

MANUAL DE USUARIO

MENÚ

EN EL PROGRAMA EXISTEN 3 MENÚS. EL MENÚ PRINCIPAL, EL MENÚ DE ENCRIPCIÓN Y EL DE ENVIAR REPORTES.

MENÚ PRINCIPAL

HAY CUATRO OPCIONES, EN LAS QUE PARA ELEGIR UNA DEBE PRESIONARSE EL NÚMERO DE LA OPCIÓN QUE SE DESEA EXPLORAR.

```
Menú
1. Encriptar
2. Desencriptar
3. Ataque Con Texto Claro
4. Generar Reportes
5. Salir
Elija una opción:
```

1. MENÚ ENCRIPtar

HAY CUATRO OPCIONES, EN LAS QUE PARA ELEGIR UNA DEBE PRESIONARSE EL NÚMERO DE LA OPCIÓN QUE SE DESEA EXPLORAR.

Menú	Menú Encriptar
1. Encriptar	1. Ingreso Mensaje
2. Desencriptar	2. Ingreso Matriz Clave A
3. Ataque Con Texto Claro	3. Ingreso Matriz Clave B
4. Generar Reportes	4. Encriptar
5. Salir	5. Volver
Elija una opción: 1	Elija una opción:

1.1. INGRESO DE MENSAJE

SE INGRESA UN MENSAJE MEDIANTE EL TECLADO, PARA POSTERIORMENTE ENCRIPtarLO.

Menú Encriptar	
1. Ingreso Mensaje	
2. Ingreso Matriz Clave A	
3. Ingreso Matriz Clave B	Ingrese el mensaje: Hola Mundo
4. Encriptar	El mensaje fue guardado exitosamente
5. Volver	
Elija una opción: 1	

1.2. INGRESO DE LA MATRIZ CLAVE A Y B

SE INGRESARÁN LAS RUTAS DE DOS MATRICES. LA CANTIDAD DE ELEMENTOS DE B ES LA MISMA QUE LA DE LETRAS QUE CONFORMAN EL MENSAJE. ESTAS MATRICES SE USARÁN PARA ENCRIPtar EL MENSAJE.

Menú Encriptar	Menú Encriptar	
1. Ingreso Mensaje	1. Ingreso Mensaje	Ingrese la ruta de matriz clave A: matrizA.txt
2. Ingreso Matriz Clave A	2. Ingreso Matriz Clave A	Clave A guardada
3. Ingreso Matriz Clave B	3. Ingreso Matriz Clave B	
4. Encriptar	4. Encriptar	Ingrese la ruta de matriz clave B: matrizB.txt
5. Volver	5. Volver	Clave B guardada
Elija una opción: 2	Elija una opción: 3	

1.3. ENCRIPtar

CODIFICARÁ Y ENCRIPtarÁ EL MENSAJE PARA QUE NO SEA LEGIBLE.

```
Menú Encriptar
1. Ingreso Mensaje
2. Ingreso Matriz Clave A
3. Ingreso Matriz Clave B
4. Encriptar
5. Volver
Elija una opción: 4
```

Mensaje Encriptado											
179	76	503	245	50	677	136	164	347	388	180	1083

2. DESENCRIPTAR

SE REALIZARÁ UN PROCESO INVERSO AL DE LA ENCRIPtACIÓN, ES DECIR SE DESENCRIPTARÁ Y LUEGO SE DECODIFICARÁ PARA VER EL MENSAJE ORIGINAL.

```
Menú
1. Encriptar
2. Desencriptar
3. Ataque Con Texto Claro
4. Generar Reportes
5. Salir
Elija una opción: 2
```

Mensaje Desencriptado: hola mundo

4. MENÚ DE REPORTES

HAY DOS OPCIONES PARA REPORTES, REPORTE DE ENCRIPtACION Y DESENCRIPTACIÓN.

Menú	Menú Reportes
1. Encriptar	1. Reporte Encriptacion
2. Desencriptar	2. Reporte Desencriptacion
3. Ataque Con Texto Claro	3. Volver
4. Generar Reportes	Elija una opción:
5. Salir	
Elija una opción: 4	

4.1. REPORTE DE ENCRIPtACION

ENVÍA EL PROCEDIMIENTO REALIZADO AL CODIFICAR Y ENCRIPtar EL MENSAJE INGRESADO A UN ARCHIVO EN FORMATO HTML.

```
Menú Reportes
1. Reporte Encriptacion
2. Reporte Desencriptacion
3. Volver
Elija una opción: 1

;Reporte Enviado!
```

4.2. REPORTE DE ENCRIPtACION

ENVÍA EL PROCEDIMIENTO REALIZADO AL DESENCRIPTAR Y DECODIFICAR EL MENSAJE INGRESADO A UN ARCHIVO EN FORMATO HTML.

```
Menú Reportes
1. Reporte Encriptacion
2. Reporte Desencriptacion
3. Volver
Elija una opción: 2

;Reporte Enviado!
```

REPORTES

REPORTE DE ENCRYPTACIÓN.

Encriptacion del Mensaje

Se ingreso un mensaje por teclado, cada letra sera sustituida por un numero comenzando en a = 0 hasta llegar a z = 26, y el espacio u otro caracter diferente a los alfabeticos se sustituiria por 27. Cada caracter del mensaje se ordenara en una matriz de 3 filas por n columnas, la matriz sera llenada por columnas. Tambien se ingreso dos matrices clave.

El mensaje ingresado es: Hola Mundo

Matriz Textual Del Mensaje									
H		a				u			o
o						n			
I			M			d			

Para poder encriptar el mensaje se debe hacer la sustitucion de las letras, sin importar si son mayasculas o minusculas, por sus respectivos numeros.

Codigo									
A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	Ñ	O	P	Q	R	S
10	11	12	13	14	15	16	17	18	19
T	U	V	W	X	Y	Z	Espacio/Caracter		
20	21	22	23	24	25	26	27		

Lo que se requiere para encriptar el mensaje es lo siguiente:

1. Matriz M Del Mensaje
2. Matriz Clave A
3. Matriz Clave B

Matriz M Del Mensaje									
7		0			21			15	
15			27		13			27	
11			12		3			27	

Matriz Clave A									
2			5				8		
7				1				1	
4				15				22	

Matriz Clave B			
2	14	5	7
1	11	1	21
8	8	2	24

Procedimiento:
 1. Multiplicar los elementos de cada fila de la Matriz Clave A por los elementos de cada columna de la Matriz M del Mensaje, y sumar los productos para encontrar cada elemento de la nueva matriz.
 Ecuacion: $\sum(A_{ik} \times M_{kj}) = AM_{ij}$

Matriz AM			
$(2)(7) + (5)(15) + (8)(11) = 177$	$(2)(0) + (5)(27) + (8)(12) = 231$	$(2)(21) + (5)(13) + (8)(3) = 131$	$(2)(15) + (5)(27) + (8)(27) = 381$
$(7)(7) + (1)(15) + (1)(11) = 75$	$(7)(0) + (1)(27) + (1)(12) = 39$	$(7)(21) + (1)(13) + (1)(3) = 163$	$(7)(15) + (1)(27) + (1)(27) = 159$
$(4)(7) + (15)(15) + (22)(11) = 495$	$(4)(0) + (15)(27) + (22)(12) = 669$	$(4)(21) + (15)(13) + (22)(3) = 345$	$(4)(15) + (15)(27) + (22)(27) = 1059$

2. Sumar cada elemento de la Matriz AM con los correspondientes elementos de la Matriz Clave B.

Matriz AM + B = C			
$177 + 2 = 179$	$231 + 14 = 245$	$131 + 5 = 136$	$381 + 7 = 388$
$75 + 1 = 76$	$39 + 11 = 50$	$163 + 1 = 164$	$159 + 21 = 180$
$495 + 8 = 503$	$669 + 8 = 677$	$345 + 2 = 347$	$1059 + 24 = 1083$

El mensaje encriptado es:
 179 76 503 245 50 677 136 164 347 388 180 1083

Generado: Sat Feb 13 19:25:40 CST 2021

REPORTE DESENCRIPTACION

REPORTE DE DESENCRIPTACIÓN.

Desencrptacion del Mensaje

Se usaran las mismas Matrices Clave, el mismo codigo de letras a numeros y ahora la Matriz C.

Matriz C			
179	245	136	388
76	50	164	180
503	677	347	1083

Matriz Clave A			
2	5	8	
7	1	1	
4	15	22	

Matriz Clave B			
2	14	5	7
1	11	1	21
8	8	2	24

Procedimiento:

1. Calcular el Determinante de la Matriz Clave A.

Determinante = $2 \cdot ((1)(22) - (1)(15)) - 5 \cdot ((7)(22) - (1)(4)) + 8 \cdot ((7)(15) - (1)(4)) = 72$

2. Obtener la Transpuesta de la Matriz Clave A.

Transpuesta A			
2	7	4	
5	1	15	
8	1	22	

3. Calcular la Adjunta de la Transpuesta A.

Adjunta A		
$(-1)^{0+0} \cdot ((1)(22) - (15)(1)) = 7$	$(-1)^{0+1} \cdot ((5)(22) - (15)(8)) = 10$	$(-1)^{0+2} \cdot ((5)(1) - (1)(8)) = -3$
$(-1)^{1+0} \cdot ((7)(22) - (4)(1)) = -150$	$(-1)^{1+1} \cdot ((2)(22) - (4)(8)) = 12$	$(-1)^{1+2} \cdot ((2)(1) - (7)(8)) = 54$
$(-1)^{2+0} \cdot ((7)(15) - (4)(1)) = 101$	$(-1)^{2+1} \cdot ((2)(15) - (4)(5)) = -10$	$(-1)^{2+2} \cdot ((2)(1) - (7)(5)) = -33$

4. Calcular la Inversa de Matriz Clave A.

Ecuacion:

$$A^{-1} = \frac{Adj A}{det A}$$

Inversa de A o A ⁻¹		
$\frac{7}{72}$	$\frac{10}{72}$	$\frac{-3}{72}$
$\frac{-150}{72}$	$\frac{12}{72}$	$\frac{54}{72}$
$\frac{101}{72}$	$\frac{-10}{72}$	$\frac{-33}{72}$

5. Calcular C - B

Matriz C - B			
179 - 2 = 177	245 - 14 = 231	136 - 5 = 131	388 - 7 = 381
76 - 1 = 75	50 - 11 = 39	164 - 1 = 163	180 - 21 = 159
503 - 8 = 495	677 - 8 = 669	347 - 2 = 345	1083 - 24 = 1059

6. Multiplicar A⁻¹ por C - B.

Matriz A ⁻¹ (C - B) = M			
$\frac{(7)(177)}{72} + \frac{(10)(75)}{72} + \frac{(-3)(495)}{72} = 7$	$\frac{(7)(231)}{72} + \frac{(10)(39)}{72} + \frac{(-3)(669)}{72} = 0$	$\frac{(7)(131)}{72} + \frac{(10)(163)}{72} + \frac{(-3)(345)}{72} = 21$	$\frac{(7)(381)}{72} + \frac{(10)(159)}{72} + \frac{(-3)(1059)}{72} = 15$
$\frac{(-150)(177)}{72} + \frac{(12)(75)}{72} + \frac{(54)(495)}{72} = 15$	$\frac{(-150)(231)}{72} + \frac{(12)(39)}{72} + \frac{(54)(669)}{72} = 27$	$\frac{(-150)(131)}{72} + \frac{(12)(163)}{72} + \frac{(54)(345)}{72} = 13$	$\frac{(-150)(381)}{72} + \frac{(12)(159)}{72} + \frac{(54)(1059)}{72} = 27$
$\frac{(101)(177)}{72} + \frac{(-10)(75)}{72} + \frac{(-33)(495)}{72} = 11$	$\frac{(101)(231)}{72} + \frac{(-10)(39)}{72} + \frac{(-33)(669)}{72} = 12$	$\frac{(101)(131)}{72} + \frac{(-10)(163)}{72} + \frac{(-33)(345)}{72} = 3$	$\frac{(101)(381)}{72} + \frac{(-10)(159)}{72} + \frac{(-33)(1059)}{72} = 27$

7. Sustituir los numeros por sus respectivas letras para descubrir el mensaje

Matriz M			
h	a	u	o
o		n	
l	m	d	

El mensaje desencriptado es:

h o l a m u n d o