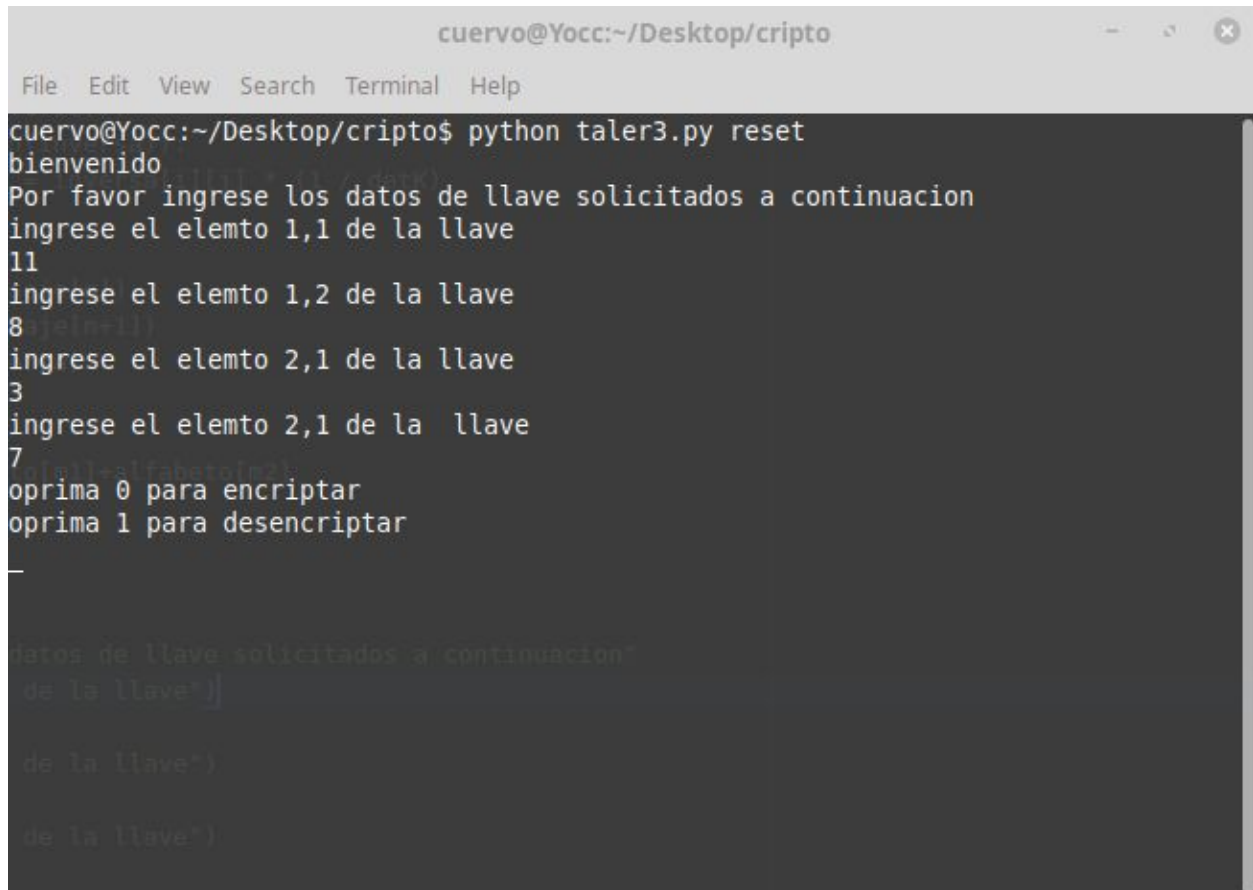


Taller 3 Introducción a la criptografía

Yonatan Orlando Cuervo Camargo

Algoritmo de Hill

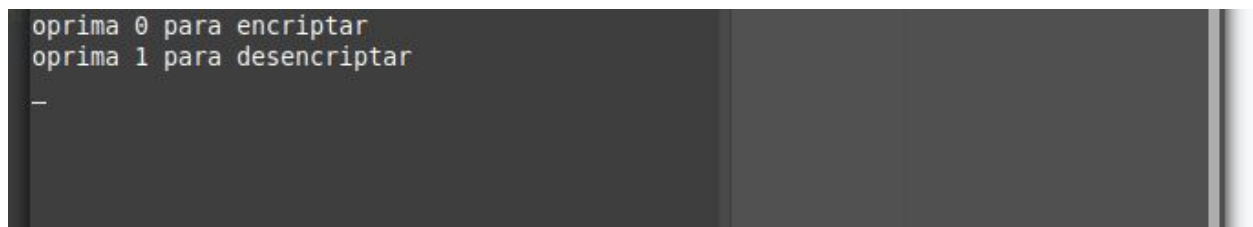
El programa al ejecutarse lo primero que pide es la llave, ya que esta es la misma para encriptar y desencriptar.



```
cuervo@Yocc:~/Desktop/cripto
File Edit View Search Terminal Help
cuervo@Yocc:~/Desktop/cripto$ python taler3.py reset
bienvenido
Por favor ingrese los datos de llave solicitados a continuacion
ingrese el elemto 1,1 de la llave
11
ingrese el elemto 1,2 de la llave
8
ingrese el elemto 2,1 de la llave
3
ingrese el elemto 2,1 de la llave
7
oprma 0 para encriptar
oprma 1 para desencriptar
_

datos de llave solicitados a continuacion"
de la llave"]
de la llave")
de la llave")
```

Posteriormente muestra un menú donde se puede seleccionar si se desea encriptar o desencriptar.



```
oprma 0 para encriptar
oprma 1 para desencriptar
_
```

Al seleccionar 0 con la llave ingresada y como mensaje “JULY” encripta el mensaje como “delw”

```
cuervo@Yocc:~/Desktop/cripto
File Edit View Search Terminal Help
cuervo@Yocc:~/Desktop/cripto$ python taler3.py reset
bienvenido
Por favor ingrese los datos de llave solicitados a continuacion
ingrese el elemto 1,1 de la llave
11
ingrese el elemto 1,2 de la llave
8
ingrese el elemto 2,1 de la llave
3 se puede seleccionar si se desea encriptar o
ingrese el elemto 2,1 de la llave
7
oprma 0 para encriptar
oprma 1 para desencriptar
0
ingrese el mensaje a codificar
july
delw
cuervo@Yocc:~/Desktop/cripto$ _
```

Al ingresar 1 en menú y como mensaje “delw” muestra el mensaje “july” en texto claro

```
cuervo@Yocc:~/Desktop/cripto
File Edit View Search Terminal Help
cuervo@Yocc:~/Desktop/cripto$ python taler3.py reset
bienvenido
Por favor ingrese los datos de llave solicitados a continuacion
ingrese el elemto 1,1 de la llave
11
ingrese el elemto 1,2 de la llave
8
ingrese el elemto 2,1 de la llave
3
ingrese el elemto 2,1 de la llave
7
oprma 0 para encriptar
oprma 1 para desencriptar
1
ingrese el mensaje a decodificar
delw
july
cuervo@Yocc:~/Desktop/cripto$ _
```

Al Ingresar el texto cifrado "VKFZRVTIAZSMISGKA" da en texto claro numbertheoryiseasy

```
cuervo@Yocc:~/Desktop/cripto
File Edit View Search Terminal Help
cuervo@Yocc:~/Desktop/cripto$ python taler3.py
bienvenido
Por favor ingrese los datos de llave solicitados a continuacion
ingrese el elemto 1,1 de la llave
11
ingrese el elemto 1,2 de la llave
8
ingrese el elemto 2,1 de la llave
3
ingrese el elemto 2,1 de la llave
7
oprime 0 para encriptar
oprime 1 para desencriptar
1
ingrese el mensaje a decodificar
VKFZRVTIAZSMISGKA
numbertheoryiseasy
cuervo@Yocc:~/Desktop/cripto$
```

En caso de ingresar una matriz sin inversa el program mostrar un mensaje de error y se detendrá

```
cuervo@Yocc:~/Desktop/cripto
File Edit View Search Terminal Help
cuervo@Yocc:~/Desktop/cripto$ python taler3.py
bienvenido
Por favor ingrese los datos de llave solicitados a continuacion
ingrese el elemto 1,1 de la llave
30
ingrese el elemto 1,2 de la llave
4
ingrese el elemto 2,1 de la llave
30
ingrese el elemto 2,1 de la llave
4
oprime 0 para encriptar
oprime 1 para desencriptar
1
ingrese el mensaje a decodificar
sad
Matriz no inverible
cuervo@Yocc:~/Desktop/cripto$ _
```