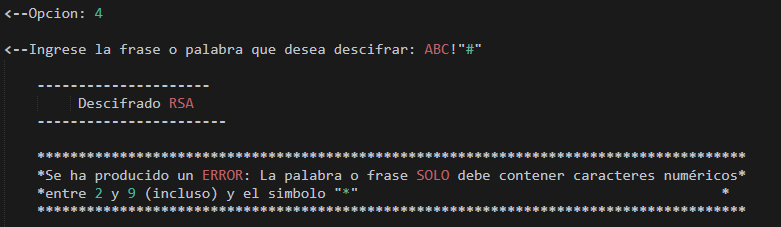
Luego de seleccionar ambas opciones el programa deberá desplegar el espacio para que el usuario ingrese la frase que desea convertir a partir del descifrado RSA (Rivest, Shamir y Adleman). Para los valores aceptados para la frase dentro de este algoritmo, se tiene que son permitidos solamente valores numéricos enteros, asteriscos y espacios en blanco.

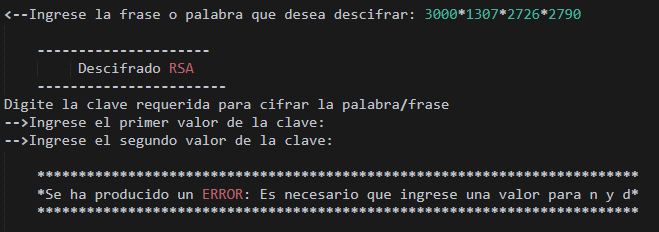
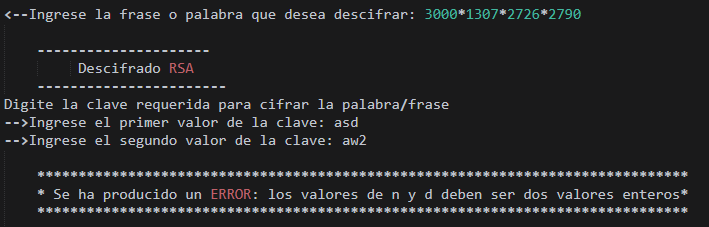
En este caso es necesario que el usuario ingrese los valores que componen la clave privada que fue utilizada para cifrar el mensaje previamente. En los posibles valores para esta, solo se permite el ingreso de dos valores enteros mayores a 0.

En caso de que la entrada del usuario sea la correcta, se mostrará el título de la sección, seguido del resultado de realizar la conversión mediante el algoritmo seleccionado y en la siguiente línea se incluyen los valores de ambas claves generadas por el algoritmo. Este proceso puede observarse en la siguiente imagen.

Si la entrada del usuario no es correcta, o incluye algún valor no válido para el algoritmo de cifrado RSA, el programa le retornará un mensaje indicando la razón por la cual no es válido es valor ingresado. En primera instancia, si no ingresa ningún valor para la frase a descifrar le retornara el siguiente mensaje.

En caso de que haya ingresado un caracter no valido o se realice una combinación de caracteres válidos y no permitidos en su entrada, se mostrará el siguiente mensaje.

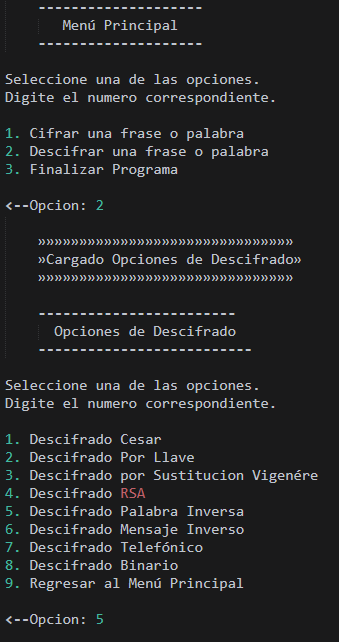
Para los valores de la clave privada que será utilizada por este algoritmo de cifrado, si no se ingresa correctamente o se omite asignar un valor para esta, se desplegaran los mensajes correspondientes indicando razón por la cual la clave ingresada no es válida. Estas excepciones pueden observarse en las siguientes imágenes.

Para todos los casos mencionados sobre las posibles entradas de este algoritmo, erradas o válidas, luego de desplegar los mensajes correspondientes, se retornará al Menú de Opciones de Descifrado.

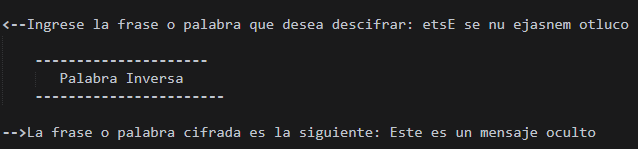


### Opción Descifrado Palabra inversa

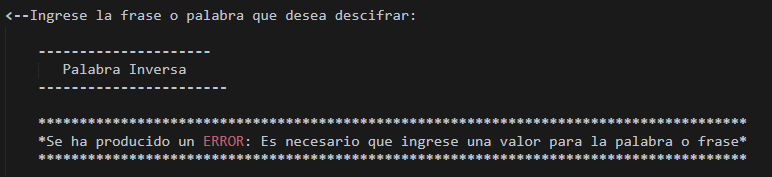
Para ingresar a esta opción es necesario seleccionar la opción 1 en el Menú Principal, y la opción 5 en el Menú de Opciones de Descifrado.

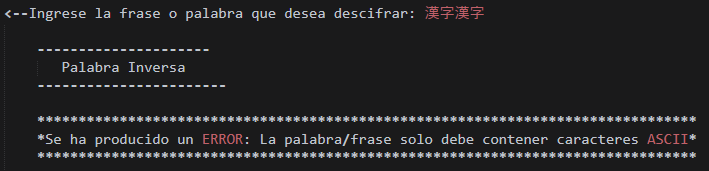


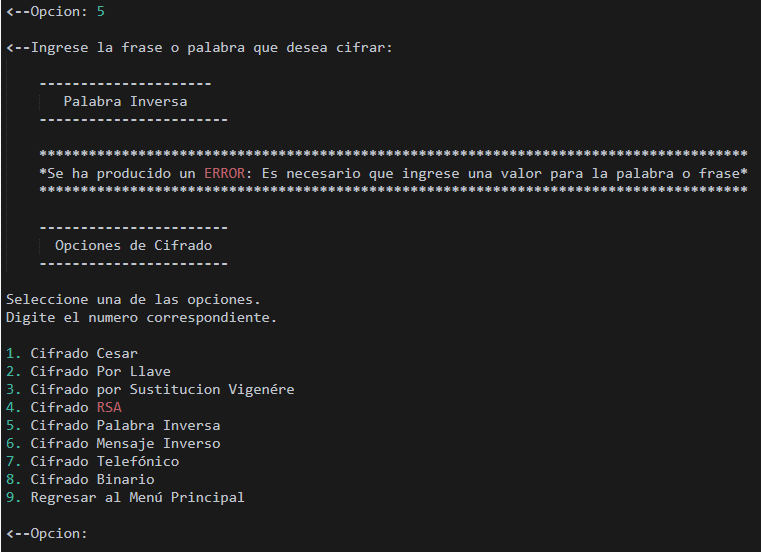
Luego de seleccionar ambas opciones el programa deberá desplegar el espacio para que el usuario ingrese la frase que desea convertir a partir del descifrado de Palabra Inversa. Para los valores aceptados para la frase dentro de este algoritmo, se tiene que son permitidos cualquiera de los 256 caracteres comprendidos dentro del [código ASCII](https://www.ascii-code.com/).

En caso de que la entrada del usuario sea la correcta, se mostrará el título de la sección, seguido del resultado de realizar la conversión mediante el algoritmo seleccionado y la siguiente línea se incluyen los valores de ambas claves generadas por el algoritmo. Este proceso puede observarse en la siguiente imagen.

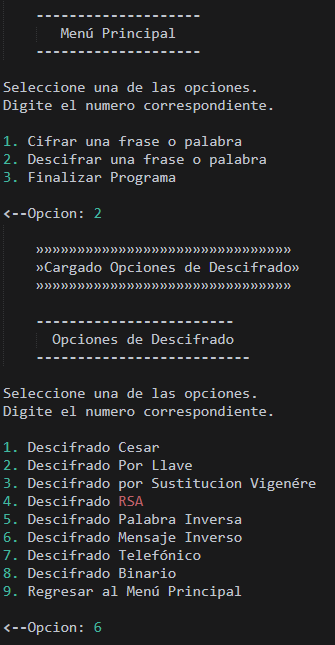
Si la entrada del usuario no es correcta, o incluye algún valor no válido para el algoritmo de descifrado de Palabra Inversa, el programa le retornará un mensaje indicando la razón por la cual no es válido es valor ingresado. En primera instancia, si no ingresa ningún valor para la frase a descifrar le retornara el siguiente mensaje.

En caso de que haya ingresado un caracter no valido o se realice una combinación de caracteres válidos y no permitidos en su entrada, se mostrará el siguiente mensaje.

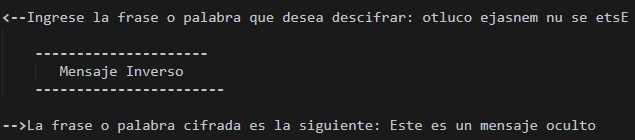


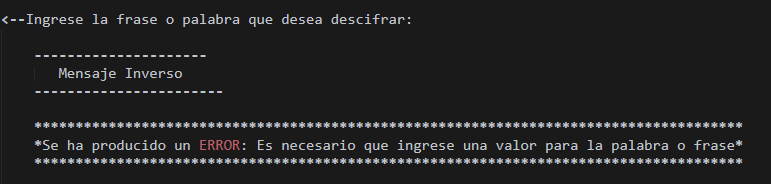
Para todos los casos mencionados sobre las posibles entradas de este algoritmo, erradas o válidas, luego de desplegar los mensajes correspondientes, se retornará al Menú de Opciones de Descifrado.

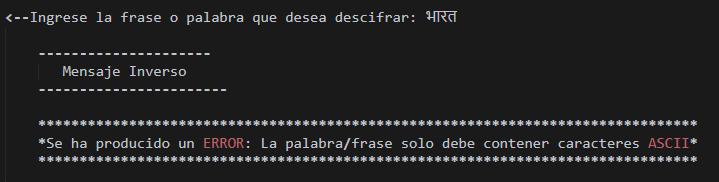
### Opción Descifrado Mensaje inverso

Para ingresar a esta opción es necesario seleccionar la opción 1 en el Menú Principal, y la opción 6 en el Menú de Opciones de Descifrado.

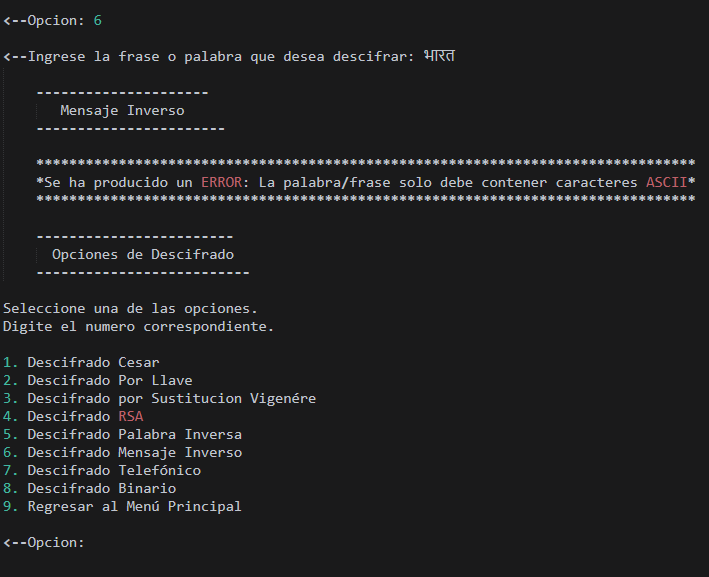
Luego de seleccionar ambas opciones el programa deberá desplegar el espacio para que el usuario ingrese la frase que desea convertir a partir del descifrado de Mensaje Inverso. Para los valores aceptados para la frase dentro de este algoritmo, se tiene que son permitidos cualquiera de los 256 caracteres comprendidos dentro del [código ASCII](https://www.ascii-code.com/).

En caso de que la entrada del usuario sea la correcta, se mostrará el título de la sección, seguido del resultado de realizar la conversión mediante el algoritmo seleccionado Este proceso puede observarse en la siguiente imagen.

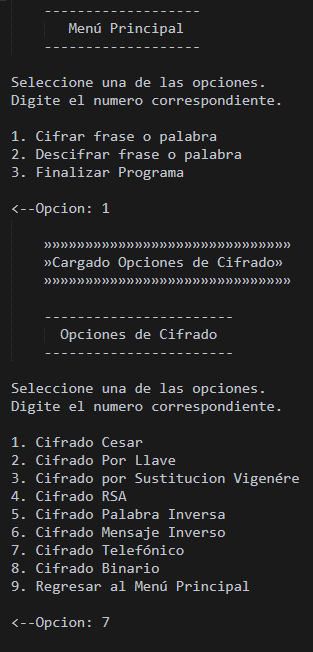
Si la entrada del usuario no es correcta, o incluye algún valor no válido para el algoritmo de descifrado de Mensaje Inverso, el programa le retornará un mensaje indicando la razón por la cual no es válido es valor ingresado. En primera instancia, si no ingresa ningún valor para la frase a descifrar le retornara el siguiente mensaje.

En caso de que haya ingresado un caracter no valido o se realice una combinación de caracteres válidos y no permitidos en su entrada, se mostrará el siguiente mensaje.

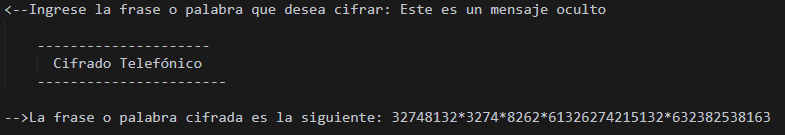
Para todos los casos mencionados sobre las posibles entradas de este algoritmo, erradas o válidas, luego de desplegar los mensajes correspondientes, se retornará al Menú de Opciones de Descifrado.



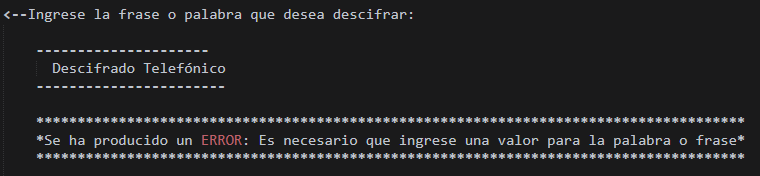
### Opción Descifrado Telefónico

Para ingresar a esta opción es necesario seleccionar la opción 1 en el Menú Principal, y la opción 7 en el Menú de Opciones de Descifrado.

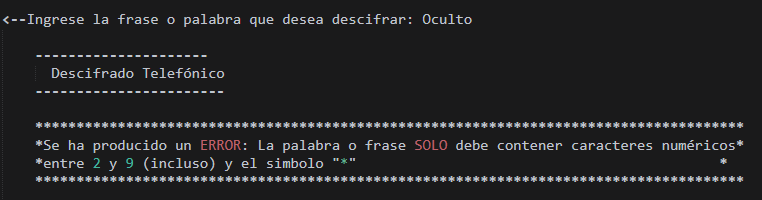
Luego de seleccionar ambas opciones el programa deberá desplegar el espacio para que el usuario ingrese la frase que desea convertir a partir del cifrado de Cifrado Telefónico. Para los valores aceptados para la frase dentro de este algoritmo, se tiene que son permitidos cualquiera de las letras que se muestran en la figura del teclado telefónico y los espacios en blanco.

En caso de que la entrada del usuario sea la correcta, se mostrará el título de la sección, seguido del resultado de realizar la conversión mediante el algoritmo seleccionado y en la siguiente línea se incluyen los valores de ambas claves generadas por el algoritmo. Este proceso puede observarse en la siguiente imagen.

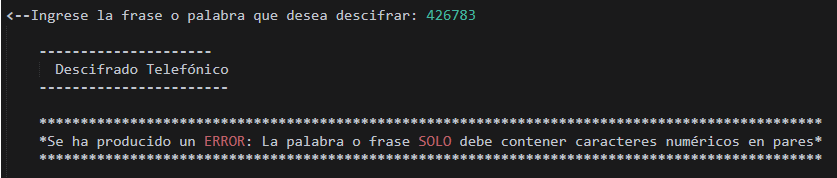
Si la entrada del usuario no es correcta, o incluye algún valor no válido para el algoritmo de cifrado de Cifrado Telefónico, el programa le retornará un mensaje indicando la razón por la cual no es válido es valor ingresado. En primera instancia, si no ingresa ningún valor para la frase a cifrar le retornara el siguiente mensaje.



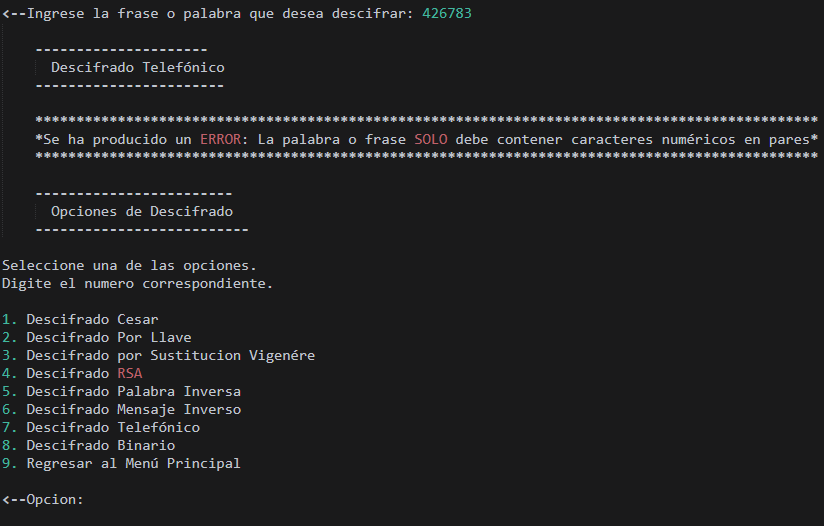
En caso de que haya ingresado un caracter no valido o se realice una combinación de caracteres válidos y no permitidos en su entrada, se mostrará el siguiente mensaje.



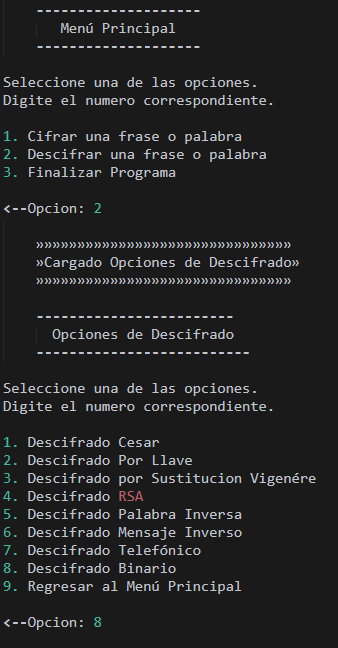
Para el caso del descifrado telefónico, es necesario además que las palabras cifradas dentro de la frase ingresada estén conformadas por grupos de pares de números de acuerdo a las posibles entradas que habilita a asignación de las letras de acuerdo a su ubicación en los números del teclado telefónico. Por ejemplo, para pares de números que inicien con 2, 3, 4, 5, 6 y 8 su segundo valor solo podrá sea 1, 2, o 3, para los pares que inicien con 7 y 9, su segundo valor podrá ser 1, 2, 3, para los que inicien con 1 o contengan como alguno de sus valores a un cero, no serán pares de números válidos. Como ejemplo de un posible caso erróneo que valide esta restricción se muestra la siguiente imagen.



Para todos los casos mencionados sobre las posibles entradas de este algoritmo, erradas o válidas, luego de desplegar los mensajes correspondientes, se retornará al Menú de Opciones de Descifrado.

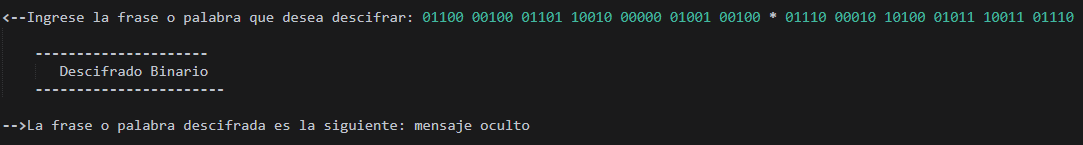


### Opción Descifrado Binario

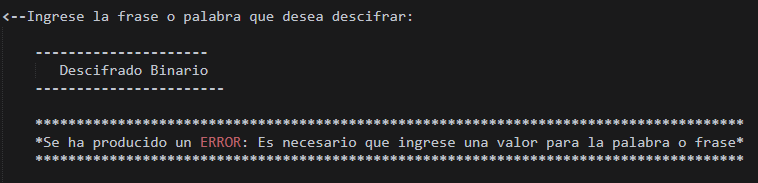
Para ingresar a esta opción es necesario seleccionar la opción 1 en el Menú Principal, y la opción 8 en el Menú de Opciones de Descifrado.

Luego de seleccionar ambas opciones el programa deberá desplegar el espacio para que el usuario ingrese la frase que desea convertir a partir del descifrado Binario. Para los valores aceptados para la frase dentro de este algoritmo, se tiene que se tiene que son permitidos son solamente el número 1 el 0 y los espacios en blanco.

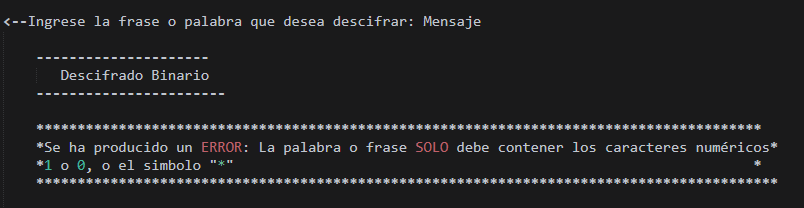
En caso de que la entrada del usuario sea la correcta, se mostrará el título de la sección, seguido del resultado de realizar la conversión mediante el algoritmo seleccionado. Este proceso puede observarse en la siguiente imagen.



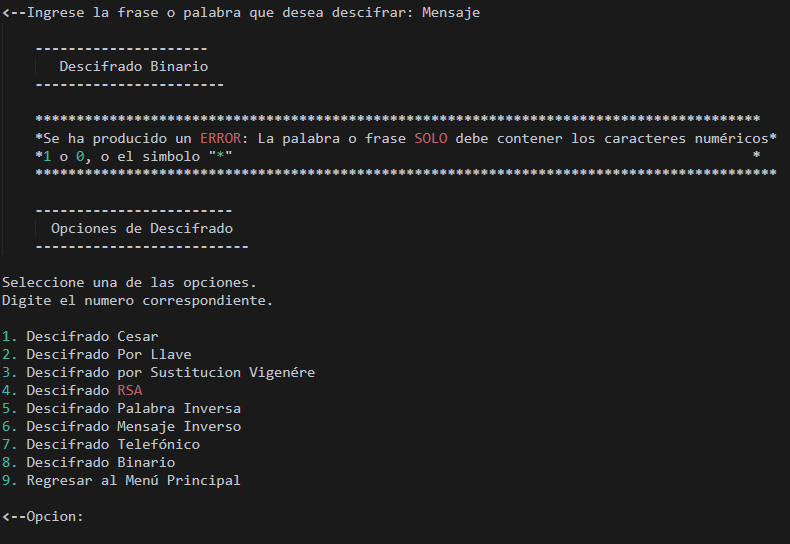
Si la entrada del usuario no es correcta, o incluye algún valor no válido para el algoritmo de descifrado Binario, el programa le retornará un mensaje indicando la razón por la cual no es válido es valor ingresado. En primera instancia, si no ingresa ningún valor para la frase a descifrar le retornara el siguiente mensaje.



En caso de que haya ingresado un caracter no valido o se realice una combinación de caracteres válidos y no permitidos en su entrada, se mostrará el siguiente mensaje.



Para todos los casos mencionados sobre las posibles entradas de este algoritmo, erradas o válidas, luego de desplegar los mensajes correspondientes, se retornará al Menú de Opciones de Descifrado.



# 

# Lecciones Aprendidas

**Josué Brenes Alfaro:**

Durante este proyecto, en lo que a mí respecta, he tenido un aprendizaje hacia la programación muy basto. Gracias a mi compañero Jose Manuel Altamirano, aparte de que es una gran persona, su habilidad de programación es muy grande, y gracias a ello he logrado aprender muchas cosas en la programación. Por ejemplo, en el desarrollo de la lógica en cada reto, tener un planteamiento del problema y resolverlo de la manera más limpia. También algo que se aprende al trabajar en parejas, es que se tiene que ser responsable con las reuniones, aportes y decisiones que se toman reto a reto.

Uno de los aprendizajes descubiertos en la programación es que, si queremos separar palabras basta con agregar un espacio al final de la cadena y así validar cuando hay un espacio saber que hasta ese punto llega la palabra. Otro aprendizaje con el import random para determinar números random para el cifrado RSA.

Obtuve el conocimiento de las herramientas para utilizar Python en Grupos de trabajo. Optamos por usar GitHub, en el cual se fueron guardando los avances de la programación, hay que tener cuidado a la hora de usar el programa ya que hay que refrescar la última actualización del código para no generar problemas. Se tuvieron algunas dificultades, sin embargo, nos quedó de experiencia y el final se pudo utilizar excelentemente para este proyecto.

Una felicitación a los profesores por la idea de este proyecto, ya que a pesar de la presión y trabajo arduo acerca a los estudiantes un poco a tener una idea de cómo es trabajar en equipo y también un agradecimiento a mi compañero por proveerme tanto conocimiento durante la ejecución del proyecto.

**José Manuel Altamirano**

Al finalizar este proyecto, han sido muchos los aprendizajes que se obtuvieron. En lo respecta a la codificación de los retos, las lecciones son principalmente en relación con el conocimiento adquirido sobre el lenguaje Python y el manejo de sus distintas funciones y algunas librerías. Para completar este proyecto se han empleado técnicas y estructuras variadas, combinando muchos de los conceptos aprendidos durante las lecciones.

En cuanto al manejo de las versiones del programa, al optar por el uso GitHub para guardar el desarrollo del proyecto, se ha facilitado mucho el control sobre progreso del código. A pesar de que en una ocasión se tuvieron algunos problemas para mantener y combinar los cambios realizados, el solucionar este problema nos permitió aprender más sobre el uso de esta herramienta, y las consideraciones que hay que tener al momento de codificar sobre un mismo proyecto.

La importancia del trabajo en equipo también ha sido un aprendizaje importante en este proyecto. El apoyo de mi compañero ha sido fundamental para poder dar solución a los retos planteados por el proyecto. Cuando en alguna ocasión no pudiéramos avanzar en alguna de las asignaciones que tuviéramos, sabíamos que podíamos recurrir a la ayuda del compañero para poder cumplir con los tiempos propuestos dentro del cronograma.

El uso de herramientas como el diagrama de Gantt para la elaboración del cronograma, ha facilitado mucho el control sobre el progreso de las tareas y el tiempo disponible para completar cada una. El incluir una columna con el porcentaje completado para cada asignación nos permitió ver en tiempo real el estado de una actividad y estimar el esfuerzo necesario para completarla.

Finalmente, el uso de la bitácora como apoyo documental del proyecto, nos permitió reflexionar sobre las labores realizadas y revisadas en cada reunión durante del desarrollo. La actualización periódica de este medio habilitó un espacio para reflejar de una forma breve la concordancia de las actividades realizadas con el tiempo asignado dentro del cronograma.

# Bitácora de Trabajo

En esta sección se incluyen los accesos a las bitácoras de trabajo de los integrantes del grupo. Para cada una se indica el nombre de quien la desarrolla y el enlace por el cual puede accederse a las publicaciones realizadas.

Josué Brenes Alfaro

Bitácora: <https://bitacoraproyecto2020054427.blogspot.com/>

José Manuel Altamirano Salazar

Bitácora: <https://2020426159.blogspot.com/>

# Análisis de Resultados

## Objetivos Alcanzados

* Desarrollar en forma completa los algoritmos de cifrado propuestos en el enunciado del proyecto.
* Desarrollar en forma completa los algoritmos de descifrado propuestos en el enunciado del proyecto.
* Complementar al acceso a las diferentes opciones por medio de un menú con un entorno amigable con el usuario.
* Incluir las validaciones necesarias para evitar que se den errores dentro de los procesos de cifrado y descifrado, así como informar al usuario sobre las necesidades de las entradas para cada algoritmo.
* Obtención de varios conocimientos sobre las diferentes formas de integrar el código desarrollado desde equipos y en condiciones distintas.
* Adquirir nuevos aprendizajes sobre el uso del lenguaje Python y las posibles técnicas para estructurar sus funciones para la resolución de los retos que se propongan.
* Explicar las funcionalidades del programa a través de un Manual para su uso y de la exposición de sus diferentes funcionalidades dentro de la documentación del proyecto.

## Objetivos No Alcanzados

Consideramos que todos los objetivos propuestos al inicio del proyecto fueron logrados y que no se ha dejado por fuera ninguna funcionalidad del programa.

# Distribución del Trabajo

|  |  |  |
| --- | --- | --- |
| **NUM. DE TAREA** | **NOMBRE DE LA TAREA O ACTIVIDAD** | **PERSONA ASIGNADA** |
|
| 1 | Actividades Generales |  |
| 1.1 | Registro del Equipo de Trabajo | Jose A y Josué B |
| 1.2 | Lectura y discusión del proyecto | Jose A y Josué B |
| 1.3 | Creación del Blog | Jose A y Josué B |
| 2 | Actividades de Desarrollo de Código |  |
| 2.1 | Algoritmos para Codificar/Cifrar |  |
| 2.1.1 | Cifrado César | Josué B |
| 2.1.2 | Cifrado por Llave | Jose A |
| 2.1.3 | Cifrado por Sustitución Vigenére | Josué B |
| 2..1.4 | Cifras RSA | Jose A |
| 2.1.4 | Cifrado Palabra Inversa | Josué B |
| 2.1.5 | Cifrado Mensaje Inverso | Jose A |
| 2.1.6 | Cifrado Telefónico | Josué B |
| 2..1.5 | Cifrado Binario | Jose A |
| 2.2 | Algoritmos para Codificar/Cifrar |  |
| 2.1.1 | Descifrado César | Jose A |
| 2.1.2 | Descifrado por Llave | Josué B |
| 2.1.3 | Descifrado por Sustitución Vigenére | Jose A |
| 2..1.4 | Descifrado RSA | Josué B |
| 2.1.4 | Descifrado Palabra Inversa | Jose A |
| 2.1.5 | Descifrado Mensaje Inverso | Josué B |
| 2.1.6 | Descifrado Telefónico | Jose A |
| 2..1.5 | Descifrado Binario | Josué B |
| 2.2 | Menús de Navegación |  |
| 2.1.6 | Menú Principal | Jose A y Josué B |
| 2.1.6 | Menú Opciones Cifrado | Jose A |
| 2..1.5 | Menú Opciones Descifrado | Josué B |
| 3 | Actividades de Documentación |  |
| 3.1 | Documentación Interna del Código |  |
| 3.1.1 | Determinar E-S-R para cada función | Jose A y Josué B |
| 3.1.2 | Verificar identificadores de funciones y variables | Jose A y Josué B |
| 3.2 | Documentación Externa/Informe Escrito |  |
| 3.2.1 | Cronograma de Trabajo | Jose A y Josué B |
| 3.2.2 | Estrategia Metodológica | Jose A y Josué B |
| 3.2.3 | Tabla de Distribución de Tareas | Jose A y Josué B |
| 3.2.4 | Manual de Usuario | Jose A y Josué B |
| 3.2.5 | Pruebas de Funcionalidad | Jose A y Josué B |
| 3.2.6 | Análisis de Resultados | Jose A y Josué B |
| 3.2.7 | Portada, Índice e Introducción | Jose A y Josué B |
| 3.2.8 | Lecciones Aprendidas | Jose A y Josué B |
| 3.2.9 | Archivo txt | Jose A y Josué B |
| 3.2.10 | Bitácora/Diario de Trabajo | Jose A y Josué B |