

# Práctica Criptografía

Hecho por Alejandro Marin de Espinosa Toth  
 En conjunto con Daniel Redondo.

# Índice.

1) Clave simétrica.....	3
2) Clave asimétrica.....	4

## 1) Clave simétrica.

Para empezar con esta práctica, creamos nuestra clave simétrica y nuestro fichero con un mensaje que consideremos que tiene que ser secreto.

```
usuario@usuario:~$ sudo openssl rand -base64 32 > clave_simetrica.txt
usuario@usuario:~$ echo "menzahe zekreto" > mensaje.txt
usuario@usuario:~$ openssl enc -aes-256-cbc -salt -in mensaje.txt -out mensaje_encriptado.bin -pass file:clave_simetrica.txt -pbkdf2 -iter 100000
usuario@usuario:~$
```



Plantillas



Público



snap



Vídeos



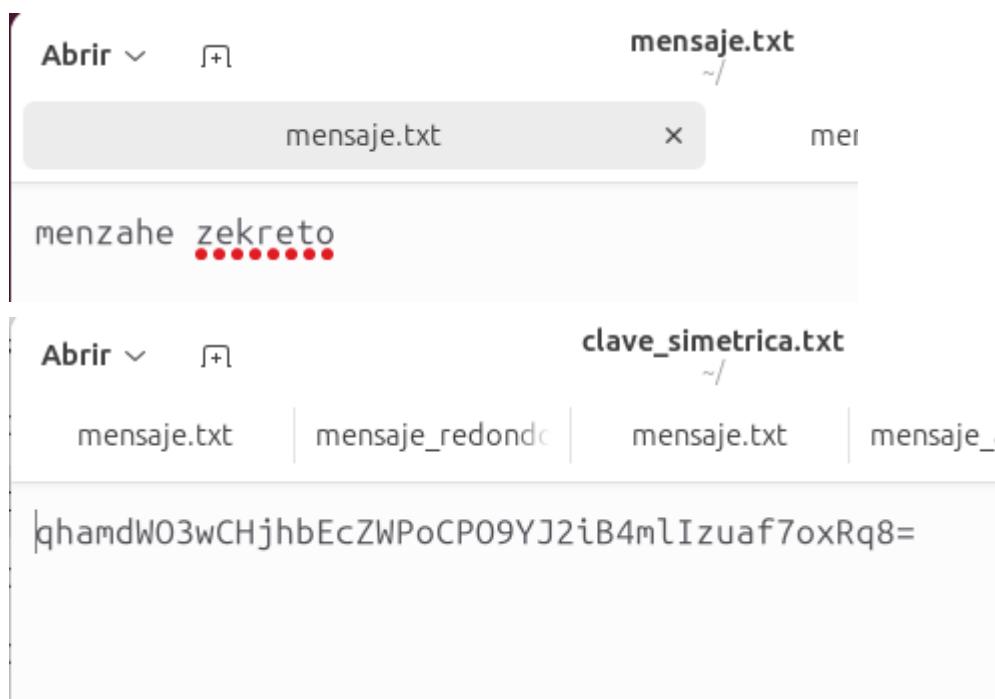
clave\_simetrica.txt



mensaje.txt

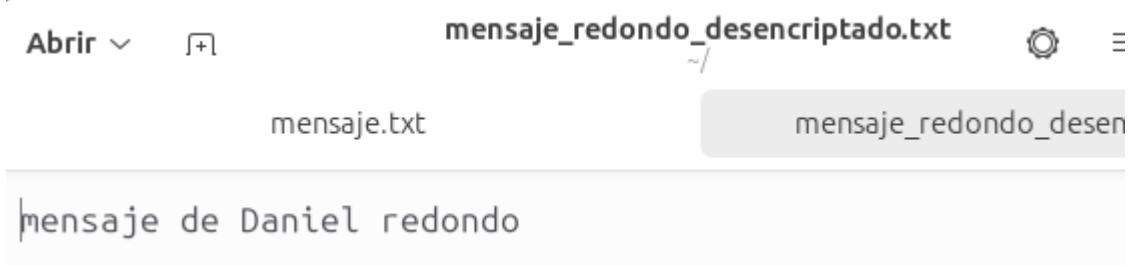


mensaje\_encriptado.bin



Luego, mandamos el fichero con la clave simétrica y con el mensaje encriptado a nuestro compañero (en nuestro caso, nos la hemos compartido por correo) y recibimos los mismos archivos de él. Una vez tengamos los archivos de clave simétrica y el mensaje encriptado de nuestro compañero, lo desencriptamos y podemos ver que sí que nos ha funcionado.

```
usuario@usuario:~$ sudo openssl enc -d -aes-256-cbc -in mensaje_redondo_encriptado.bin -out mensaje_redondo_desencriptado.txt -pass file:clave_simetrica_redondo.txt -pbkdf2 -iter 100000
usuario@usuario:~$
```



2) Clave asimétrica.

Para empezar con este tipo de clave, primero de todo generamos una clave pública y otra privada y mandamos nuestra clave pública a nuestro compañero y recibimos la suya.

Empezamos por la clave privada.

Y seguimos con la clave pública.

```
usuario@usuario:~/asimetrico$ sudo openssl rsa -pubout -in private_key_alejandro.pem -out public_key_alejandro.pem  
writing RSA key  
usuario@usuario:~/asimetrico$
```

Después, creamos el mensaje que vamos a encriptar con la clave pública de nuestro compañero, que hemos recibido previamente.

```
usuario@usuario:~/asimetrico$ sudo echo "Mensaje para Daniel Redondo" > mensaje.txt  
[sudo] contraseña para usuario:  
usuario@usuario:~/asimetrico$
```

Siguiendo con el punto, encriptamos el mensaje que hemos hecho antes con la clave pública de nuestro compañero. Hemos tenido que cambiar **rsautl** por **pkeyutl** porque rsautl ya está descontinuado.

```
usuario@usuario:~/asimetrico$ sudo openssl pkeyutl -encrypt -inkey public_key_danielredondo.pem -pubin -in mensaje.txt -out mensaje_a_danielredondo.bin
```



mensaje\_a\_  
danielredon  
do.bin

Y luego ya, se lo enviamos a nuestro compañero (hemos usado el comando scp debido a que no nos funcionaba bien el correo a la hora de enviar los archivos) y recibimos el de nuestro compañero.

```
usuario@usuario:~/asimetrico$ scp /home/usuario/asimetrico/mensaje_a_danielredondo.bin usuario@192.168.5.195:/home/usuario/
usuario@192.168.5.195's password:
mensaje_a_danielredondo.bin
```

Para finalizar, desencriptamos el mensaje que nos ha pasado nuestro compañero encriptado con nuestra clave pública.

```
usuario@usuario:~/asimetrico$ sudo openssl pkcs12 -inkey private_key_alejandro.pem -in mensaje_a_alejandro.bin -out mensaje_a_alejandro_desencriptado.txt
usuario@usuario:~/asimetrico$
```

Y podemos ver que está desencriptada.

Abrir ▾       **mensaje\_a\_alejandro\_desencriptado.txt**  
~asimetrico

mensaje.txt    |    mensaje\_redondo\_des |    mensaje.txt

este mensaje es secreto

La clave privada que nos ha generado es esta. (la hemos visto usando sudo nano)

```
GNU nano 7.2
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgqhkiG9w0BAQEFAASCBKcwgSjAgEAAoIBAQCoUU/lQfIiPR9W
4hL7y4lmgSgtU3tZeMUKYK7GwgDckhgLKw+wsnCd624s1GNFn0Ug8HL/J2G3ju4
vVBy+PGxDessqg5pTsvGXX3xGqxSH2IXxDxgG3XPz+Y5UZgNozxW1HMBELggGPpD
U8yzq3Vhr0FPeDcFp467mfLqhfdabvtN2Wj5G0cUeQ4BuV8SdVxd5vq6hldBwhe
TgJfRrEbfQ0AupC2YhSFysa/HifvRW7F/o55S2utCgdFWqud0lqH9f0/DMx3r+Sx
R42i7cs4A166pnOV3odDGCVS/j0xXO+avG8LVQ/fxfJML43pkRtzKDRskouTiMBL
YKqt4xApAgMBAECCgEADckVGfjcQ5If0u0dZuqEFHxYW4Tl6Zjj7j9psTho0goI
4/mc70F4ZAPzIj0wlcqJZqHmRDZVJ405indU6LrmGGH/M4SyZ/fDEvooHRBlxyxu
Agt5ihc4Vl7NGL+LoChRAj07CxNgZTPugVz9Fxpmo4CU4nz6AZnyTS97/ZwqQgu4
hzTfLG0vgHcmvCfb+uaNDLQK12fSnxuXTHXrnLrx3mZXWhtAJzPvPtj9XRNTggpB
Jy+NANnrtLW8yd1ZVrw0A6a6zesSIEaqTJywVwdH/Xw7p1Z/ZNG+N20LDbiKeMzB+
VuV/HKND5yfVloJ/KxVB3cb2ld/OlyAGQ8XpSEV9QKBgQDT9LtwE4DKPeK8oy3C
DcYeTGUx25TSHCVIMDwxluuOPZXUltY0Eyp04KYjjhMJP09Zn8qMvIRPI3ysG/W
15UV2PrFHH99sABC10FyTq3f4DLF0esa76m2UXNAP8LLKA4GNYrHirp7sS8dkq
6QtBE/qp5MvN8LwGEqBSNQqBdQKBgQDLsY6T80smPC/RJE1rz3dhqlt4P+oWiHxG
v2gyPzSGDsy0vG0h1CA+c2pPdvxWtCIIdWpDJvdaFvpHDX0I0/snJ0qF8+ZvCkq9
A1HyPtC7bYSYnkLjv0feCSCLIixzibPL8DaE3GVYKoN27nIq5SGsRePlffJBiaF
IgUreXfpZQKBgQC3FA1TIV9Kzdn+STtGTinsxXY25IyG6DdLw1idrN6KXmes2Rz
sniFuEx1uWKnYs0mNYJh0N+GQ+fYWM5BpLUBygnRedN5nSyzBLtjINLPLb5ksKeC
/MB69hx0lwefzZlPhRdOhGXPszwjtgn+GPgMoGxfg8MM4Q10qGAYJBsgQKBgHvQ
p2auuCdqYskjLhAghJAOPi+Jhd4BdId2TlTDF0oh/f0fa9zCLufQXQTLyw49fGKP
+i87rUztUlWSDoQ075dQsZGyEbexcgGagw9iWKi+ugKZKS3jW78MmqjCt/4KdJWZ
BQEM9JHBFPFp0MY6UjSSqUHnVdRe7ZkKNlHbHkrNAoGAaoaFm/ikg39U8hFZl+iC
jm0/Hcm1me//8n0Iel2skqRxSarmXXCaagnPy79W5/szSvDxkBaLj367H50N6v4S
ygvvEGtEp4DowpbepeuUTs/wRJLPkf/MLQ8Wbuo0D6MtMcnj6efrE9nY1KjPpmsqx
DuL8gr+IQfUYSYFylJ3dsi0=
-----END PRIVATE KEY-----
```

La clave pública que nos ha generado es esta. (la hemos visto con sudo nano también)

```
GNU nano 7.2                                     public_key_alejandro.pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIIBCgKCAQEAgFFP5UHyIj0fVuIS+8uJ
ZtYEoLVN7WXjFJCuxloA3JIYCyIvsLJwnetuLCBjRZ6FIPBy/ydht47uL1Qcvjx
lw3rLko0aU7Lx1198RqsUh9iF8QBYBt1z8/mOVGYDaM8VtRzARC4IBj601PMs6t1
YazhXz3g3Bae0u5ny0IX3WLW7Tdlo+RjnFHkOAbLfEnVcXeb6uoZlw8IXk4CX0ax
G30NALqQtmIUhcrgVxyH70Vuxf60eUtrrQoHRVqrndJah/XzwzMd6/ksUeNou3L
0ANeuqZzld6HQxnFUv4zsVzvmrxvJVUP38YyTC+N6ZEbcyg0bJKLk4jAS2CqreMQ
KQIDAQAB
-----END PUBLIC KEY-----
```

La clave pública de nuestro compañero es.

```
GNU nano 7.2                                     usuario@usuario: ~/asimetrico
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIIBCgKCAQEAIctGIkXLtvyKfiNAH5bh
ap9+4xs7BRnLR/dFPz0E4Zsi+ub+dkXhDL8b6Sg2evhewFwaXQ6qkvXkkFM99uT1
hd4Zm1XMGA1nIDm90WQQqfuf/VRwenLbbNgGVEa+fD14ay88pIkP2X/zuRWuPmt
PmZq2izLl8Xz5pJguZAo/38MoNaKkTSHyN384Ye4b0HGTlm7jRfVvpDePCflGMtG
DXxshm4aOBd9yez2BJjK9H8IVs9C3LRQMjTqgtVSZKsNxFULXmMt75J89PPAS+4
qRx65oEKmk/oPfzXhXZ6CaFxSXm44k261DmKmQ0l/6QcdRJibLziXLjdu6/V6Tox
wwIDAQAB
-----END PUBLIC KEY-----
```