

UNIVERSIDAD DON BOSCO
Seguridad de Redes
(SDR404 G03L)



Guía 3

INTEGRANTE:

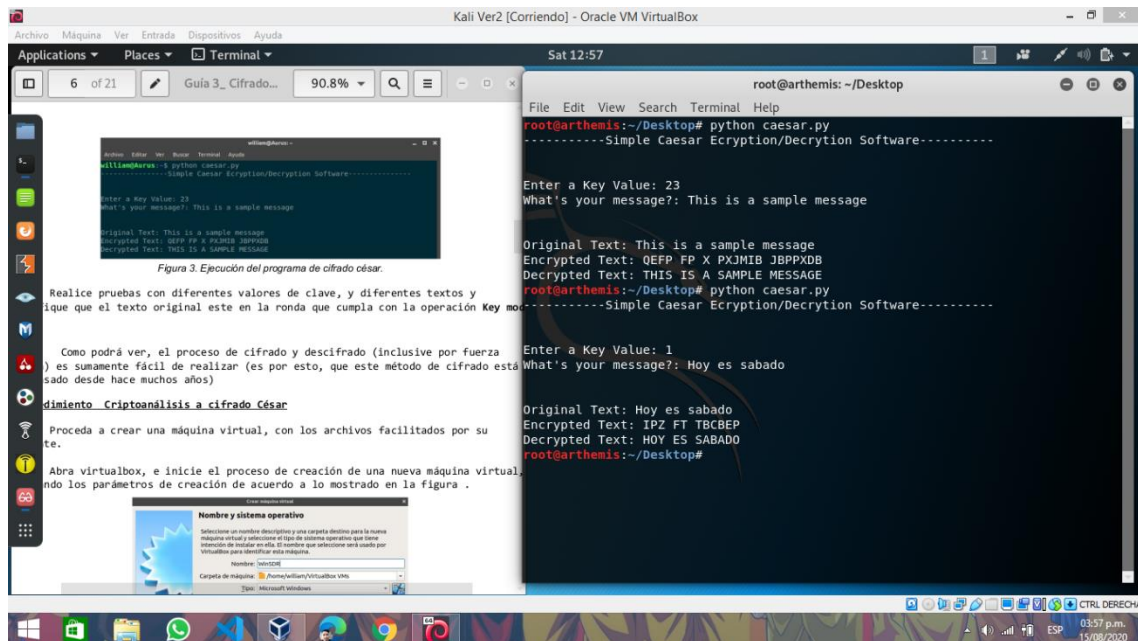
Apellidos	Nombres	Carné
Peñate Salazar	Carlos Eduardo	PS190756

DOCENTE:

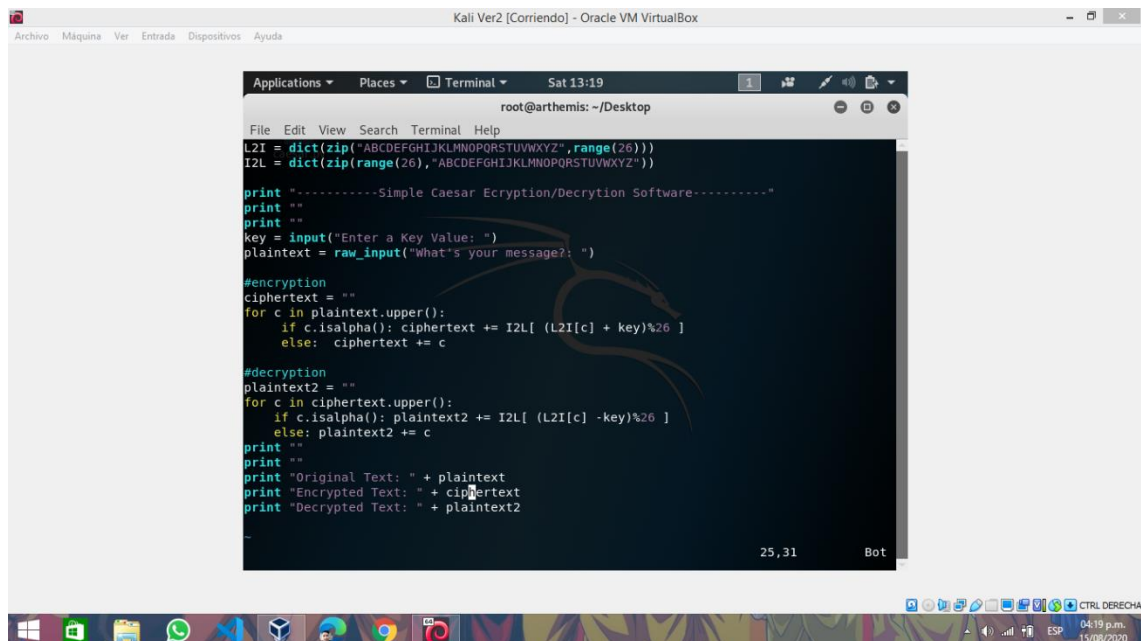
Nelson Stanley Belloso Huevo

Parte 1

Captura 1

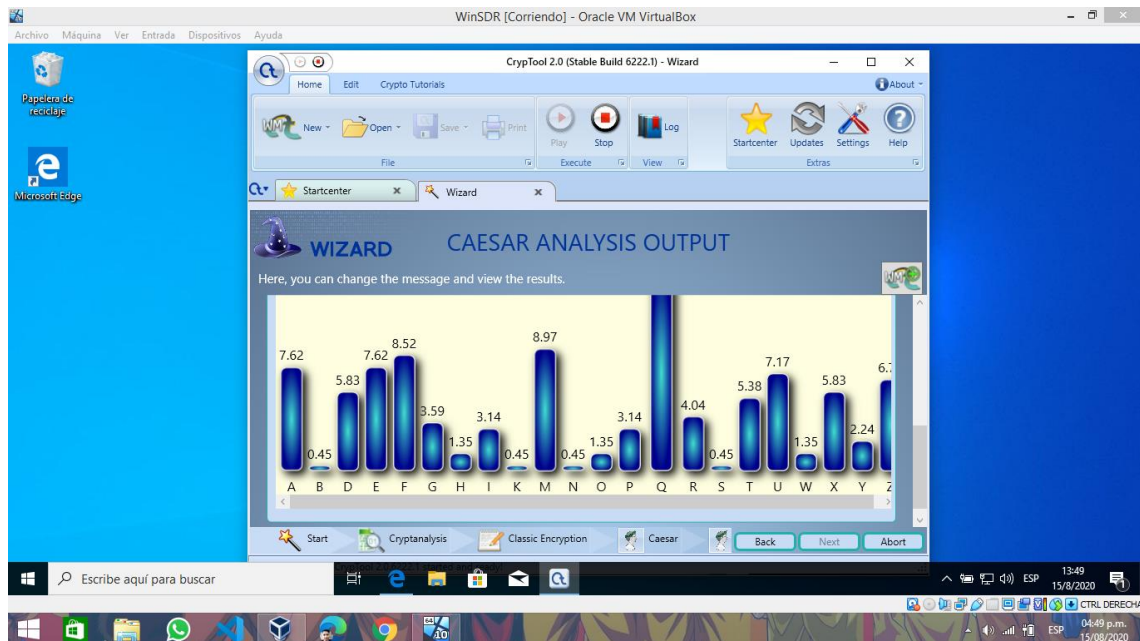


Captura 2

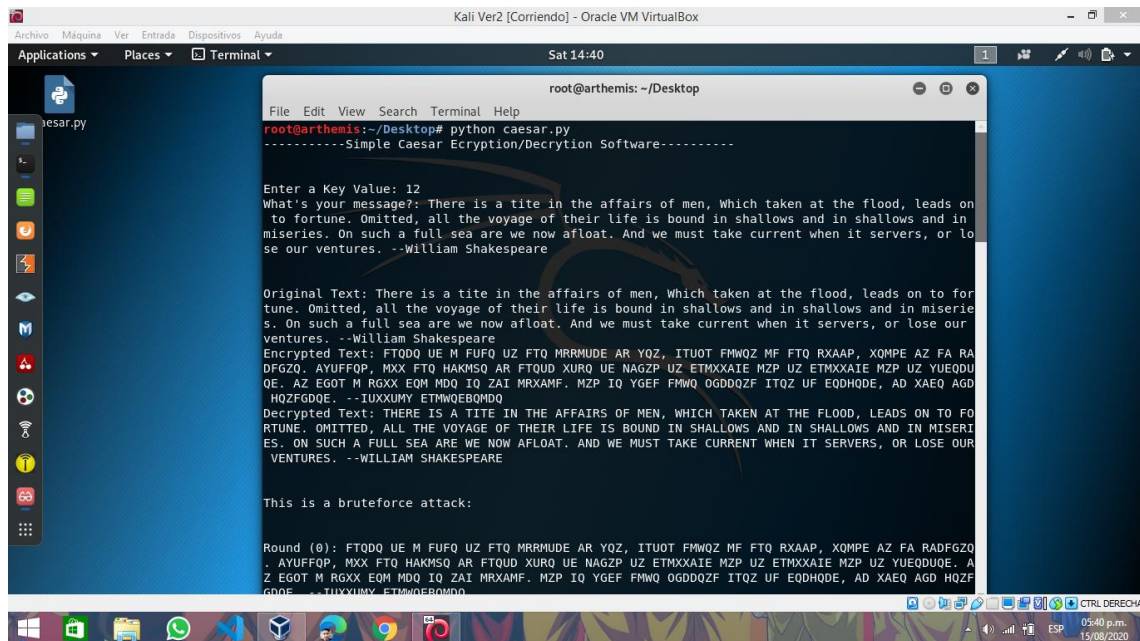


Parte 2

Captura 3

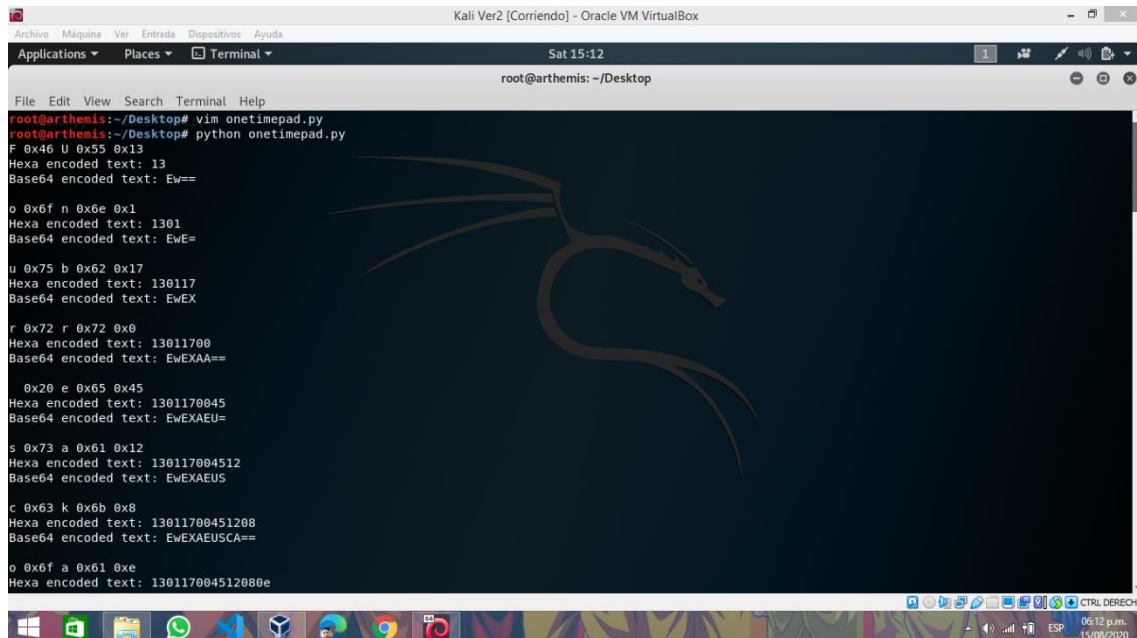


Captura 4



Parte 3

Captura 5



```
Kali Ver2 [Corriendo] - Oracle VM VirtualBox
Applications Places Terminal Sat 15:12
root@arthemis: ~/Desktop
File Edit View Search Terminal Help
root@arthemis:~/Desktop# vim onetimepad.py
root@arthemis:~/Desktop# python onetimepad.py
F 0x46 U 0x55 0x13
Hexa encoded text: 13
Base64 encoded text: Ew==

o 0x6f n 0x6e 0x1
Hexa encoded text: 1301
Base64 encoded text: EwE=

u 0x75 b 0x62 0x17
Hexa encoded text: 130117
Base64 encoded text: EwEX

r 0x72 r 0x72 0x0
Hexa encoded text: 13011700
Base64 encoded text: EwEXAA==

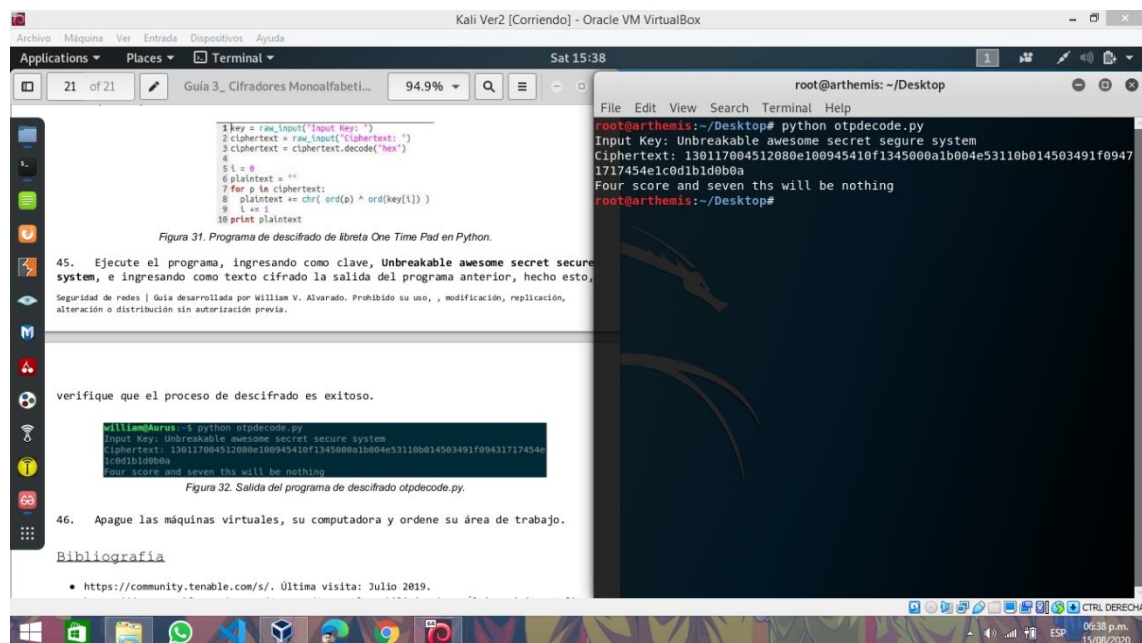
0x20 e 0x65 0x45
Hexa encoded text: 1301170045
Base64 encoded text: EwEXAEU=

s 0x73 a 0x61 0x12
Hexa encoded text: 130117004512
Base64 encoded text: EwEXAEUS

c 0x63 k 0x6b 0x8
Hexa encoded text: 13011700451208
Base64 encoded text: EwEXAEUSCA==

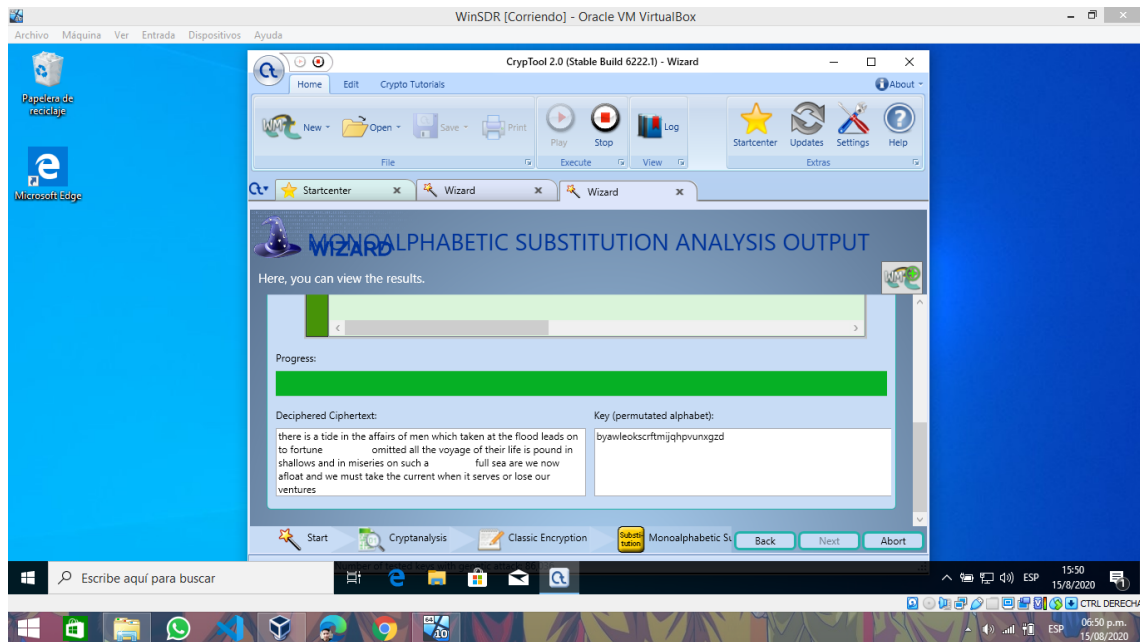
o 0x6f a 0x61 0xe
Hexa encoded text: 130117004512080e
```

Captura 6



```
Kali Ver2 [Corriendo] - Oracle VM VirtualBox
Applications Places Terminal Sat 15:38
21 of 21 Guía 3_ Cifradores Monoalfabeti... 94.9%
root@arthemis: ~/Desktop
File Edit View Search Terminal Help
root@arthemis:~/Desktop# python otpdecode.py
Input Key: Unbreakable awesome secret secure system
Ciphertext: 130117004512080e100945410f1345000a1b004e53110b014503491f0947
1717454e1c0d1b1d0b0a
Four score and seven ths will be nothing
root@arthemis:~/Desktop#
```

Captura 7



Análisis

Cifrado César: es uno de las más fáciles que puede haber y la forma de descryptar es la forma inversa de encriptar entonces sería fácil descryptar conociendo el Frecuencia o la llave. Pero si se analiza desde la fecha en que fue creado este método en Roma AC se puede percibir que los métodos de encriptación han avanzado bastante desde que se inventaron, al introducir la encriptación en sistemas operativos se ha revolucionado la forma de encriptar la información haciendo así cada vez más segura la información, al introducir el cifrado mono alfabético por sustitución y codificación a hexadecimal se pueden crear muchas formas y combinaciones para proteger la información.