Universidad Nacional Autónoma de México

Facultad de Ingeniería

Práctica 1
"The Bifid cipher"

Criptografía

Grupo: 02

Profesora: Rocío Aldeco, PhD

Elaborado por:
Medel Sánchez Berenice

Semestre 2020-2

Cd. Universitaria a 11 de Febrero del 2020

Objetivo.

Entender el algoritmo de cifrado Bifido, así como llevar a cabo la implementación de dicho algoritmo. Además, proponer el algoritmo de descifrado que logra romper el algoritmo bífido e implementarlo.

Actividades.

- Describir paso a paso como descifrar un mensaje usando el cifrado Bifido.
    1. Buscar las coordenadas de cada palabra en el texto cifrado y almacenarlas todas juntas en una lista según el orden en el mensaje.
    2. Separar esa lista en dos partes iguales y almacenarlas en diferentes listas A y B. La primer mitad (A) serán las coordenadas en x de las letras a encontrar; la segunda mitad (B)serán las coordenadas de y.
    3. Realizando pares entre las dos listas, buscar las coordenadas en la tabla dada. Es decir, posición 1 de lista A con posición 1 de lista B, será una coordenada x, y.
    4. Escribir las letras encontradas en dichas coordenadas

- Usar el algoritmo con la tabla dada para
    1. Cifrar “BRING ALL YOUR MONEY”

       Buscando los índices dentro de la tabla

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

       Listando los índices, primero todos los índices en x y luego todos los índices en y.
       10202133034033001 33311200420312104
       Agrupando en pares y buscando la letra en esos índices

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

    2. Descifrar “PDRRNGBENOPNIAGGF

       Buscar los índices de las letras cifradas

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

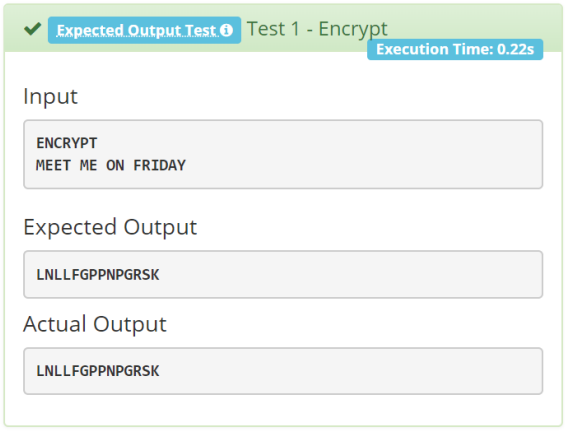
       Separar todas las coordenadas en dos y escribirlas en listas separadas, buscar las letras cifradas

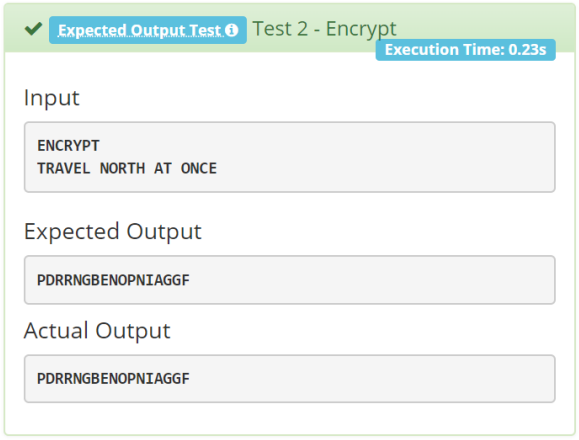
1	0	1	4	0	3	0	3	0	1	2	1	1	3	0	0	0
1	2	3	1	0	0	1	2	3	1	2	2	1	2	1	2	0
T	R	A	V	E	L	N	O	R	T	H	A	T	O	N	C	E

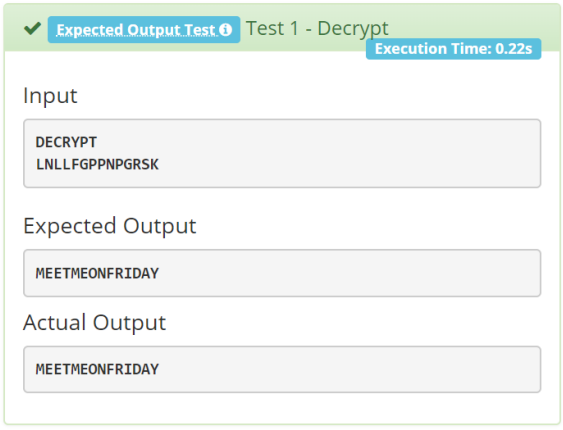
- Crear el pseudocódigo para implementar el cifrado Bifido. Incluyendo el mensaje encryption y decryption

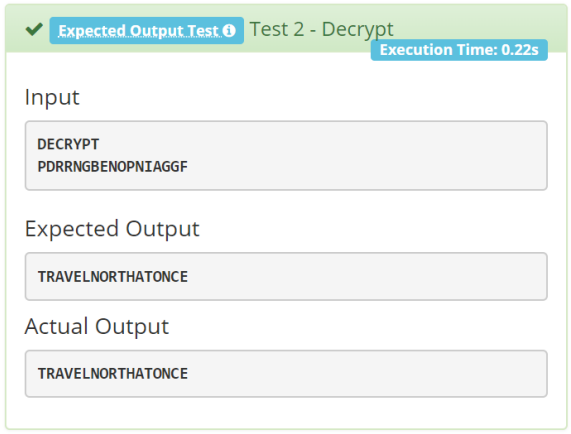
```
INICIO
    A, B, C = []
    Leer entrada
    Método <- entrada1
    Texto <- entrada2
    M <- Crear matriz de índices

    SI método == “encryption” ENTONCES
        Por cada letra en texto
            Buscar coordenadas en M
            Insertar x en A y y en B
        Unir A y B en C
        Por cada par de elementos en C
            Buscar la letra almacenada en las coordenadas en Matriz M
            Imprimir texto.
    Si método == “decryption” ENTONCES
        Por cada letra en texto ENTONCES
            Buscar  coordenadas y almacenar en C
        Almacenar elementos de C[0 – longitud C / 2] en A
        Almacenar elementos de C[longitud C / 2  - longitud] en B
        Por cada elemento en A, B
            Buscar coordenadas en M = M[An,Bn]
            Imprimir texto
FIN
```

Resultados.









Conclusiones.

Se implementó de manera exitosa el algoritmo de cifrado bífido, así como se propuso y se implementó el algoritmo para descifrar los mensajes. Se observó que no es un algoritmo complicado de implementar y, por lo tanto, no es difícil de descifrar los mensajes cifrados con dicho algoritmo.