“Cifrado Clásico”

Informe N°11

Laboratorio de Seguridad en Redes

Melanny Dávila
Ingeniería en Telecomunicaciones
Facultad de Eléctrica y Eléctronica
Quito, Ecuador
melanny.davila@epn.edu.ec

Alejandra Silva
Ingeniería en Telecomunicaciones
Facultad de Eléctrica y Eléctronica
Quito, Ecuador
alejandra.silva@epn.edu.ec

***Abstract*—En el siguiente documento se presentan pequeñas implementaciones acerca de cifrado y descifrado clásico, con el fin de comprender el funcionamiento de los diferentes algoritmos y analizar cuán seguros lo son.**

***Index Terms*—Algoritmo, cifrado, descifrado, desplazamiento.**

I. Introducción

Entre los diferente tipos de algoritmos de cifrado, se tiene uno que es el mas básico y sencillo que es por sustitución, se basa en que las unidades de texto son sustituidas con texto cifrado, existen dos alfabetos en esta sustitución monoalfabético que usa una sustitución fija y polialfabético que usa diferentes sustituciones en diferentes mecanismo del mensaje.

Existen otro dos tipos de cifrado,el primero es cifrado Vigenére es un criptosistema simétrico, es decir, utiliza la misma clave para cifrar y descifrar. Se trata de un algoritmo de cifrado simétrico polialfabético, es decir, es basado en diferentes series de caractéres o letras del cifrado Cesar formando estos caracteres una tabla y finalmente el cifrado Hill este sistema es polialfabético pues puede darse que un mismo carácter en un mensaje a enviar se encripte en dos caracteres distintos en el mensaje encriptado.

II. Objetivos

- Probar varios algoritmos de cifrado clásico.
- Implementar un algoritmo sencillo de cifrado clásico.

III. Cuestionario

A. Presente la configuración realizada en el laboratorio.

1) CIFRADO:

- **César**
  El primer paso se debe seleccionar la opción llamada “Desplazamiento Puro”, posterior a eso se debe escoger el diccionario que se va a utilizar como indica en la siguiente figura en este caso el diccionario utilizado será “EspañolZ27”.

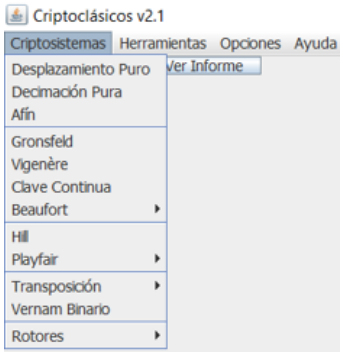

Fig. 1. Opción de criptosistema

Fig. 2. Diccionario

A continuación, se despliega una pantalla en la que se debe ingresar la entrada a cifrar y se mostrará resultado final de igual manera; donde previamente se debe seleccionar el desplazamiento con el que se desea trabajar.

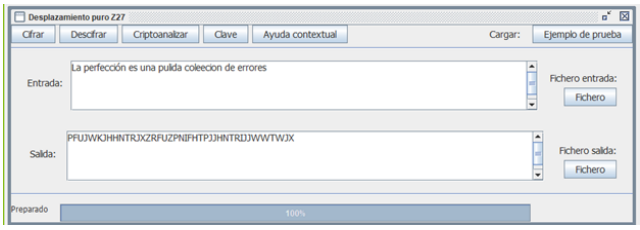

Fig. 3. Texto a cifrar

La aplicación presenta la oportunidad de crear un informe en el cual se detalla como es el proceso de cifrado.

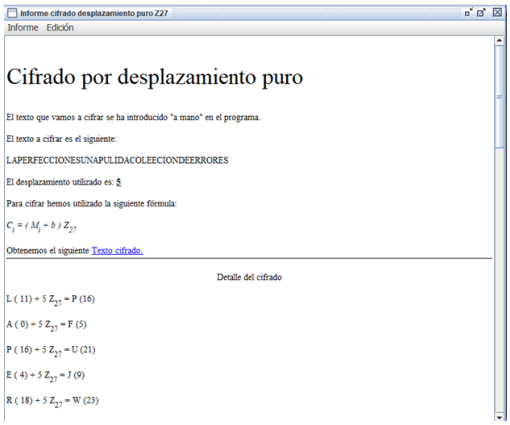

Fig. 4. Informe obtenido con el algoritmo César

Aquí se puede evidenciar que esto se hace por un reemplazo que lo que hace es desplazar cierto número de letras, por ejemplo si se tiene la A y desplazo 3, dicha letra cambia a D como se evidencia en la figura presentada anteriormente.

- **Vigenére**
  De la misma manera, se debe seleccionar en la opción de criptosistemas y escoger Vigenére como se indica en la figura 1, de forma similar se puede escoger el diccionario con el que se trabajará. Una vez que se realizó dichas selecciones, se despliega una pestaña para introducir la frase a cifrar como se indica a continuación

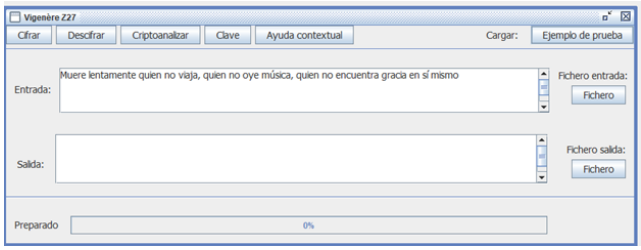

Fig. 5. Ingreso de la frase

En este caso, se debe ingresar la clave con la que se va cifrar.

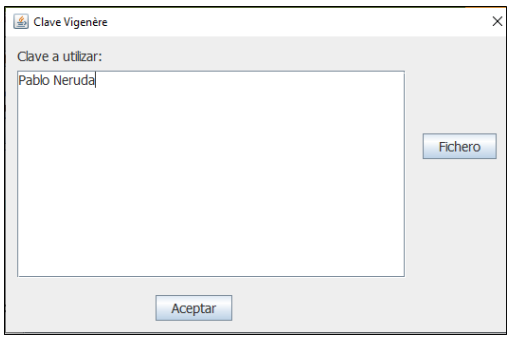

Fig. 6. Ingreso de la clave

Finalmente se obtiene el informe que detalla como es el proceso de cifrado.

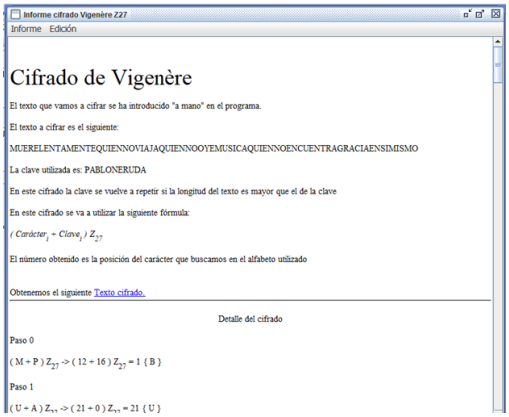

Fig. 7. Informe cifrado con Vigenére

La explicación es sencilla ya que se basa en el desplazamiento pero lo hace en función de la posición de las palabras de la clave.

- **Hill**
  Se debe seleccionar la opción de criptosistemas y escoger Hill como se indica a continuación:

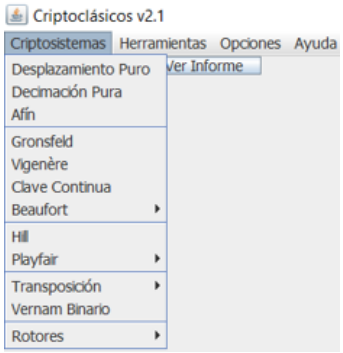

Fig. 8. Opción de criptosistema-Hill

Se debe seleccionar el alfabeto con el cual se trabajará y luego de eso se escoge la dimensión de la matriz verificando que tenga inverso.

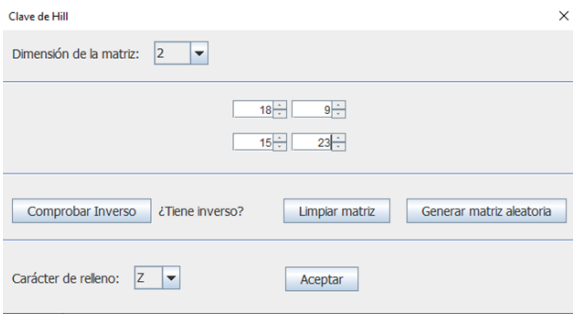

Fig. 9. Generación de Hill

Se ingresará el texto que se desea cifrar y posterior a eso se otendrá el informe que detalla dicho proceso.

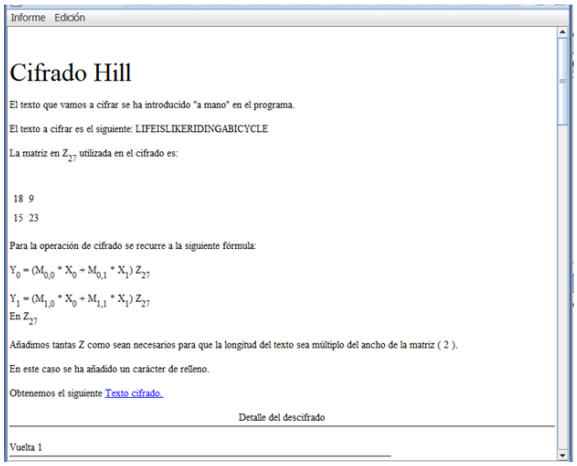

Fig. 10. Informe cifrado con algoritmo Hill

El que consiste en el producto punto entre la matriz y el valor de los caractéres para sacar el nuevo valor y ahí efectúa el remplazo; en este caso de 2 en 2 para que tenga sentido.

2) DESCIFRADO:

- **César**
  De la misma manera, se selccionará la opción de criptosistema y el diccionario, como se lo presenta en las figuras 1 y 2. Posterior a eso se ingresa el texto que se va a descifrar y la longitud del desplazamiento. De manera similar se puede observar el informe cuya extensión es html.

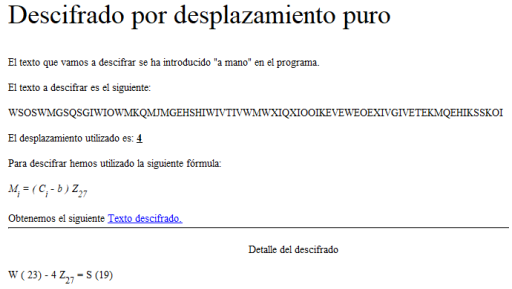

Fig. 11. Informe del descifrado con el algoritmo César

- **Vigenére**
  Para este caso, se debe ingresar la clave con la cual se descifrará el texto previo a que ya se realizó la selección del algoritmo con el que se trabajará y el diccionario. Una vez que se realizó esto, se obtuvo el informe del proceso de descifrado.

Fig. 12. Informe del descifrado con el algoritmo Vigenére

- **Hill**
  En este caso de igual manera se selección el diccionario y el algoritmo con el que se trabajará, es importante mencionar que se ingresó la clave que era una matriz 2x2 que no tiene transpuesta, que, sin embargo, permitió cifrar el texto.

Fig. 13. Informe del descifrado con el algoritmo Hill

3) CRIPTOANÁLISIS: El primer paso es seleccionar el criptosistema que en este caso es Vigenére y se desplegara la siguiente pantalla.

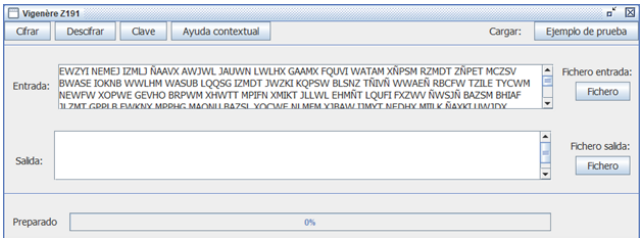

Fig. 14. Entrada de frase

En la entrada se debe colocar el texto citado en la hoja guía de la sesión de laboratorio y se debe seleccionar el botón criptoanalizar y se despliega la siguiente pantalla:

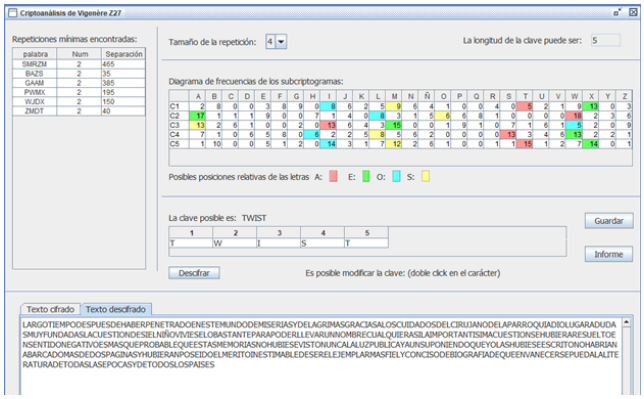

Fig. 15. Pantalla de criptoanálisis

Aquí se puede evidenciar que se tiene que encontrar el número de repeticiones al cual se debe sacar el máximo común divisor en este caso sería 5 y este va a ser la longitud de la clave que se necesita. Entonces una vez obtenido este dato y una vez descubierta la longitud de la clave con la que se cifró el texto tan sólo hay que dividir el texto en bloques del mismo tamaño que la longitud de la clave y aplicar el método estadístico tradicional del cifrado César.

Así se obtiene tanto la clave que en este caso siguiendo el patrón es *TWIST*.

4) CRIPTOANÁLISIS con texto incompleto: El primer paso es cambiar el alfabeto a 191 y se despliega una pantalla como se indica a continuación

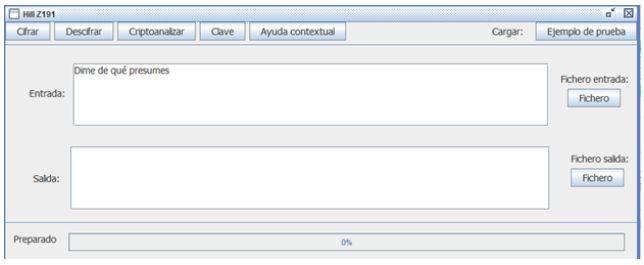

Fig. 16. Entrada de frase

Al igual que el anterior criptoanálisis se selecciona la opción criptoanálisis y se despliega las siguiente pantalla

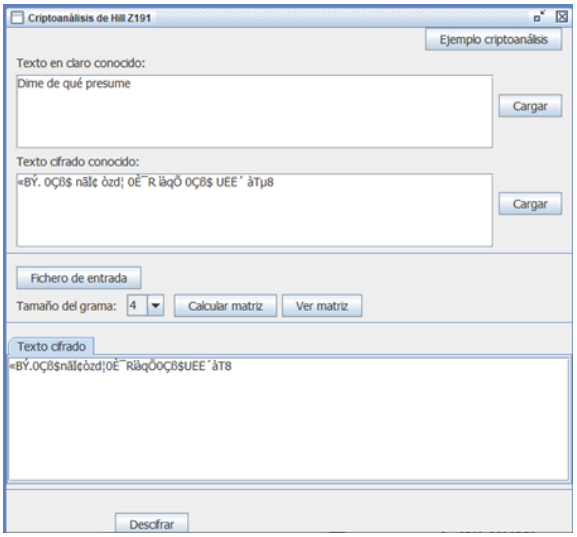

Fig. 17. Pantalla de criptoanálisis

En la que se debe volver a colocar el texto en claro y el texto cifrado conocido, finalmente se selecciona la opción de calcular matriz y decifrar y se obtiene el resultado final. Apartir de esto se puede obtener un informe que indica lo que hace este criptoanálisis.

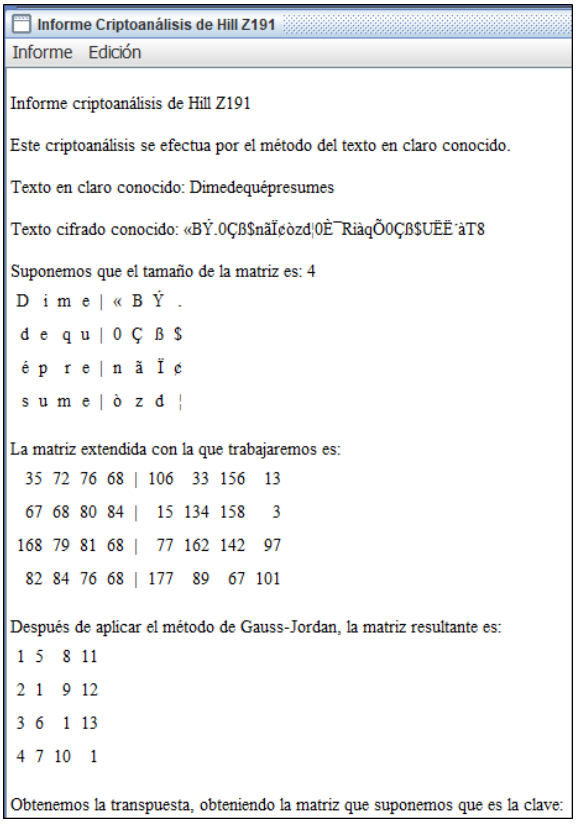

Fig. 18. Pantalla de criptoanálisis

Este criptoanálisis utiliza matriz de Gauss Jordan usando una matriz cuadrada (K) de orden 3 (tres filas y tres columnas).

Por tanto, sustituyendo cada una de las letras, tanto del texto en claro como del criptograma, por la posición que ocupa cada una de ellas en el alfabeto español.

B. Explique los resultados obtenidos durante la práctica.

A continuación, se presentan los resultados obtenidos durante la sesión de laboratorio, la misma que se dividió en dos partes:

1) **CIFRADO**
Donde M es la frase que se cifrará y C es la frase resultante después del cifrado.
   - César
     - M: La perfección es una pulida colección de errores
     - C: PFUJWKJHHNTRJXZRFUZPNIFHTPJHHNTRIJJWWTWJX
   - Vigenére
     - M: Muere lentamente quien no viaja, quien no oye música, quien no encuentra gracia en sí mismo
     - C: BUFCSXIEÑDMTNUOFHMVHPOLIBTODYZYPNEOZOAHWZWDQKIFXBBIEWXECTSLUEETCDECSJWWFPG
   - Hill
     - M: Life is like riding a bicycle
     - C: AYRFRQAYAZRVRNRJJWAEJPRÑ
2) **DESCIFRADO**
En este caso, se presenta A que corresponde al texto cifrado y M al texto descifrado
   - César
     - A:WSOSWMGSQSGIWIOWMKQMJMGEHSHIWIVTIVWMWXIQXIOOIKEVEWEOEXIVGIVETEKMQEHIKSSKOI
     - Desplazamiento: 4
     - M:SOLOSICONOCESELSIGNIFICADODESERPERSISTENTELLEGARASALATERCERAPAGINADEGOOGLE
     - Con espacios: SOLO SI CONOCES EL SIGNIFICADO DE SER PERSISTENTE LLEGARAS A LA TERCERA PAGINA DE GOOGLE
   - Vigenére
     - A:ʼÉëÉ¥ÚÖÖ×âÀÅæÔ¡àÙÉÝÜã¾ÍÙÌ®âÔÇÌÒÙ¿ÃíÂ²ÖØFÚã±ØìÒ¡ÜØÈÔÜÕ¾ÉçÑÒÖÙÒÙ¿Ìä0Å§ÎØÅÓæ
     - Clave: Maya Angelou
     - M:Sisiempreintentassernormalnuncadescubriráslo-extraordinarioquepuedesllegaraser
     - Con espacios: Si siempre intentas ser normal nunca descubrirás lo extraordinario que puedes llegar a ser
   - Hill
     - A: QNQ WHO RES RAU QXB IBV ÑDV GYS ÑNZ JEB LFJ IKJ
     - Clave digrámica: Life is like riding a bicycle
     - M:NODEJESPARAMAÑANALOQUEPUEDASHACERHOY
     - Con espacios: NO DEJES PARA MAÑANA LO QUE PUEDAS HACER HOY
3) **VIGENÉRE Y HILL**
Lo primero que se realizó fue encontrar la posible clave:

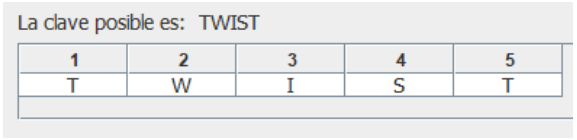

Fig. 19. Clave encontrada

Ahora, el texto descifrado es el siguiente:

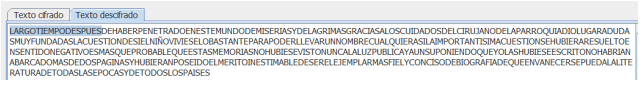

Fig. 20. Texto Decifrado

Donde las tres primeras palabras son: *LARGO TIEMPO DESPUES* de acuerdo a la figura anterior.

4) **Hill mod 191**
Al realizar el criptoanálisis del criptograma C si se sabe que se ha cifrado con Hill mod 191 en bloques de 4 letras y que el texto en claro comienza por:

- La clave en este caso seria la matriz de 4 bloques que se genero, que se indica a continuación

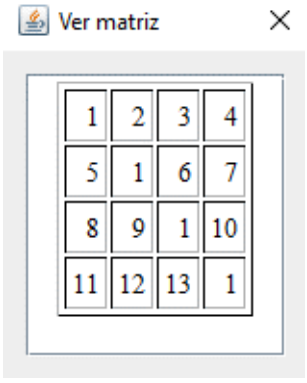

Fig. 21. Matriz.

Permitiendo así obtener como resultado el texto en claro completo es el siguiente: *Dime de qué presumes y te diré de qué caràT8*

C. Implementar el algoritmo César (cifrado y descifrado), utilizando el lenguaje de programación de su preferencia, siguiendo las siguientes directrices:

- Debe permitir seleccionar la magnitud del desplazamiento;

- Al cifrar, asuma que el texto claro solamente tiene letras del alfabeto y espacios, no cifre los espacios.
- Muestre 2 ejemplos de funcionamiento del algoritmo implementado tanto del cifrado como del descifrado.

```
def cifrado_seguridades(text,desp):
    cipher = ""
    for i in range(len(text)): #Para cada letra del texto
        char = text[i]
        if (char.islower()):
            cipher += chr((ord(char) + desp - 97) % 26 + 97) #97 letra minuscula (a)
        elif char==" ":
            cipher += " "
        else:
            cipher += chr((ord(char) + desp-65) % 26 + 65) # Prima letra mayuscula (A)
    return cipher
def descifrado_seguridades(text,desp):
    plain = ""
    for i in range(len(text)):
        char = text[i]
        if (char.islower()):
            plain += chr((ord(char) -97-desp) % 26 + 97)
        elif char == " ":
            plain += " "
        else:
            plain += chr((ord(char) -65-desp) % 26 + 65)
    return plain
#Importante: Este codigo no considera la "n" debido la funcion de python usada para obtener el codigo ascii de la letra
if __name__ == '__main__': #inicio funcion principal
    opcion = input("Seleccione el numero de la opcion que desea realizar:\n 1. Cifrar\n 2. Descifrar\n")
    if opcion == "1":
        texto = input("Ingrese el texto a cifrar: ")  # Ingreso el texto que quiero cifrar
        desplazamiento = int(input("Ingrese el desplazamiento: "))  # Ingreso el desplazamiento para realizar el cifrado
        print("El resultado es:\n")
        print(cifrado_seguridades(texto,desplazamiento))
    elif opcion == "2":
        texto = input("Ingrese el texto a descifrar: ")  # Ingreso el texto que quiero descifrar
        desplazamiento = int(input("Ingrese el desplazamiento: "))  # Ingreso el desplazamiento para realizar el cifrado
        print("El resultado es:\n")
        print(descifrado_seguridades(texto,desplazamiento))
    else:
        print("Opcion erronea")
```

A continuación, se presentan los resultados que fueron obtenidos en base al código desarrollado en el lenguaje de programación Python.

- Cifrado
  - Ejemplo 1

```
Seleccione el numero de la opcion que desea realizar:
 1. Cifrar
 2. Descifrar
1
Ingrese el texto a cifrar: El karma es una energia trascendente
Ingrese el desplazamiento: 2
El resultado es:

Gn mctoc gu wpc gpgtikc vtcuegpfgpvg
```

Fig. 22. Ejemplo de cifrado con desplazamiento 2

    - M: El karma es una energia trascendente
    - C: Gn mctoc gu wpc gpgtikc vtcuegpfgvg
  - Ejemplo 2

```
Seleccione el numero de la opcion que desea realizar:
 1. Cifrar
 2. Descifrar
1
Ingrese el texto a cifrar: Cifrar es escribir un mensaje en clave mediante un sistema de signos
Ingrese el desplazamiento: 4
El resultado es:

Gmjvev iw iwgvmfmv yr qirweni ir gpezi qihmerxi yr wmwxiqe hi wmkrsw
```

Fig. 23. Ejemplo de cifrado con desplazamiento 4

    - M: Cifrar es escribir un mensaje en clave mediante un sistema de signos
    - C: Gmjvev iw iwgvmfmv yr qirweni ir gpezi qihmerxi yr wmwxige hiwmkrsw
- Descifrado
  - Ejemplo 1

```
Seleccione el numero de la opcion que desea realizar:
 1. Cifrar
 2. Descifrar
2
Ingrese el texto a descifrar: Kqnziz ma makzqjqz cv umvairm mv ktidm umlqivbm cv aqabmui lm aqoywa
Ingrese el desplazamiento: 8
El resultado es:

Cifrar es escribir un mensaje en clave mediante un sistema de signos
```

Fig. 24. Ejemplo de descifrado con desplazamiento 8

    - M: Kqnziz ma makzqjqz cv umvairm mv ktidm umlqivbm cv aqabmui lm aqoywa
    - C: Cifrar es escribir un mensaje en clave mediante un sistema de signos
  - Ejemplo 2

```
Seleccione el numero de la opcion que desea realizar:
 1. Cifrar
 2. Descifrar
2
Ingrese el texto a descifrar: Ov ukbwk oc exk oxobqsk dbkcmoxnoxdo
Ingrese el desplazamiento: 10
El resultado es:

El karma es una energia trascendente
```

Fig. 25. Ejemplo de descifrado con desplazamiento 10

    - M: Ov ukbwk oc exk oxobqsk dbkcmoxnoxdo
    - C: El karma es una energia trascendente

D. Conclusiones

- El uso de cifrado ayuda a garantizar: confidencialidad, autenticación e integridad en los datos que se transmiten, en el caso de los algoritmos simétricos su principal beneficio el procesamiento rápido para encriptar y desencriptar un alto volumen de datos.
- Los algoritmos de cifrado ayudan a prevenir el fraude de datos, como por ejemplo el perpetrado por piratas informáticos que obtienen ilegalmente información financiera electrónica.
- El álgebra lineal que ha servido para desarrollar el cifrado de Hill, también sirve para romper su código para evitar esto se debe modificar el algoritmo para que la calve no sea fija si no dinámica y no exista este tipo de vulnerabilidad.

E. Recomendaciones

- Es importante implementar algoritmos de cifrado en la transmisión de datos debido a que es un componente vital para garantizar la seguridad del envío de dichos datos.
- Es necesario tener muy en claro los diferentes tipos de cifrado ya que esto ayuda a mantener una buena seguridad.

REFERENCES

[1] ”Cifrado por sustitucion” (2012).https://es.slideshare.net/GAlbertoHoyos/cifrado-por-sustitucion. accedido (31,ago,2021).

[2] ”¿Qué es el cifrado César y cómo funciona?”.https://ayudaleyprotecciondatos.es/2020/06/10/cifrado-cesar/. accedido (31,ago,2021).

[3] NIHIL, “Criptografía en Python: Cifrado cesar y vigenère”, La cripta del hacker, oct. 25, 2020. https://lacriptadelhacker.wordpress.com/2020/10/25/criptografia-en-python-cifrado-cesar-y-vigenere/ (accedido ago. 31, 2021).

[4] “El cifrado de Vigenère”. https://www.ugr.es/ anillos/textos/pdf/2011/EXPO-1.Criptografia/02a11.htm (accedido ago. 31, 2021).

[5] “Criptosistema Hill”, jun. 26, 2005. https://www.textoscientificos.com/criptografia/hill (accedido ago. 31, 2021).

[6] “Criptografía (XXIII): cifrado de Hill (I), Criptografía (XLIX): el algoritmo DES (I)”, Criptografía (I). https://mikelgarcialarragan.blogspot.com/2015/03/criptografia-i.html (accedido ago. 31, 2021).