Proyecto 2:
Cifrado utilizando matrices

Objetivos:

- Integrar los contenidos aprendidos durante el curso.
- Poner en práctica los conocimientos adquiridos sobre vectores bidimensionales y cadenas.
- Reforzar la resolución de problemas

Marco Teórico:

Existen muchas formas de escribir de manera enigmática, en la actualidad a pesar de la infraestructura con la que se cuenta, se suele sacrificar rendimiento con tal de asegurar la confidencialidad de un mensaje. Existen muchas formas de cifrar un mensaje, una de las más populares y que ha durado muchos años como inquebrantable, consiste en lo siguiente:

- Se tiene una matriz de n*n donde su primera fila es el alfabeto completo, y cada una de las filas siguientes es el alfabeto con un corrimiento hacia la izquierda que incrementa de fila a fila, como se muestra en la imagen:

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

- En base a la tabla se crea una relación fila columna entre la clave y el mensaje que se necesita cifrar donde se busca encontrar la intersección entre las letras de la clave y el mensaje, por ejemplo:
  Se tiene que el mensaje es "IMPOSTOR"
  Y como clave "ROJO"

  La primera letra del mensaje representará la posición de las columnas y la primera de la clave la posición en las filas, por lo que la primera letra del mensaje cifrado sería la Z:

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

- La clave debe repetirse cuantas veces sea necesario para cubrir el mensaje.

I	M	P	O	S	T	O	R	Mensaje
R	O	J	O	R	O	J	O	Clave

  De lo anterior, el mensaje cifrado resultante sería: **ZAYCJHXF**

- Una variante de este algoritmo es que al llegar al final de la clave, se coloca parte del mensaje, desde su inicio para completar la cifra.

I	M	P	O	S	T	O	R	Mensaje
R	O	J	O	I	M	P	O	Clave

  De lo anterior el mensaje cifrado sería:

ZAYCAFDF

Este método de cifrado fue vigente durante muchos años, hasta que se utilizó la redundancia del lenguaje como ayuda para identificar la clave, la redundancia del lenguaje nos indica qué tan probable es que ciertas letras aparezcan, para el idioma español se tiene la siguiente estadística:

Letra	Porcentaje
e	14,0%
a	12,2%
o	9,9%
s	7,7%
n	6,6%
r	6,2%
i	5,5%
l	5,4%
d	5,3%
u	4,8%
t	3,8%
c	3,6%
m	2,7%
p	2,2%
q	2,0%
y	1,5%
b	1,5%
h	1,2%
v	1,1%
g	1,0%
j	0,6%
f	0,5%
z	0,4%
k	0,1%

Instrucciones:

Se le pide elaborar un programa utilizando Macro Assembler donde le permita al usuario las siguientes opciones:

a. Ingresar un mensaje en claro y una clave y generar el criptograma correspondiente
b. Ingresar un mensaje en claro y una clave y generar el criptograma utilizando la variante del algoritmo, es decir, tomar parte del mensaje como clave.
c. Descifrar un criptograma dada una clave y el criptograma.
d. Dado un criptograma que puede llegar a ser idealmente 3 veces más grande que el alfabeto para que sea significativo, calcular la estadística de las letras por su ocurrencia en el mensaje y deducir qué letras podrían ser las originales en el mensaje.

Indicaciones adicionales:

Este método de cifrado no toma en cuenta un alfabeto extendido como sería el ASCII, por lo que si el usuario ingresa algún caracter especial o número, deberá ser ignorado para cifrar o descifrar.

Deberá hacer uso específico de matrices y su recorrido para hacer los cálculos.

Entregables:

1. Código fuente con su documentación interna
2. Descripción en un diagrama de flujo de su solución
3. Manual de usuario

Codificación	85
Diseño de la solución	10
Manual de usuario	5
Total	100