

Cifrado y descifrado mediante matrices

Manual de usuario

El programa llamado «Project2» es capaz de cifrar y descifrar un mensaje usando una matriz que contiene el abecedario. Las imágenes de referencia de este manual fueron tomadas en un equipo con Windows 10 de 64 bits.

Indicaciones generales

1. El programa es capaz de reconocer únicamente letras mayúsculas. Si el mensaje o la clave se ingresan con letras minúsculas, se producirán resultados inesperados.
2. A pesar de que el programa solo trabaja con letras mayúsculas, es capaz de ignorar caracteres ajenos al abecedario (como @, +, /, !, #...), es decir que estos caracteres no se toman en cuenta tanto en el mensaje como en la clave al momento de cifrar o descifrar. La letra «ñ» también es tomada como un carácter ajeno.
3. Existen dos maneras de realizar el cifrado con su respectivo descifrado: la primera es repitiendo la clave tantas veces como sea necesario para abarcar el mensaje completo y la variante es tomar la clave y, si esta no abarca la longitud total del mensaje, tomar parte del mensaje mismo.
4. El programa realiza el cifrado de la siguiente manera:

Se tiene una matriz cuadrada base que contiene todas las letras del abecedario (en mayúscula). En cada fila se realiza un desfase hacia la izquierda, tal como se aprecia 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

Así, el cifrado se realiza buscando la letra inicial del mensaje en la primera fila y la letra inicial de la clave en la primera columna, tal como se muestra en la siguiente imagen, donde se usa como mensaje IMPOSTOR y como clave ROJO:

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

De este modo, se busca la intersección entre dichas fila y columna y se toma la letra resultante como parte del mensaje cifrado. Luego se realiza el mismo procedimiento con la siguiente letra, tanto del mensaje como de la clave, hasta terminar de cifrar el mensaje. El mensaje cifrado, siguiendo esta norma, queda ZAYCJHXF.

```

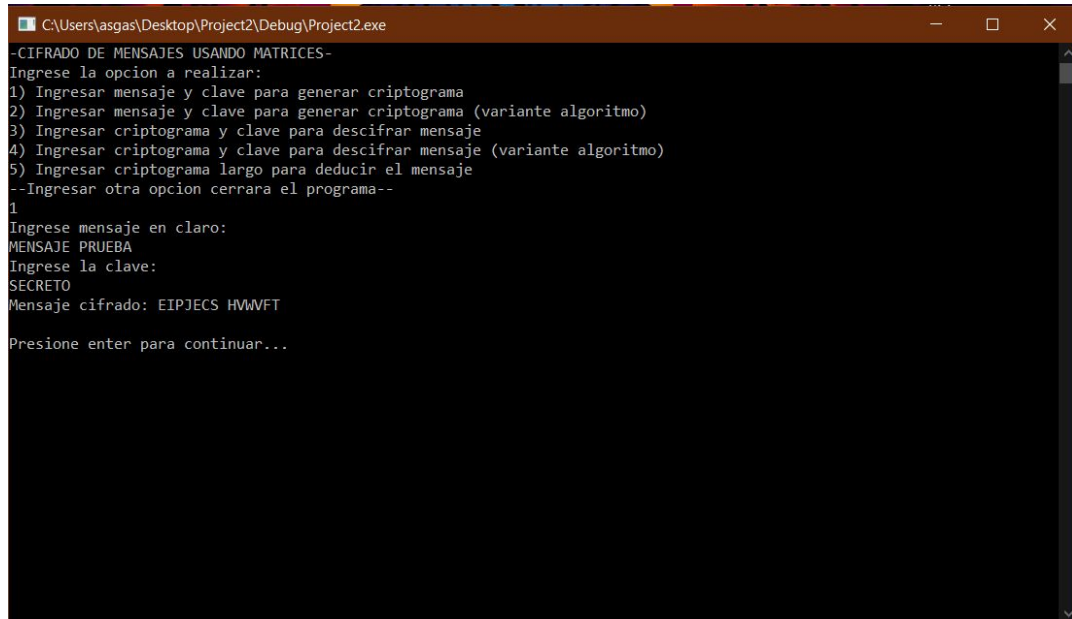
C:\Users\asgas\Desktop\Project2\Debug\Project2.exe
--CIFRADO DE MENSAJES USANDO MATRICES--
Ingrese la opcion a realizar:
1) Ingresar mensaje y clave para generar criptograma
2) Ingresar mensaje y clave para generar criptograma (variante algoritmo)
3) Ingresar criptograma y clave para descifrar mensaje
4) Ingresar criptograma y clave para descifrar mensaje (variante algoritmo)
5) Ingresar criptograma largo para deducir el mensaje
--Ingresar otra opcion cerrara el programa--

```

Vista del menú principal de la aplicación.

1. Cifrado de un mensaje

Para cifrar un mensaje usando el algoritmo original, presione la tecla 1 seguido de enter. A continuación se le pedirá que ingrese el mensaje y la clave a usar. Automáticamente se devolverá en el mensaje cifrado.

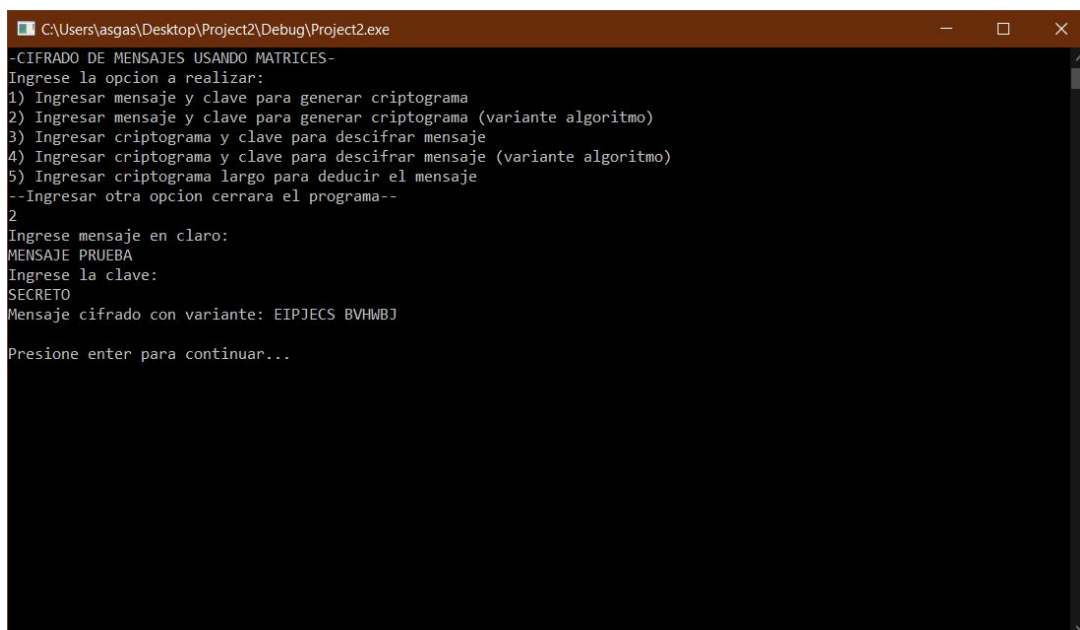


```
C:\Users\asgas\Desktop\Project2\Debug\Project2.exe
-CIFRADO DE MENSAJES USANDO MATRICES-
Ingrese la opcion a realizar:
1) Ingresar mensaje y clave para generar criptograma
2) Ingresar mensaje y clave para generar criptograma (variante algoritmo)
3) Ingresar criptograma y clave para descifrar mensaje
4) Ingresar criptograma y clave para descifrar mensaje (variante algoritmo)
5) Ingresar criptograma largo para deducir el mensaje
--Ingresar otra opcion cerrara el programa--
1
Ingrese mensaje en claro:
MENSAJE PRUEBA
Ingrese la clave:
SECRETO
Mensaje cifrado: EIPJCS HWVFT
Presione enter para continuar...
```

Resultado del cifrado de MENSAJE PRUEBA con la clave SECRETO.

2. Cifrado de un mensaje con la variante del algoritmo

Para cifrar un mensaje usando la variante del algoritmo, presione la tecla 2 seguido de enter. A continuación se le pedirá que ingrese el mensaje y la clave a usar. Automáticamente se devolverá en el mensaje cifrado.

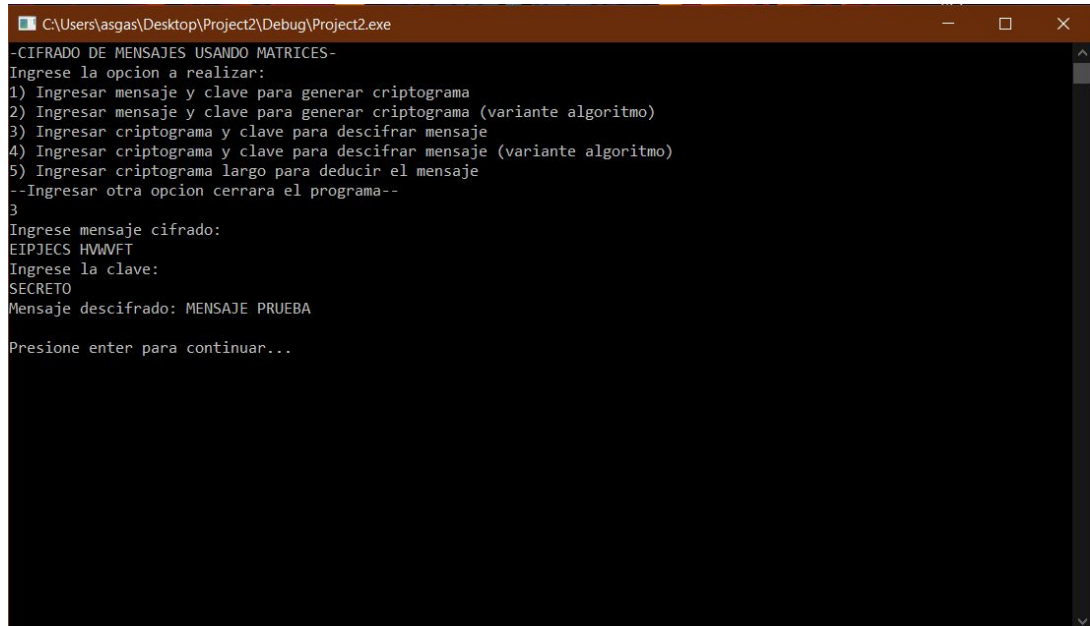


```
C:\Users\asgas\Desktop\Project2\Debug\Project2.exe
-CIFRADO DE MENSAJES USANDO MATRICES-
Ingrese la opcion a realizar:
1) Ingresar mensaje y clave para generar criptograma
2) Ingresar mensaje y clave para generar criptograma (variante algoritmo)
3) Ingresar criptograma y clave para descifrar mensaje
4) Ingresar criptograma y clave para descifrar mensaje (variante algoritmo)
5) Ingresar criptograma largo para deducir el mensaje
--Ingresar otra opcion cerrara el programa--
2
Ingrese mensaje en claro:
MENSAJE PRUEBA
Ingrese la clave:
SECRETO
Mensaje cifrado con variante: EIPJCS BVHWBJ
Presione enter para continuar...
```

Resultado del cifrado con variante de MENSAJE PRUEBA con la clave SECRETO.

3. Descifrado de un mensaje

Para descifrar un mensaje usando el algoritmo original, presione la tecla 3 seguido de enter. A continuación se le pedirá que ingrese el mensaje cifrado y la clave a usar. Automáticamente se devolverá en el mensaje descifrado.

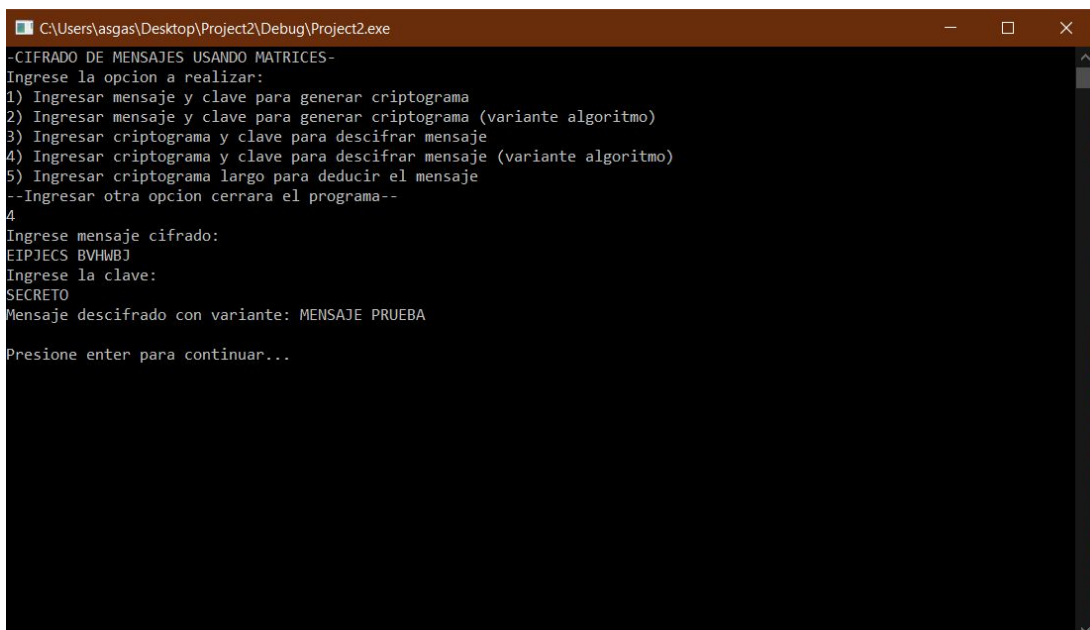


```
C:\Users\asgas\Desktop\Project2\Debug\Project2.exe
-CIFRADO DE MENSAJES USANDO MATRICES-
Ingrese la opcion a realizar:
1) Ingresar mensaje y clave para generar criptograma
2) Ingresar mensaje y clave para generar criptograma (variante algoritmo)
3) Ingresar criptograma y clave para descifrar mensaje
4) Ingresar criptograma y clave para descifrar mensaje (variante algoritmo)
5) Ingresar criptograma largo para deducir el mensaje
--Ingresar otra opcion cerrara el programa--
3
Ingrese mensaje cifrado:
EIPJECs HVVFT
Ingrese la clave:
SECRETO
Mensaje descifrado: MENSAJE PRUEBA

Presione enter para continuar...
```

Resultado del descifrado de EIPJECs HVVFT con la clave SECRETO.

4. Descifrado de un mensaje con la variante del algoritmo



```
C:\Users\asgas\Desktop\Project2\Debug\Project2.exe
-CIFRADO DE MENSAJES USANDO MATRICES-
Ingrese la opcion a realizar:
1) Ingresar mensaje y clave para generar criptograma
2) Ingresar mensaje y clave para generar criptograma (variante algoritmo)
3) Ingresar criptograma y clave para descifrar mensaje
4) Ingresar criptograma y clave para descifrar mensaje (variante algoritmo)
5) Ingresar criptograma largo para deducir el mensaje
--Ingresar otra opcion cerrara el programa--
4
Ingrese mensaje cifrado:
EIPJECs BVHNBj
Ingrese la clave:
SECRETO
Mensaje descifrado con variante: MENSAJE PRUEBA

Presione enter para continuar...
```

Resultado del descifrado con variante de EIPJECs BVHNBj con la clave SECRETO.

5. Proceso de deducción de un mensaje

Para el proceso de deducción de un mensaje se solicita que ingrese un criptograma, con el texto ingresado se hará el cálculo de la frecuencia de aparición de cada carácter para que pueda ser comparado con las frecuencias de aparición que se tiene en el idioma español.

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%

Para finalizar el programa, puede presionar en cualquier momento el botón que contiene una x en la parte superior derecha, así como, desde el menú principal, ingresar un número o un caracter que no esté listado en las opciones. Los demás botones funcionan para minimizar y maximizar la ventana, - y □, respectivamente.



Ubicación del botón de cerrar (x).