

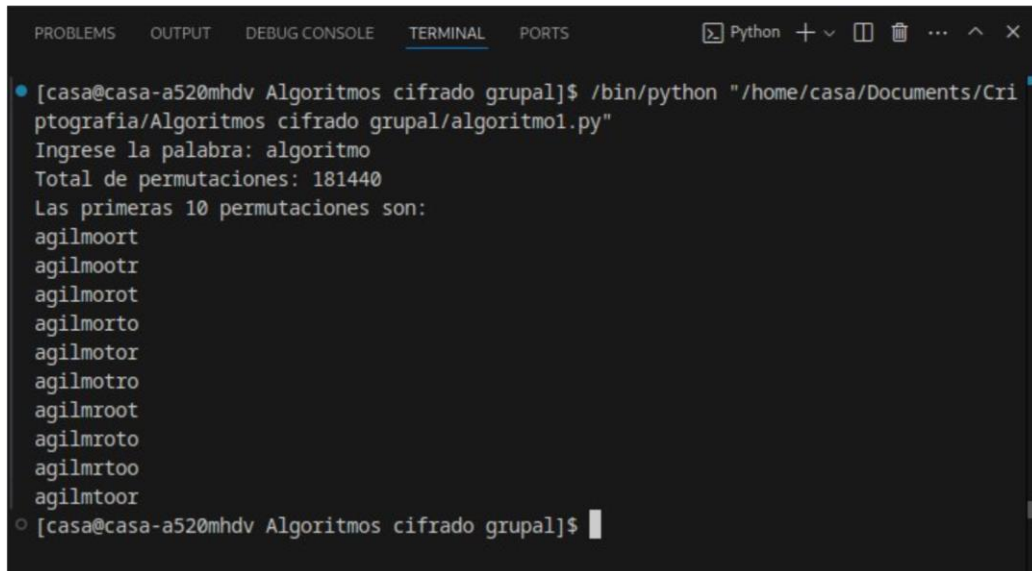
Universidad Central del Ecuador
Carrera de Computación
Criptografía y Seguridad de la Información



Tema: Tarea03-U1-G05
Resultados de Ejecución de Algoritmos
Criptográficos Básicos

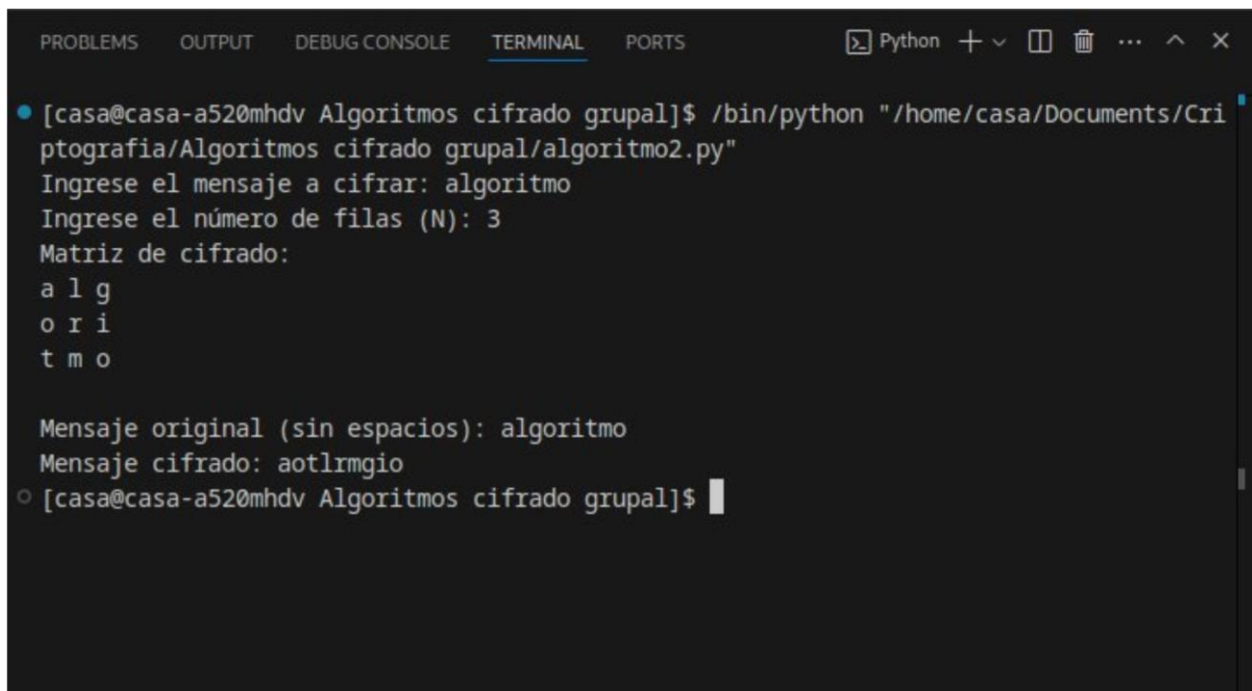
Integrantes:
Pineda Marco
Ramírez Leonardo
Vinueza Edlith

1. Algoritmo que escriba todas las permutaciones posibles de una palabra de longitud n SIN espacios (Anagrama). La palabra se ingresa al iniciar el algoritmo. El algoritmo debe mostrar el número total de permutaciones y las 10 primeras ordenadas alfabéticamente.



```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS Python + - [ ] [ ] ... ^ X
[casa@casa-a520mhdv Algoritmos cifrado grupal]$ /bin/python "/home/casa/Documents/Criptografia/Algoritmos cifrado grupal/algoritmo1.py"
Ingrese la palabra: algoritmo
Total de permutaciones: 181440
Las primeras 10 permutaciones son:
agilmoort
agilmootr
agilmorot
agilmorto
agilmotor
agilmotro
agilmroot
agilmroto
agilmrtoo
agilmtoor
[casa@casa-a520mhdv Algoritmos cifrado grupal]$
```

2. Algoritmo que realice el cifrado de un mensaje por permutación de filas, teniendo como clave n filas. Tanto n como el texto del mensaje se ingresan al iniciar el algoritmo. El algoritmo debe controlar que el número de caracteres del mensaje (sin espacios), sea menor o igual que $n \times n$. Imprima la matriz de cifrado, el mensaje original y el mensaje cifrado. Si en la matriz de cifrado sobran espacios para almacenar los caracteres del mensaje original, estos deben llenarse con "*".



```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS Python + - [ ] [ ] ... ^ X
[casa@casa-a520mhdv Algoritmos cifrado grupal]$ /bin/python "/home/casa/Documents/Criptografia/Algoritmos cifrado grupal/algoritmo2.py"
Ingrese el mensaje a cifrar: algoritmo
Ingrese el número de filas (N): 3
Matriz de cifrado:
a l g
o r i
t m o

Mensaje original (sin espacios): algoritmo
Mensaje cifrado: aotlrmgio
[casa@casa-a520mhdv Algoritmos cifrado grupal]$
```

3. Algoritmo que realice el cifrado de un mensaje por permutación de columnas, teniendo como clave n columnas. Tanto n como el texto del mensaje se ingresan al iniciar el algoritmo. El algoritmo debe controlar que el número de caracteres del mensaje (sin espacios), sea menor o igual que $n \times n$. Imprima la matriz de cifrado, el mensaje original y el mensaje cifrado. Si en la matriz de cifrado sobran espacios para almacenar los caracteres del mensaje original, estos deben llenarse con "*".

```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS Python + - [ ] [ ] ... ^ X

• [casa@casa-a520mhdv Algoritmos cifrado grupal]$ /bin/python "/home/casa/Documents/Cri
ptografia/Algoritmos cifrado grupal/algoritmo3.py"
Ingrese el número de columnas (n): 3
Ingrese el mensaje a cifrar: algoritmo
Matriz de cifrado:
a l g
o r i
t m o
Mensaje original: algoritmo
Mensaje cifrado: aotlrmgio
○ [casa@casa-a520mhdv Algoritmos cifrado grupal]$
```

4. Algoritmo que realice el cifrado de una cadena de caracteres mediante un método de sustitución Monoalfabético de desplazamiento n caracteres a la derecha. Tanto la palabra como el valor de n se ingresan al iniciar el algoritmo. El algoritmo debe mostrar el alfabeto original, el alfabeto cifrado, la cadena de caracteres ingresada y su resultado.

```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS Python + - [ ] [ ] ... ^ X

• [casa@casa-a520mhdv Algoritmos cifrado grupal]$ /bin/python "/home/casa/Documents/Cri
ptografia/Algoritmos cifrado grupal/algoritmo4.py"
Seleccione un alfabeto:
1. Alfabeto en español
2. Alfabeto en inglés
3. Alfabeto en francés
4. Alfabeto en alemán
5. Ingresar un alfabeto personalizado
Ingrese el número de la opción deseada: 2
Ingrese el valor de desplazamiento (n): 3
Ingrese el mensaje a cifrar: algortimo
RESULTADOS
Alfabeto original: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Alfabeto cifrado: DEFGHIJKLMNOPQRSTUVWXYZABC
Cadena original: algortimo
Cadena cifrada: DOJRUWLPR
○ [casa@casa-a520mhdv Algoritmos cifrado grupal]$
```

5. Algoritmo que realice el cifrado de una cadena de caracteres mediante un método de sustitución Polialfabético de Vigenère. La cadena se ingresa al iniciar el algoritmo. El algoritmo debe mostrar la cadena de caracteres ingresada, la clave de cifrado y la cadena de caracteres cifrada.

```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS Python + v [ ] [ ] ... ^ x
• [casa@casa-a520mhdv Algoritmos cifrado grupal]$ /bin/python "/home/casa/Documents/Criptografia/Algoritmos cifrado grupal/algoritmo5.py"
Texto de entrada
algotimo
-----
Llave de cifrado
key
-----
Entrada preparada
algotimo
-----
Texto cifrado
kpeyxgws
-----
Texto descifrado
algotimo
-----
○ [casa@casa-a520mhdv Algoritmos cifrado grupal]$
```

6. Algoritmo que realice el cifrado de una cadena de caracteres utilizando la siguiente tabla de cifrado:

*	A	S	D	F	G
Q	a	b	c	d	e
W	f	g	h	i	j
E	k	l	m	n	o
R	p	q	r	s	t
T	u	v	x	y	z

La cadena de caracteres se ingresa al iniciar el programa. Si algún carácter del texto no existe en la matriz, coloque "**". Imprima la matriz de cifrado, el mensaje original y el mensaje cifrado.

```
• [casa@casa-a520mhdv Algoritmos cifrado grupal]$ /bin/python "/home/casa/Documents/Criptografia/Algoritmos cifrado grupal/algoritmo6.py"
Texto de entrada: alworitmo12
Texto de entrada:
alworitmo12
-----
Texto limpio:
al*oritmo**
-----
Tabla de cifrado:
['*', 'A', 'S', 'D', 'F', 'G']
['Q', 'a', 'b', 'c', 'd', 'e']
['W', 'f', 'g', 'h', 'i', 'j']
['E', 'k', 'l', 'm', 'n', 'o']
['R', 'p', 'q', 'r', 's', 't']
['T', 'u', 'v', 'x', 'y', 'z']
-----
Texto de salida:
QAES**EGRDWFRGEDEG****
-----
Texto de descifrado:
al*oritmo**
-----
○ [casa@casa-a520mhdv Algoritmos cifrado grupal]$
```