UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA, 2023-1

CRIPTOGRAFÍA

PRACTICAL SESSION 1

The Bifid Cipher

PROFESORA:

Dra. Rocío Aldeco Pérez

ALUMNA:

Karla Andrea Najera Noyola

Practical Session 1: The Bifid Cipher

Instrucciones

i. Describir paso a paso como se puede desencriptar un mensaje usando Cifrado Bífido.
ii. Usar el tableau proporcionado para:
    a. Encriptar: BRING ALL YOUR MONEY
    b. Desencriptar: PDRRNGBENOPNIAGGF

	0	1	2	3	4
0	E	N	C	R	Y
1	P	T	A	B	D
2	F	G	H	I	K
3	L	M	O	Q	S
4	U	V	W	X	Z

iii. Implementar este proceso en el lenguaje de programación de nuestra preferencia.

Introducción

Dado que desde el inicio de los tiempos el ser humano ha buscado la forma de enviar mensajes de forma confidencial y que solo personas autorizadas sean capaces de comprender, hoy en día existe una clasificación de la criptografía que hace referencia a algoritmos que han dejado una marca importante en el desarrollo de los sistemas de cifrados actuales la cual recibe el nombre de criptografía moderna.

Dentro de esta categoría podemos encontrar 2 principales tipos:

- **Algoritmos de transposición:** Son métodos en los que los caracteres que conforman un mensaje en claro se cambian de posición dentro de su mismo mensaje dando lugar a una cadena que no es comprendida a simple vista. El ejemplo más común es la escítala griega.
- **Algoritmos de sustitución simple**: Son aquellos en los que los caracteres del texto original se reemplazan por alguno otro dentro de un determinado alfabeto. Es decir, se realiza una correspondencia entre parejas de caracteres, en donde el segundo elemento de una pareja establece el carácter que sustituye al primer elemento de la pareja. Tienen importancia

En este trabajo practico nos centraremos en la última categoría mencionada, haciendo énfasis en el método de Cifrado Bífido, el cual es uno de los algoritmos más representativos y seguros dentro del apartado de métodos de sustitución clásicos.

Marco Teórico

La presente investigación hará uso del siguiente concepto:

- **Cifrado bífido**

El cifrado bífido es un algoritmo creado en el año de 1901 por parte de Felix Delastalle, un criptógrafo francés y aunque nunca se utilizó con fines bélicos o un motivo de particular relevancia, cuenta con un diseño bastante elegante y difícil de romper en comparación con algunos otros algoritmos de sustitución simple.

Es considerado como una evolución del cuadrado de Polybius, haciendo uso de transposición para lograr difusión. En realidad, la clave de este cifrado hace uso de permutaciones del alfabeto (con excepción de la J), haciendo uso de una palabra clave que no contenga palabras clave y completar la permutación de las letras con el sobrante en los elementos del abecedario con el fin de llenar una matriz de 5x5 que recibe el nombre de tableau a partir de la cual se hará la posterior correspondencia entre caracteres.

Dado que hoy en día es muy fácil de romper en comparación de algoritmos más modernos solo se ve su uso por parte de personas que dan sus primeros pasos dentro de la criptografía.

Análisis del problema

Para comprender mejor este algoritmo, será necesario en primer lugar conocer la manera en la que se cifra un mensaje con el Cifrado Bífido. En primer lugar, contaremos con una palabra clave que no contenga caracteres repetidos (idealmente), con la cual llenaremos la primera parte del tableau. Una vez que esta palabra fue colocada, se llena con el resto de las letras disponibles de nuestro alfabeto modificado con el fin de obtener una matriz de 5x5. Para esta práctica se hará uso de la palabra “ENCRYPT” como clave, además de un abecedario modificado que no contempla el uso de J con el fin de llenar las 25 posiciones sin que nos sobren o hagan falta elementos.

El resultado obtenido es el siguiente:

	0	1	2	3	4
0	E	N	C	R	Y
1	P	T	A	B	D
2	F	G	H	I	K
3	L	M	O	Q	S
4	U	V	W	X	Z

Una vez que se realizó lo anterior, se procede a hacer la correspondencia de caracteres en nuestro mensaje colocando las coordenadas en 2 filas (arriba la coordenada vertical y abajo la coordenada horizontal). Por ejemplo, supongamos que nuestro mensaje encriptado es la frase "HOLA MUNDO". La correspondencia de caracteres quedaría de la siguiente forma

H	O	L	A		M	U	N	D	O
2	3	3	1		3	4	0	1	3
2	2	0	2		1	0	1	4	2

Acto seguido, se colocan todos los elementos en una sola fila (no se consideran espacios).

2331340132202101 42

Se acomoda por pares y se hace nuevamente la correspondencia entre caracteres

23	31	34	01	32	20	21	01	42
I	M	S	N	O	F	G	N	W

El texto cifrado es el siguiente:

IMSNOFGNW

Considerando el proceso de cifrado como el antecedente principal, a continuación, veremos el proceso contrario, la resolución de los ejercicios propuestos y su implementación mediante el lenguaje de programación Java.

Hipótesis

A partir del proceso de cifrado, obtendremos el método por el cual se puede descifrar un mensaje dado mediante la técnica Bífida.

Para probar la siguiente hipótesis, propongo los siguientes pasos como el proceso general para desencriptar una cadena:

En primer lugar, se buscan las letras en el tableau dado, con el fin de obtener los pardes de números de la correspondencia. Cada letra nos dirá un valor numérico "X" que representa la fila en que se encuentra (en este caso, la coordenada vertical) y, a su vez, también obtenemos un valor numérico "Y" que representa la columna del tableau en que se halla la letra (coordenada horizontal). Una vez hecho lo anterior se obtiene un conjunto de pares "XY", de tal manera que toda nuestra frase podrá verse como "X1Y1 X2Y2..XnYn".

A continuación, dividimos nuestro conjunto de números, de manera que la primera mitad de esos números pasa a permanecer en una fila superior y la otra mitad de esos números pasa a la fila inferior.

Así tenemos:

Fila superior: XX XX XX XX…XX
Fila inferior: YY YY YY YY…YY

Cabe destacar que en este caso las X's serán nuestra primera mitad del total de valores y las Y's la segunda parte. Por lo que, dado que todas las correspondencias tienen la forma (X,Y), sabemos que las X son el numero de fila, mientras que la Y representa a la columna, por lo que queda buscar en el tableau las coordenadas

Para probar esta hipótesis, usaremos la cadena obtenida en el ejemplo de cifrado anterior: **IMSNOFGNW.** Para ello, buscaremos sus valores numéricos dentro del tableau.

I	M	S	N	O	F	G	N	W
23	31	34	01	32	20	21	01	42

El arreglo resultante queda como: **233134013220210142.**

Este arreglo resultante se divide en 2 mitades para obtener los índices del mensaje original

2	3	3	1	3	4	0	1	3
2	2	0	2	1	0	1	4	2

A partir de las coordenadas obtenidas, desciframos para obtener el mensaje original:

22	32	30	12	31	40	01	14	32
H	O	L	A	M	U	N	D	O

El texto descifrado nos sale como **HOLAMUNDO**, lo que confirma nuestra hipótesis.

Conociendo el proceso de cifrado y dado un algoritmo de descifrado, usar el tableau proporcionado para:

- ***a. Encriptar: BRING ALL YOUR MONEY***
- ***b. Desencriptar: PDRRNGBENOPNIAGGF***

En primer lugar, encriptaremos el mensaje **BRING ALL YOUR MONEY.**

El primer paso será obtener los índices tomando en cuenta el tableau proporcionado para la práctica:

B	R	I	N	G		A	L	L		Y	O	U	R		M	O	N	E	Y
1	0	2	0	2		1	3	3		0	3	4	0		3	3	0	0	0
3	3	3	1	1		2	0	0		4	2	0	3		1	2	1	0	4

Vemos que el arreglo resultante será:

1 0 2 0 2 1 3 3 0 3 4 0 3 3 0 0 0 3 3 3 1 1 2 0 0 4 2 0 3 1 2 1 0 4

Acomodamos por pares y obtenemos la siguiente correspondencia:

10	20	21	33	03	40	33	00	03	33	11	20	04	20	31	21	04
P	F	G	Q	R	U	Q	E	R	Q	T	F	Y	F	M	G	Y

Tomando en cuenta lo anterior, el texto cifrado será: **PFGQRUQERQTFYFMGY**.

Para hacer el proceso de descifrado vamos a utilizar la cadena ***PDRRNGBENOPNIAGGF.*** Procedemos a buscar en el tableau los índices de cada letra, lo que nos permite obtener el siguiente arreglo:

10	14	03	03	01	21	13	00	01	32	10	01	23	12	21	21	20
P	D	R	R	N	G	B	E	N	O	P	N	I	A	G	G	F

Al ponerlo en una sola fila queda como:

1 0 1 4 0 3 0 3 0 1 2 1 1 3 0 0 0 1 3 2 1 0 0 1 2 3 1 2 2 1 2 1 2 0

Lo dividimos en 2 mitades con el fin de obtener los índices para descifrar el mensaje original:

1	0	1	4	0		3	0	3	0	1	2	1	1	3	0	0	0
1	3	2	1	0		0	1	2	3	1	2	2	1	2	1	2	0

Con las coordenadas obtenidas, podemos obtener el mensaje a partir del tableau.

T	R	A	V	E	L	N	O	R	T	H	A	T	O	N	C	E

El mensaje descifrado queda como: **TRAVELNORTHATONCE**.

Conociendo el proceso de ambos algoritmos, realizar la implementación en el lenguaje de programación de nuestra preferencia.

Se selecciono Java debido a su manejo de arreglos y listas, los cuales serán de mucha utilidad al momento de codificar ambos procesos.

Se hará uso de 2 clases por medio de las cuales un usuario podrá cifrar y/o descifrar sus mensajes:

- **Main.java:** Es la clase principal del proyecto. A través de esta se harán las interacciones con el usuario, incluyendo la captura del mensaje y el cifrado/descifrado tras la aplicación del algoritmo. Se compone de un único método (Main) en el cual se imprime el menú de usuario y se realiza el flujo del programa.
- **tableau.java:** Dentro de esta clase se definen todos los procesos y funciones que permiten el cifrado y descifrado de los mensajes que el usuario ingrese. Se compone de las siguientes 3 variables de instancia:
  - matriz: Arreglo de 2 dimensiones en el que se almacenará el tableau a utilizar para el cifrado de los datos.
  - abecedario: Se compone de un arreglo de 1 sola dimensión que almacena el alfabeto modificado a usar dentro del programa (25 letras sin contar la Ñ o la I).
  - clave: Arreglo de una dimensión que almacena los caracteres de la palabra clave para el ordenamiento del tableau. En este caso se definirá como "ENCRYPT".

  Asimismo, dentro de esta clase se encuentran los siguientes métodos:
  - tableau(): Constructor de la calse. En esta se definen las variables de instancia y se llama al método que permite el llenado del tableau.
  - llenadoTableau(): A partir de 2 ciclos For anidados hará el llenado del tableu colocando en primera posición los caracteres no repetidos de la palabra clave para proseguir con aquellos caracteres que no hayan sido utilizados. Tras llenar las 25 posiciones el arreglo de 2 dimensiones queda listo para su uso.
  - encriptarMensaje(): Permite la encriptación del mensaje al implementar el algoritmo previamente comentado para el cifrado. Para cada uno de los caracteres realiza la búsqueda de su posición dentro del tableau y lo almacena dentro de un arreglo que en este caso hará alusión a las 2 filas de coordenadas. Tras generar estas filas, genera el mensaje encriptado mediante un ciclo haciendo búsqueda de los caracteres que sustituyen a la cadena original. Devuelve como valor un String que en este caso representa al mensaje encriptado.
  - desencriptarMensaje(): Realiza el proceso contrario al cifrado. En primer lugar, realiza la búsqueda de los caracteres dentro del tableau y almacena las posiciones dentro de un arreglo que posteriormente permitirá hacer la correspondencia entre los caracteres cifrado y los del texto plano. Devuelve una String que representa al mensaje desencriptado.

Para la ejecución de este programa, se implementa un menú con las siguientes 3 opciones:

1. **Encrypt**: Al seleccionar esta opción, se realiza la encriptación de un mensaje que un usuario brinde con el tableau indicado por las instrucciones de esta práctica.
2. **Decrypt**: Al seleccionar esta opción, se realiza el descifrado de un mensaje dado a partir del algoritmo propuesto, haciendo uso del tableau de esta práctica.
3. **Exit**: Termina la ejecución del programa.

Cabe destacar que el programa se repite de manera infinita hasta que el usuario seleccione la opción de "Exit".

Aunque las clases ya han sido compiladas, en caso de ser requerido se puede compilar con la siguiente instrucción:

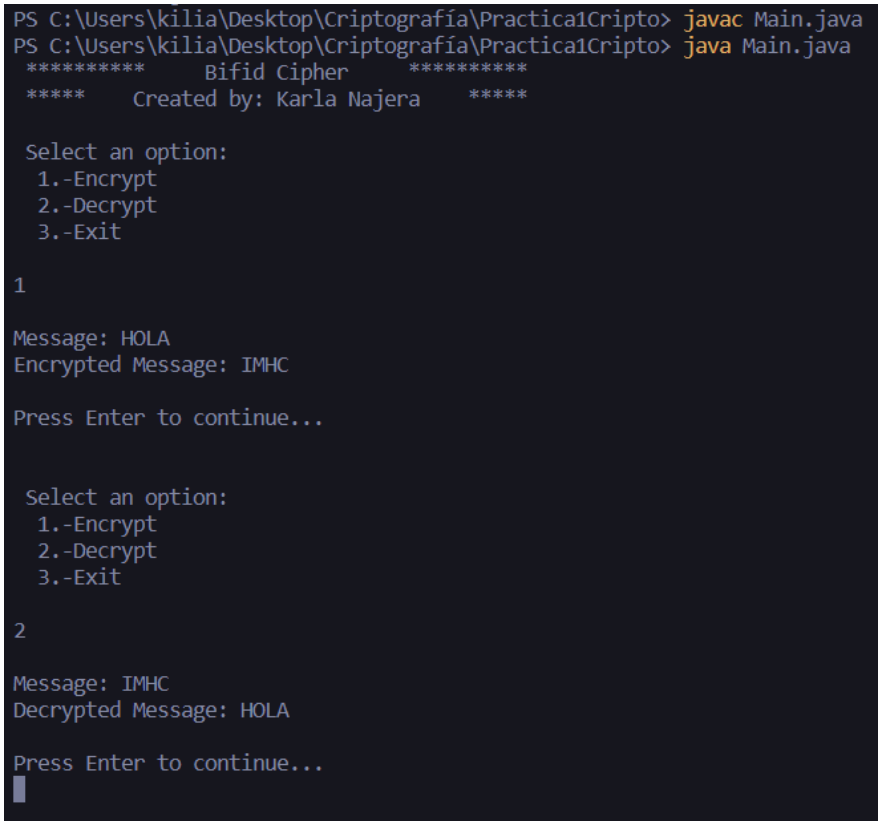
javac Main.java

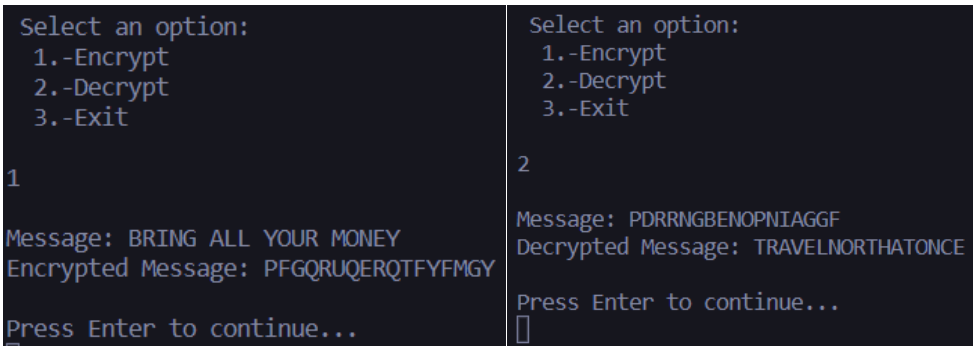
Y se ejecuta con el siguiente comando:

java Main.java

Nota: Para su compilación es necesario tener instalada alguna versión de JDK, aunque la versión que fue utilizada para su elaboración es la 18.0.2.1.

A continuación, se muestran algunas capturas de pantalla de su funcionamiento:





Aunque se adjunta un archivo en zip con los archivos utilizados para esta práctica, se comparte el enlace de GitHub: https://github.com/kiliapplered/Practica1Cripto.git

Conclusiones

Del presente trabajo es posible obtener las siguientes conclusiones:

- A partir de la presente práctica fue posible conocer uno de los algoritmos más famosos de sustitución simple, siendo en este caso el Cifrado Bífido.
- Aunque hoy en día podría resultar simple el funcionamiento de este algoritmo, no quedan dudas que en su momento presentó un avance significativo con respecto a lo que hoy conocemos como Criptografía Clásica.
- Pese a que el código solo muestra una palabra clave por defecto, con algunos cambios menores sería posible crear una opción que permita cambiar la palabra clave para ordenar el tableau.
- La realización de este ejercicio permitió solidificar los conocimientos adquiridos durante la revisión teórica de la asignatura.

Referencias

[1] «Geeks for Geeks,» 6 Noviembre 2019. [En línea]. Available: https://www.geeksforgeeks.org/bifid-cipher-in-cryptography/. [Último acceso: 17 Septiembre 2022].

[2] «JC Mouse,» 26 Junio 2011. [En línea]. Available: https://www.jc-mouse.net/net/encriptacion-por-el-metodo-bifido. [Último acceso: 17 Septiembre 2022].

[3] «Acervo Lima,» 2017. [En línea]. Available: https://es.acervolima.com/cifrado-bifido-en-criptografia/#:~:text=Esta%20t%C3%A9cnica%20de%20cifrado%20se,luego%20los%20vuelve%20a%20combinar.. [Último acceso: 17 Septiembre 2022].

Yo, Karla Andrea Najera Noyola, hago mención que esta práctica fue de mi autoría.