Guía Práctica de Laboratorio
Sesión 13: INTRODUCCIÓN A LA PROGRAMACIÓN
MLBC - VACJ - CJFV

En esta sesión, se habla de criptogramas cuya misión es el cifrado o decifrado de mensajes, a través de alguna estrategia, que se usa de manera sistemátca para ambos efectos..

Se describe algunas de éstas técnicas y se espera que implementes la funcionalidad para poder automatizar el cifrado y decifrado de mensajes.

Se explica en todas las técnicas la forma de cifrar, el proceso de decifrar vendría a ser el inverso del proceso explicado.

1. Cifrador de Polybios

A mediados del siglo II antes de J.C., se encuentra el cifrador por sustitución de caracteres más antiguo que se conoce. Atribuido al historiador griego Polybios, el sistema de cifrado consistía en hacer corresponder a cada letra del alfabeto, un par de letras que indicaban la fila y la columna en la cual aquella se encontraba. Para esto se considera una grilla de $5x5 = 25$ caracteres, transmitiéndose por tanto en este caso el mensaje como un criptograma. En el Cuadro 1 se muestra una tabla de cifrar de Polybios adaptada al inglés, con un alfabeto de cifrado consistente en el conjunto de letras A, B, C, D y E, que podría ser reemplazada por cualquier palabra de cinco letras, todas ellas diferentes por ejemplo: C, L, A, V y E.

En este sistema, la I y la J, tienen el mismo cifrado, ya que el mensaje se puede entender aun cuando se alterna estas letras.

	A	**B**	**C**	**D**	**E**
A	A	B	C	D	E
B	F	G	H	IJ	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Cuadro 1: Matriz de cifrado de Polybios

Acorde con este método, considerando la tabla del Cuadro 1, la letra A se cifrará como AA, la H como BC, etc. Esto significa que se aplica una sustitución al alfabeto $A, B, C, .., X, Y, Z$ de 26 letras convirtiéndolo en un alfabeto de cifrado $AA, AB, AC, ..., EC, ED, EE$ de 25 caracteres, en la que sólo se necesitan 5 símbolos diferentes, en el ejemplo A, B, C, D, E.

Por ejemplo, si se tiene el mensaje “QUE BUENA IDEA LA DEL GRIEGO”, con clave “ABCDE”, el mensaje cifrado será: “DADEAE ABDEAECCAA BDADAEAA CAAA ADAECA BBDBBDAEBBCD”, fijate que todo espacio en blanco también se duplica. En esta técnica, el mensaje cifrado siempre tendrá el doble de caracteres del mensaje original.

El mismo mensaje, “QUE BUENA IDEA LA DEL GRIEGO”, pero con clave “CLAVE”, obtendrá el mensaje cifrado: “VCVECE CLVECEAACC LVCVCECC ACCC AVCEAC LLVLCELLAV”

En esta versión del analizador de mensajes, cada mensaje tiene una clave de cinco letras diferentes, que se utiliza para obtener el mensaje cifrado.

- dado un mensaje, conseguir el mensaje cifrado (método $cifrar$)
- dado un mensaje cifrado, conseguir el mensaje original (método $decifrar$)
- mantener el registro de los mensajes que ha atendido
- reportar los mensajes que no han podido ser cifrados y/o decifrados a causa de una clave no adecuada

Recuerda que cada mensaje tiene su propia clave de cifrado.

2. El cifrador de Alberti

En el siglo XVI Leon Battista Alberti presenta un manuscrito en el que describe un disco cifrador con el que es posible cifrar textos sin que exista una correspondencia única entre el alfabeto del mensaje y el alfabeto de cifrado como en los casos analizados anteriormente. Con este sistema, cada letra del texto en claro podía ser cifrada con un carácter distinto dependiendo esto de una clave secreta. Se dice entonces que tales cifradores usan más de un alfabeto por lo que se denominan cifradores polialfabéticos, a diferencia de los anteriores denominados monoalfabéticos

Para la tarea de hoy, se hace una variante del disco de Alberti, en este caso el analizador tiene un disco doble, en el disco externo se tienen las letras del alfabeto y los dígitos decimales, en el disco interno se tienen las letras del alfabeto y los dígitos decimales en orden aleatorio. Ambos discos tienen una marca (punto) que es el lugar de inicio de disco interno, para poder cifrar se requiere saber cuanto el disco interno debe rotar ya sea en sentido horario (positivo) o en sentido antihorario (negativo). En la figura 1 se muestran ejemplos del disco, en a) se tiene el disco doble en su situación inicial, en b) se tiene el disco después de que el disco interno ha rotado 10 posiciones en sentido horario (+10) y en c) se tiene el disco después de que el disco interno ha rotado 5 posiciones en sentido antihorario (-5)

Las rotaciones del disco interno, se hacen desde el punto de partida que esta identificado por un punto en ambos discos: externo e interno. En el ejemplo de la figura, el punto esta en 'A'del disco externo y en la letra 'Vén el disco interno, por lo que que el inicio para las rotaciones es cuando los dos discos coinciden en la marca que en este caso es el PUNTO.

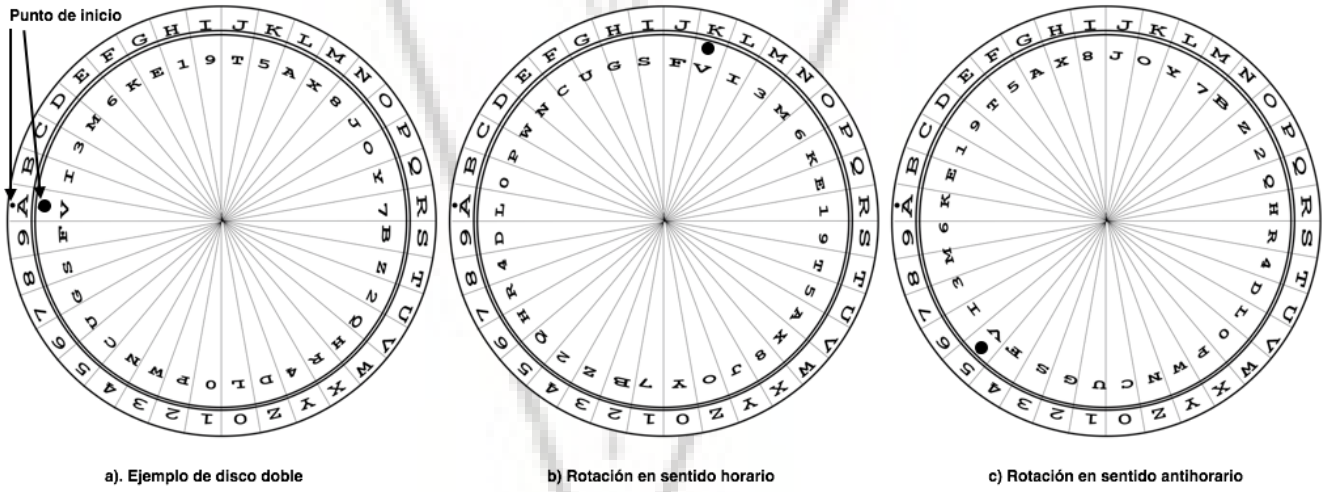

Figura 1: Ejemplo de Disco de Alberti - adaptación

Si se toma el disco del inciso a) de la figura, y se quiere cifrar el mensaje "HOLA MUNDO", con una rotación de +10, el disco en realidad que se tomará para el cifrado es del inciso b) de la figura; entonces se obtendrá el mensaje cifrado "G6IL 35MW6".

Si se toma el disco del inciso a) de la figura, y se quiere cifrar el mensaje "HOLA MUNDO", con una rotación de -5, el disco en realidad que se tomará para el cifrado es del inciso c) de la figura; entonces se obtendrá el mensaje cifrado "XZYK 7DB9Z".

En este cifrador, si se encuentra un espacio en blanco este espacio se respeta.

Considerando este contexto se te pide diseñar un programa que permita:

- dado un mensaje, conseguir el mensaje cifrado
- dado un mensaje cifrado, conseguir el mensaje original
- mantener el registro de los mensajes que ha atendido

- reportar los mensajes que no ha podido cifrar y/o decifrar a causa de una clave no adecuada

3. Cifrador Tabular

En esta ocasión, para cifrar un mensaje se utiliza una clave que consta de letras distintas, la clave debe ser una palabra. Con esta información se genera una matriz cuyas columnas son las letras de la clave y se tienen tantas filas como caracteres tenga el mensaje. En caso de faltar caracteres se completa con las primeras letras del alfabeto.

Por ejemplo, si se tiene el mensaje es "LOS CUADRADOS ESTAN DE COMPLICADOS ES HORA DE OBTENER LOS LADOS" y la clave es "CURADO", se genera una matriz asi:

C	U	R	A	D	O
L	O	S		C	U
A	D	R	A	D	O
S		E	S	T	A
N		D	E		C
O	M	P	L	I	C
A	D	O	S		E
S		H	O	R	A
	D	E		O	B
T	E	N	E	R	
L	O	S		L	A
D	O	S	A	B	C

La segunda fase es ordenar la clave considerando sus caracteres, en el ejemplo, la clave con sus carateres ordenados es: "ACDORU"; considerando este orden, las columnas de la matriz cambiaran de lugar, en el ejemplo la columna 0 ahora será la columna 1, la columna 1 será la columna 5 y asi; la matriz resultante de esta transformación es la siguiente:

A	C	D	O	R	U
	L	C	U	S	O
A	A	D	O	R	D
S	S	T	A	E	
E	N		C	D	
L	O	I	C	P	M
S	A		E	O	D
O	S	R	A	H	
		O	B	E	D
E	T	R		N	E
	L	L	A	S	O
A	D	B	C	S	O

El mensaje cifrado se recoge de la matriz leyendo de izquierda a derecha y de arriba a abajo, por lo que el mensaje cifrado es:

" LCUSOAADORDSSTAE EN CD LOICPMSA EODOSRAH OBEDETR NE LLASOADBCSO"

Considerando este contexto se te pide diseñar un programa que permita:

- dado un mensaje, conseguir el mensaje cifrado

- dado un mensaje cifrado, conseguir el mensaje original
- mantener el registro de los mensajes que ha atendido
- reportar los mensajes que no ha podido cifrar y/o decifrar a causa de una clave no adecuada