Tarea Programada #1

Criptografía y tipos de criptografía

Manual de Usuario

Samuel Garcés Castillo – 2022129139

Carlos Daniel Guzmán Ramírez – 2022437782

Samuel Garcés – 2022129139
Carlos Guzmán – 2022437782

Contenido

Samuel Garcés – 2022129139
Carlos Guzmán – 2022437782

1. Introducción

1.1. Objetivo

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

1.2. Requerimientos mínimos

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

Samuel Garcés – 2022129139
Carlos Guzmán – 2022437782

2. Navegación del sistema

2.1. Menú principal

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

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

2.2. Menú secundario

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

Samuel Garcés – 2022129139
Carlos Guzmán – 2022437782

Interfaz básica:

```
Seleccione una opción: 1

_____________________________
¿Que acción desea realizar? - Cifrado César
1- Codificar     2- Decodificar     0- Regresar al menú
>>>
```

Caso 1:

```
_____________________________
¿Que acción desea realizar? - Cifrado César
1- Codificar     2- Decodificar     0- Regresar al menú
>>> 1


_____________________________________________________________
Cifrado César - (codificar)

Por favor, ingrese la frase que desea codificar:
```

Caso 2:

```
_____________________________
¿Que acción desea realizar? - Cifrado César
1- Codificar     2- Decodificar     0- Regresar al menú
>>> 2


_____________________________________________________________
Cifrado César - (decodificar)

Por favor, ingrese la frase que desea decodificar:
```

Caso 3:

```
_____________________________
¿Que acción desea realizar? - Cifrado César
1- Codificar     2- Decodificar     0- Regresar al menú
>>> 0

*************************
*      Criptografía     *
*************************
1. Cifrado César
2. Cifrado por llave
3. Sustitución Vigenére
4. Sustitución XOR y llave
5. Palabra inversa
6. Mensaje inverso
7. Cifrado telefónico
8. Cifrado binario
0. Terminar
Seleccione una opción:
```

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

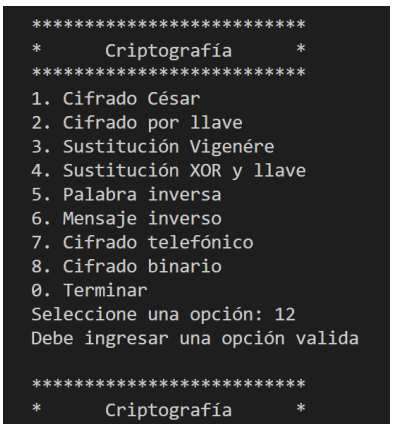
Samuel Garcés – 2022129139
Carlos Guzmán – 2022437782

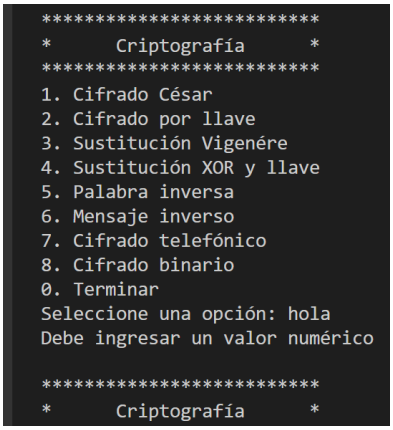
2.3. Validaciones

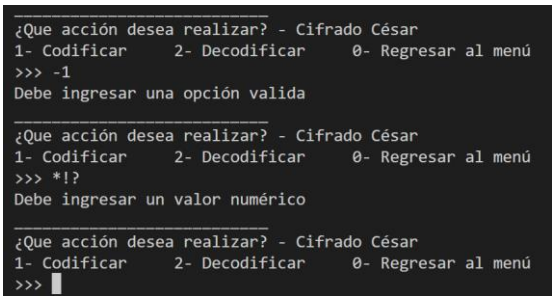
Para asegurar la robustez del sistema, se trabajó con una serie de validaciones principales que fueron aplicadas recursivamente a lo largo del código. Gracias a ello, se permitió contrarrestar numerosos tipos de errores, asegurando así la integridad de la aplicación. De la misma manera, estas repetirán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

a) Validación del menú:

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

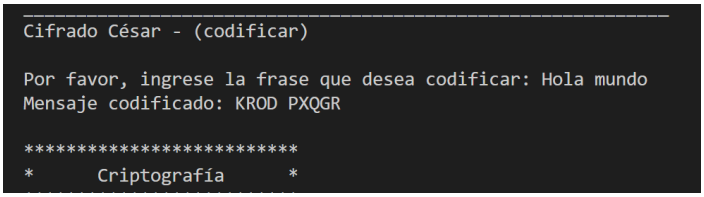


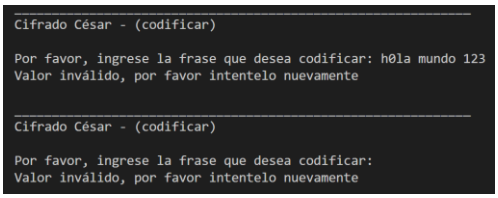




b) Validación de frases:

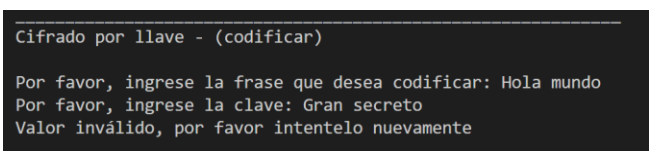
Asegura el ingreso correcto de frases largas al sistema, únicamente con valores alfabéticos y espacios en blanco. Este tipo de validación se utiliza en la gran mayoría de ingresos de frases a codificar o decodificar

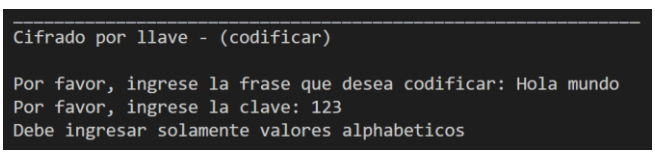




c) Validación de palabras:

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

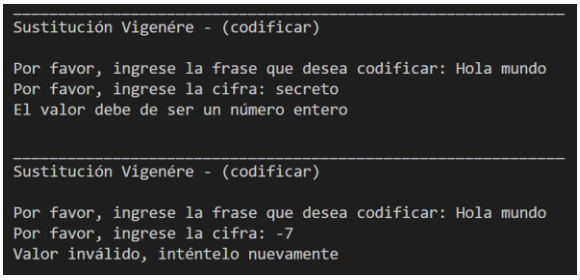


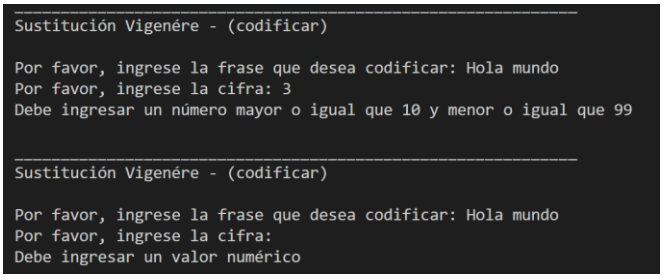


Samuel Garcés – 2022129139
Carlos Guzmán – 2022437782

d) Validación numérica:

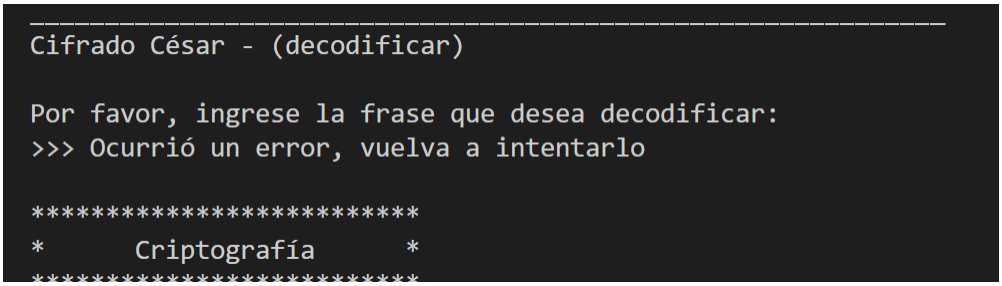
Permite validar el ingreso de datos numéricos dentro de un rengo determinado. Esta validación se utiliza al trabajar con datos numéricos, como en el caso de la “Codificación Vigenére”.





e) Validación de error desconocido:

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



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

Samuel Garcés – 2022129139
Carlos Guzmán – 2022437782

3. Opciones del sistema

3.1. Cifrado César

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

```
Cifrado César - (codificar)
Por favor, ingrese la frase que desea codificar: tarea programada
Mensaje codificado: WDUHD SURJUDPDGD
```

```
Cifrado César - (decodificar)

Por favor, ingrese la frase que desea decodificar: WDUHD SURJUDPDGD
Mensaje decodificado: tarea programada
```

3.2. Cifrado por llave

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

```
Cifrado por llave - (codificar)

Por favor, ingrese la frase que desea codificar: tarea programada de codificacion
Por favor, ingrese la clave: tango
Mensaje codificado: nbflp jscngunokp xf qvscgwjpwjcu
```

```
Cifrado por llave - (decodificar)

Por favor, ingrese la frase que desea decodificar: nbflp jscngunokp xf qvscgwjpwjcu
Por favor, ingrese la clave: tango
Mensaje decodificado: tarea programada de codificacion
```

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

```
Cifrado por llave - (decodificar)

Por favor, ingrese la frase que desea decodificar: nbflp jscngunokp xf qvscgwjpwjcu
Por favor, ingrese la clave: secreto
Mensaje decodificado: uwctk pdjidciuvw sc yqynnrgxrpnb
```

Samuel Garcés – 2022129139
Carlos Guzmán – 2022437782

3.3. Sustitución Vigenére

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

```
____________________________________________________________
Sustitución Vigenére - (codificar)

Por favor, ingrese la frase que desea codificar: tarea programada
Por favor, ingrese la cifra: 23
Mensaje codificado: vdthc striucpcgc
```

```
____________________________________________________________
Sustitución Vigenére - (decodificar)

Por favor, ingrese la frase que desea decodificar: vdthc striucpcgc
Por favor, ingrese la cifra: 23
Mensaje codificado: tarea programada
```

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

3.4. Sustitución XOR y llave

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

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

```
____________________________________________________________
Sustitución XOR y llave - (codificar)
Por favor, ingrese la frase que desea codificar: tarea programada
Por favor, ingrese la clave: secreto
Mensaje codificado: '\x07\x04\x11\x17\x04T\x1f\x01\n\x04\x00\x04\x19\x0e\x17\x04'
```

```
¿Desea decodificar este mensaje?
1 -Sí    2 -No
>>> 1


____________________________________________________________
Sustitución XOR y llave - (decodificar)

Datos a trabajar: ['\x07', '\x04', '\x11', '\x17', '\x04', 'T', '\x1f', '\x01', '\n', '\x04', '\x00', '\x04', '\x19', '\x0e', '\x17', '\x04']
Clave asignada: secreto
Mensaje decodificado: tarea programada
```

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

Samuel Garcés – 2022129139
Carlos Guzmán – 2022437782

3.5. Palabra inversa

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

```
_____________________________________________________
Palabra inversa - (codificar)

Por favor, ingrese la frase que desea codificar: tarea programada
Mensaje codificado: aerat adamargorp
```

```
_____________________________________________________
Palabra inversa - (decodificar)

Por favor, ingrese la frase que desea decodificar: aerat adamargorp
Mensaje decodificado: tarea programada
```

3.6. Mensaje inverso

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

```
_____________________________________________________
Mensaje inverso - (codificar)

Por favor, ingrese la frase que desea codificar: tarea programada
Mensaje codificado: adamargorp aerat
```

```
_____________________________________________________
Mensaje inverso - (decodificar)

Por favor, ingrese la frase que desea decodificar: adamargorp aerat
Mensaje decodificado: tarea programada
```

3.7. Cifrado telefónico

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

```
_____________________________________________________
Cifrado por código telefónico - (codificar)

Por favor, ingrese la frase que desea codificar: tarea programada
Mensaje codificado: 81 21 73 32 21 * 71 73 63 41 73 21 61 21 31 21
```

```
_____________________________________________________
Cifrado por código telefónico - (decodificar)

Por favor, ingrese la frase que desea decodificar: 81 21 73 32 21 * 71 73 63 41 73 21 61 21 31 21
Mensaje decodificado: tarea programada
```

Samuel Garcés – 2022129139
Carlos Guzmán – 2022437782

3.8. Cifrado binario

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

```
------------------------------------------------------------
Cifrado binario - (codificar)
Por favor, ingrese la frase que desea codificar: tarea programada
Mensaje codificado: 10011 00000 10001 00100 00000 * 01111 10001 01110 00110 10001 00000 01100 00000 00011 00000
```

```
------------------------------------------------------------
Cifrado binario - (decodificar)
Por favor, ingrese la frase que desea decodificar: 00010 10001 01000 01111 10011 01110 00110 10001 00000 00101 01000 00000 * 00011 00000 10011 01110 10010
Mensaje decodificado: criptografia datos
```

3.9. Terminar

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

```
**************************
*      Criptografía      *
**************************
1. Cifrado César
2. Cifrado por llave
3. Sustitución Vigenére
4. Sustitución XOR y llave
5. Palabra inversa
6. Mensaje inverso
7. Cifrado telefónico
8. Cifrado binario
0. Terminar
Seleccione una opción: 0

---Ejecución finalizada---
```