



UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS DE QUIXADÁ

RELATÓRIO: LAB 07

QUIXADÁ
2022

Introdução:

Abaixo seguem as chaves em base64 como pedido.

Chave do arquivo chave.txt em base64:

MzYyMWY1MTY2NDBlOTY1MGY3ZDlmZDkyMjdhMTQwY2Q=

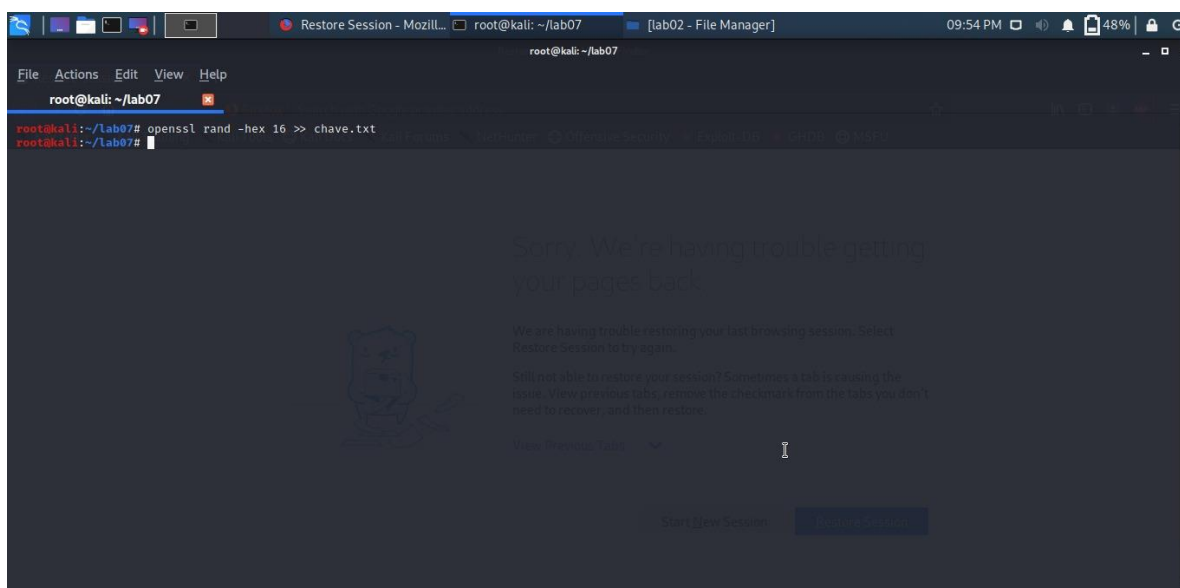
Chave 2 do arquivo chave2.txt em base64:

ZTQ1ODQ0NDBkNDY3OTY2MTAxZTQxZmFmMDg2NmI1MWI=

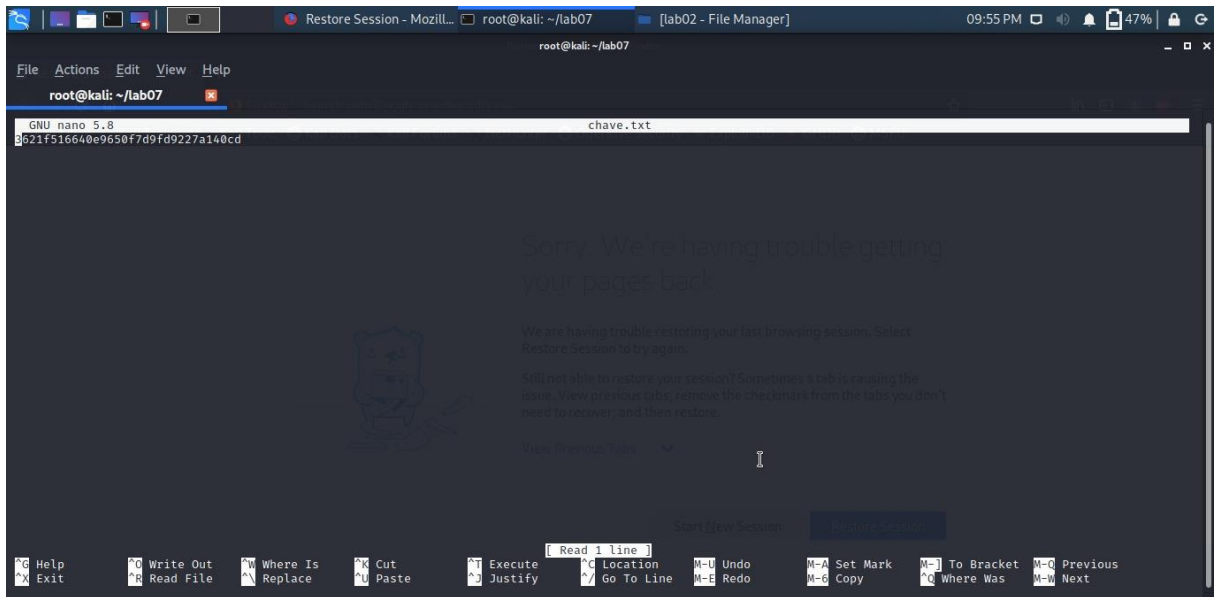
1 - Criação das chaves.

Criamos duas chaves para a realização da atividade, a primeira a ser criada foi uma de 128 bits que foi armazenada em um arquivo de nome **chave.txt**, utilizando o seguinte comando abaixo:

openssl rand -hex 16 >> chave.txt

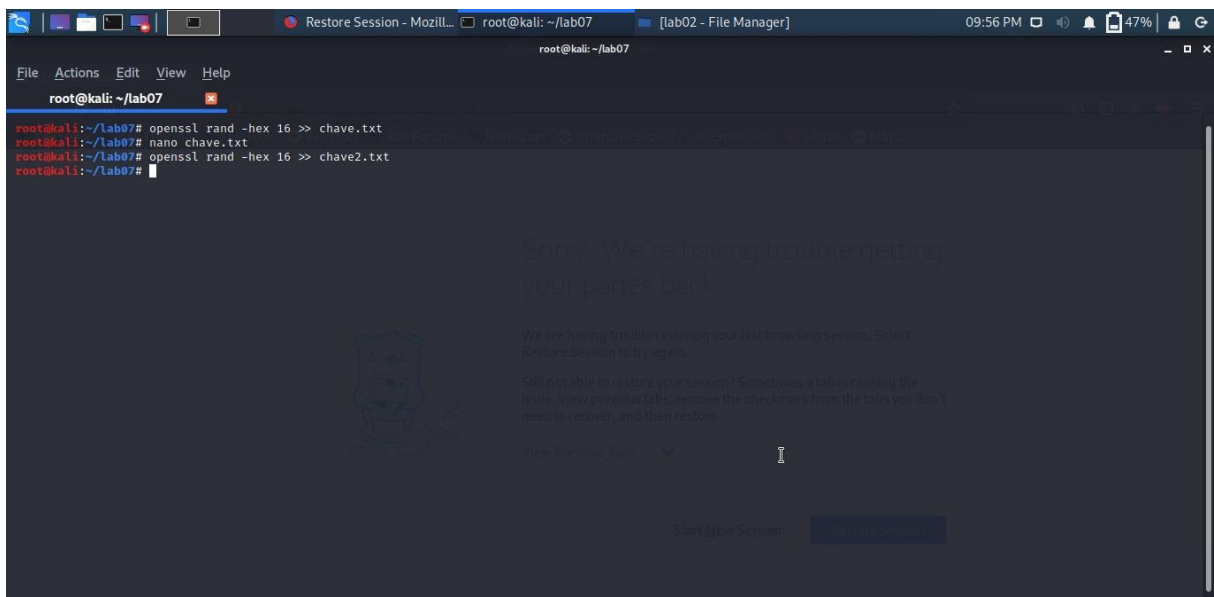


Abaixo podemos ver o conteúdo do arquivo:

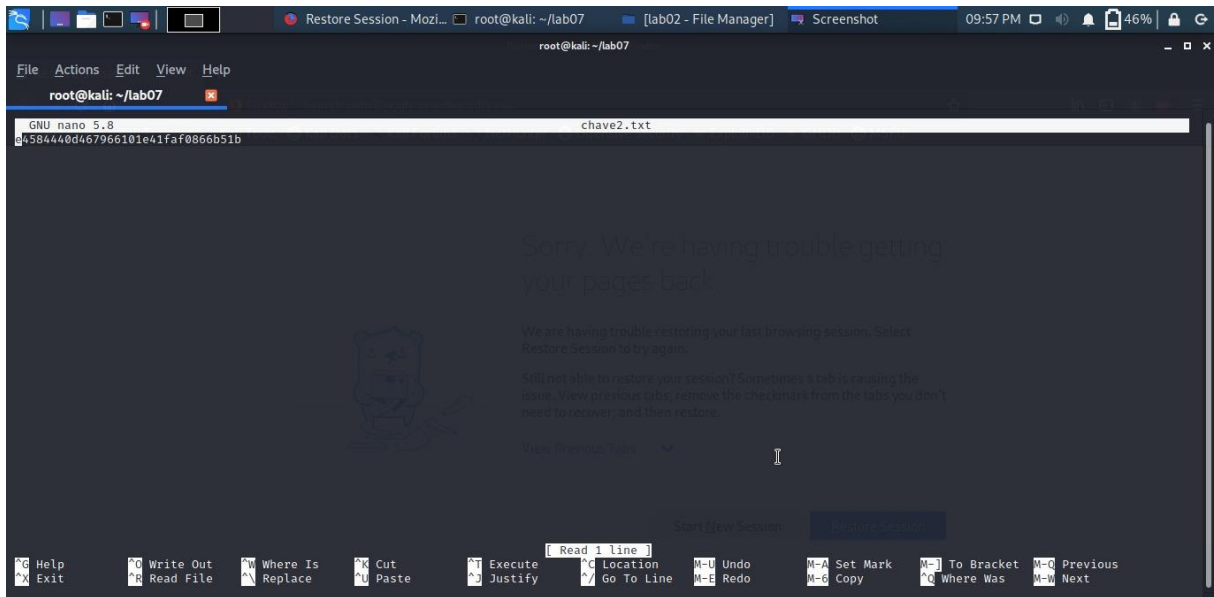


Criamos mais uma chave e armazenamos ela em um arquivo de nome chave2.txt utilizando o seguinte comando:

openssl rand -hex 16 >> chave2.txt

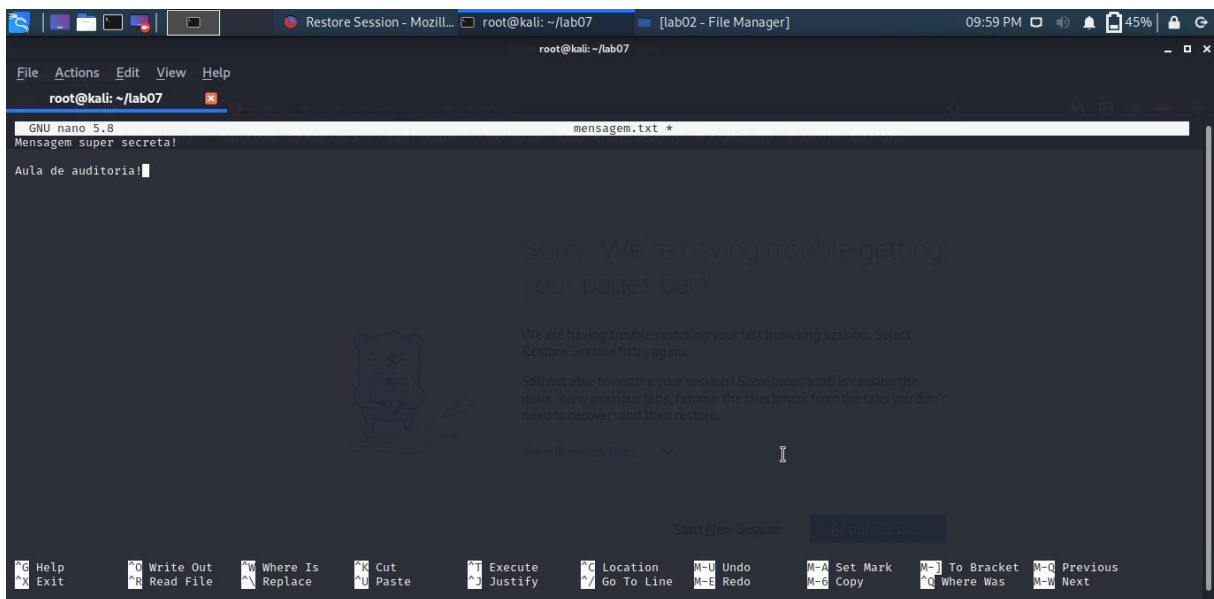


Abaixo o conteúdo do arquivo:



2 - Encriptando arquivos.

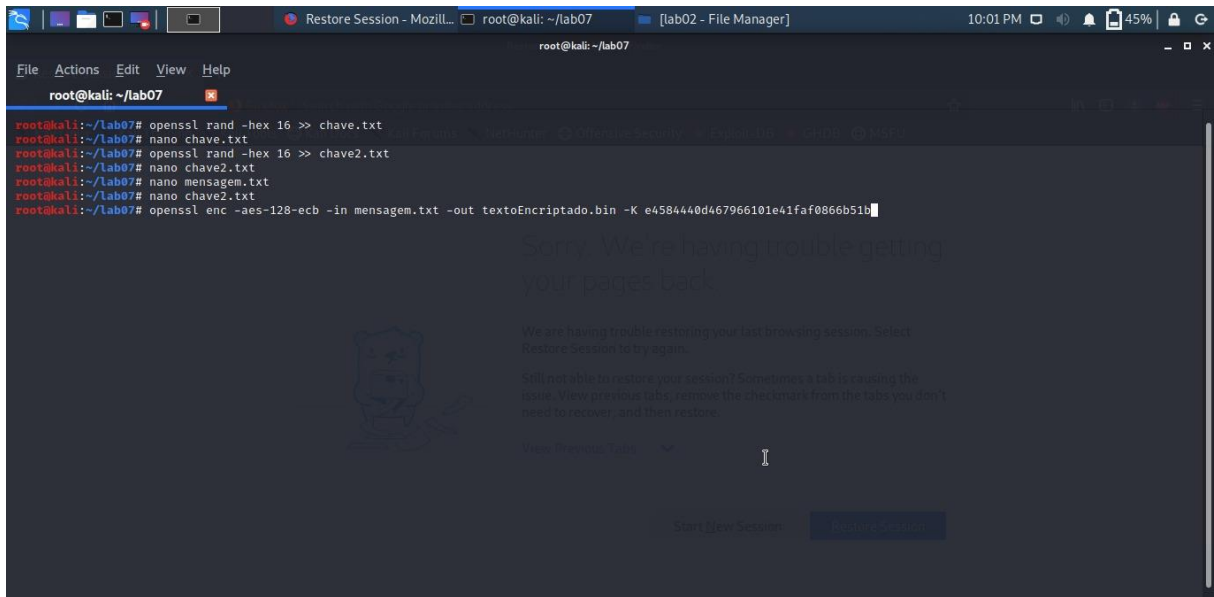
Criamos um arquivo de nome *mensagem.txt* contendo um pouco de texto para a realização dos nossos testes.



2.1 - Encriptar um arquivo de texto qualquer (exemplo) e uma das chaves criadas.

Encriptando o arquivo criado anteriormente a chave 2 usando o seguinte comando:

```
openssl enc -aes-128-ecb -in mensagem.txt -out textoEncriptado.bin -K  
e4584440d467966101e41faf0866b51b
```



The screenshot shows a terminal window with the following commands and output:

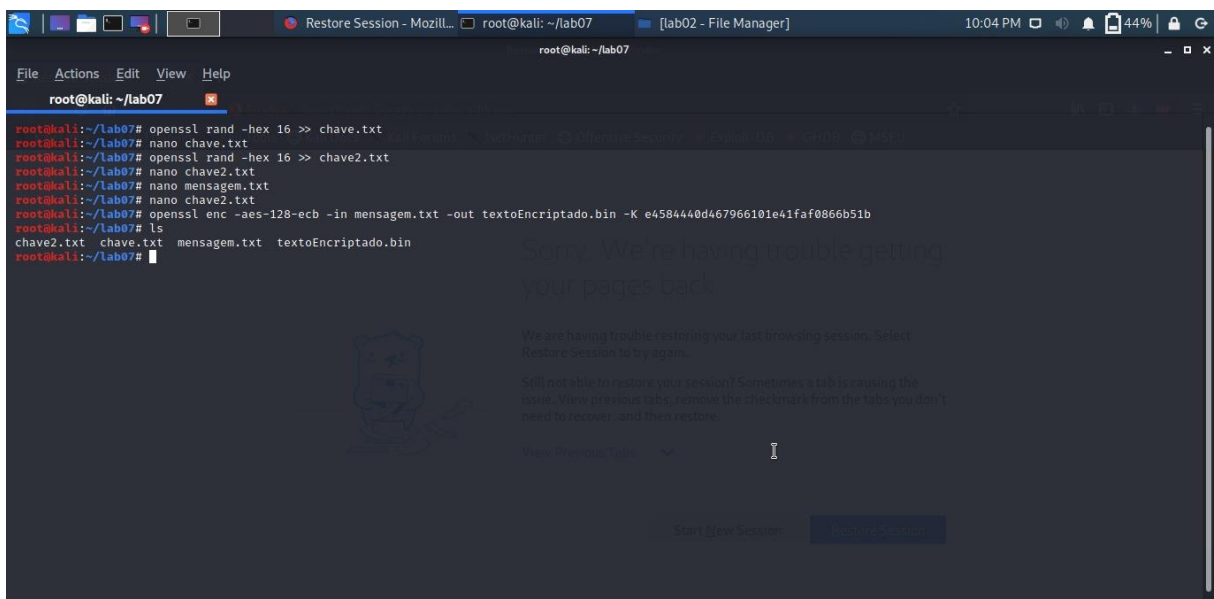
```

root@kali: ~/lab07
root@kali:~/lab07# openssl rand -hex 16 >> chave.txt
root@kali:~/lab07# nano chave.txt
root@kali:~/lab07# openssl rand -hex 16 >> chave2.txt
root@kali:~/lab07# nano chave2.txt
root@kali:~/lab07# nano mensagem.txt
root@kali:~/lab07# openssl enc -aes-128-ecb -in mensagem.txt -out textoEncriptado.bin -K e4584440d467966101e41faf0866b51b

```

The terminal output shows the successful execution of these commands, resulting in the creation of the file `textoEncriptado.bin`.

Abaixo podemos ver que foi criado um novo arquivo de nome *textoEncriptado.bin*



The screenshot shows a terminal window with the following commands and output:

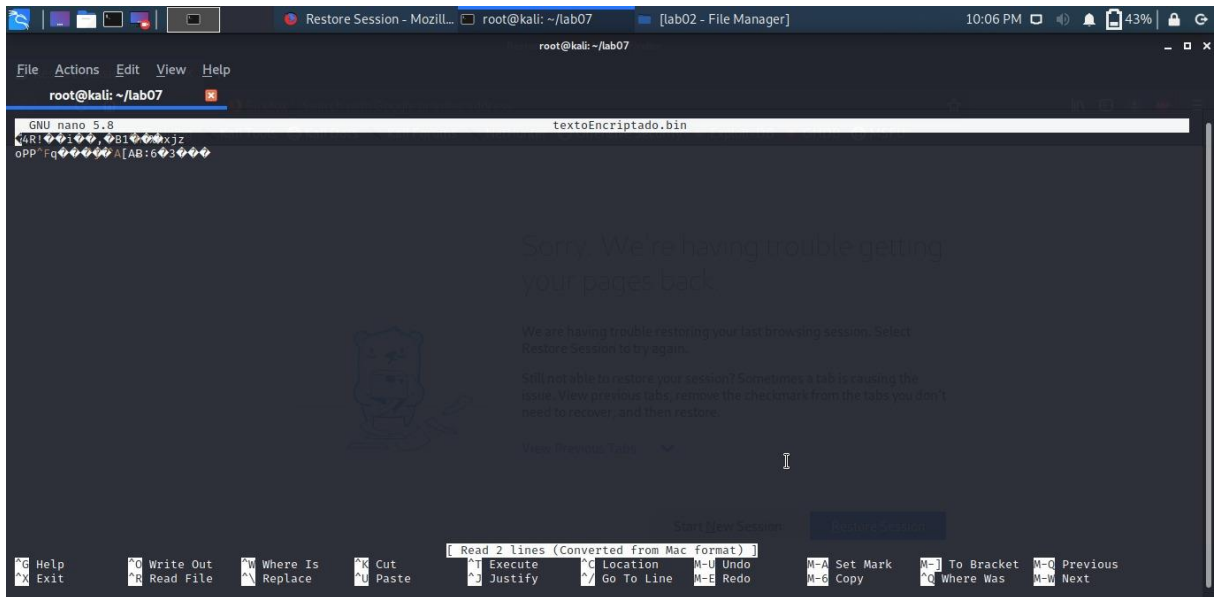
```

root@kali: ~/lab07
root@kali:~/lab07# openssl rand -hex 16 >> chave.txt
root@kali:~/lab07# nano chave.txt
root@kali:~/lab07# openssl rand -hex 16 >> chave2.txt
root@kali:~/lab07# nano chave2.txt
root@kali:~/lab07# nano mensagem.txt
root@kali:~/lab07# openssl enc -aes-128-ecb -in mensagem.txt -out textoEncriptado.bin -K e4584440d467966101e41faf0866b51b
root@kali:~/lab07# ls
chave2.txt  chave.txt  mensagem.txt  textoEncriptado.bin
root@kali:~/lab07#

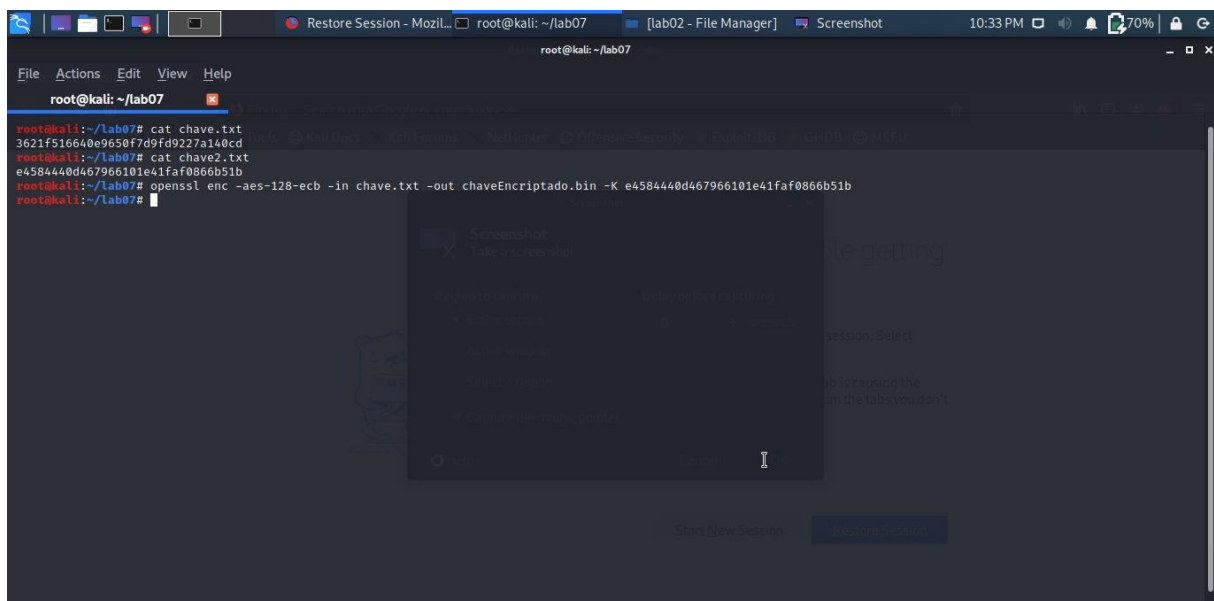
```

The terminal output shows the successful execution of these commands, resulting in the creation of the file `textoEncriptado.bin`. The `ls` command output confirms the presence of the file in the current directory.

Ao analisar o conteúdo do arquivo verifica-se que é impossível a leitura do arquivo:



Agora vamos encriptar o arquivo que contém a *chave.txt* usando a chave do arquivo *chave2.txt*



2.2 - Decriptar o texto utilizando diferentes chaves e analisar o resultado.

Ao decriptar o arquivo usando o comando abaixo e a chave 2 é possível ver que um arquivo de nome *textoClaro.txt*

```
openssl enc -aes-128-ecb -in textoEncriptado.bin -out textoClaro.txt -K  
e4584440d467966101e41faf0866b51b -d
```

```

root@kali: ~/lab07
File Actions Edit View Help
root@kali: ~/lab07
root@kali:~/lab07# openssl rand -hex 16 >> chave.txt
root@kali:~/lab07# nano chave.txt
root@kali:~/lab07# openssl rand -hex 16 >> chave2.txt
root@kali:~/lab07# nano chave2.txt
root@kali:~/lab07# nano mensagem.txt
root@kali:~/lab07# openssl enc -aes-128-ecb -in mensagem.txt -out textoEncriptado.bin -K e4584440d467966101e41faf0866b51b
root@kali:~/lab07# ls
chave2.txt  chave.txt  mensagem.txt  textoEncriptado.bin
root@kali:~/lab07# nano textoEncriptado.bin
root@kali:~/lab07# openssl enc -aes-128-ecb -in textoEncriptado.bin -out textoClaro.txt -K e4584440d467966101e41faf0866b51b -d
root@kali:~/lab07# nano textoClaro.txt
root@kali:~/lab07# ls
chave2.txt  chave.txt  mensagem.txt  textoClaro.txt  textoEncriptado.bin
root@kali:~/lab07#

```

Podemos ver o conteúdo original:

```

GNU nano 5.8
textoClaro.txt
mensagem super secreta!
Aula de auditoria!

```

Ao tentar descriptar com uma chave diferente da original ocorre o seguinte erro:

```

root@kali: ~/lab07
root@kali:~/lab07# openssl enc -aes-128-ecb -in textoEncriptado.bin -out textoClaro.txt -K 3621f516640e9650f7d9fd9227a140cd -d
bad decrypt
140703271974144:error:06065064:digital envelope routines:EVP_DecryptFinal_ex:bad decrypt:../crypto/evp/evp_enc.c:610:
root@kali:~/lab07#

```

2.3 - Modificar alguns bits do texto encriptado e tentar decríptá-lo. Analisar o resultado.

Ao editar os bits do arquivo através do Vi e tentar fazer a descriptação é possível ver que um erro ocorreu durante o processo. É possível ver nos prints abaixo:

```

root@kali: ~/lab07
00000000: ff34 5221 91c3 699c b42c d842 31a0 ecaa .4R! ..i...B1 ...
00000010: c288 4f25 6878 6a7a 0d6f 5050 0671 a7e4 ..0%hxjz.oPP.q..
00000020: 8ad2 1dff 015b 41c9 833a 36d1 33d2 f6be .....[A...:6.3 ...
00000030: 0a

```

Mesmo com a chave correta não é possível descriptar o arquivo:


```

root@kali: ~/lab07
root@kali:~/lab07# cat chave2.txt
e4584440d467966101e41faf0866b51b
root@kali:~/lab07# openssl enc -aes-128-ecb -in textoEncriptado.bin -out textoClaro.txt -K e4584440d467966101e41faf0866b51b -d
bad decrypt
140246459450624:error:0606506D:digital envelope routines:EVP_DecryptFinal_ex:wrong final block length:../crypto/evp/evp_enc.c:599:
root@kali:~/lab07#

```

2.4 - Construir um arquivo de texto que possua um padrão que se repete várias vezes. Observar o padrão no arquivo encriptado.

Ao observar os bits do arquivo não foi possível determinar um padrão, abaixo segue o print do arquivo *repetição.txt*:

```

root@kali:~/lab07# cat chave2.txt
e4584440d467966101e41faf0866b51b
root@kali:~/lab07# openssl enc -aes-128-ecb -in textoEncriptado.bin -out textoClaro.txt -K e4584440d467966101e41faf0866b51b -d
bad decrypt
140246459450624:error:0606506D:digital envelope routines:EVP_DecryptFinal_ex:wrong final block length:../crypto/evp/evp_enc.c:599:
root@kali:~/lab07# nano repeticao.txt
root@kali:~/lab07# openssl enc -aes-128-ecb -in repeticao.txt -out repeticaoEncriptado.bin -K e4584440d467966101e41faf0866b51b
root@kali:~/lab07# nano repeticaoEncriptado.bin
root@kali:~/lab07# vi repeticaoEncriptado.bin
root@kali:~/lab07# cat repeticao.txt
oi
oi
olaamigo
root@kali:~/lab07# cat repeticaoEncriptado.bin
00000000: 5108 2e8e e1a9 faf3 c0d9 917d fea5 621f Q.....}..b.
00000009: 0a
root@kali:~/lab07#

```

2.5 - Enviar seu nome encriptado (em base64) para o professor usando o algoritmo aes-128-ecb e a senha, disponível na pasta do drive compartilhada entre você e o professor.

Salvando em base64:

The screenshot shows a Kali Linux terminal window with the following content:

```

root@kali: ~/lab07
File Actions Edit View Help
root@kali: ~/lab07

root@kali:~/lab07# echo "Gabriel Brito" | base64 >> gabriel.txt
root@kali:~/lab07# cat gabriel.txt
R2FicmllbC8Ccm10bwo=
root@kali:~/lab07# openssl enc -aes-128-ecb -in gabriel.txt -out gabriel_brito.bin -K e4584440d467966101e41faf0866b51b
root@kali:~/lab07# cat gabriel_brito.bin
*****
clear

```

A modal window titled "Screenshot" is overlaid on the terminal, with the text "Take a screenshot" and a "Screenshot" button.