Uso de OpenSSL

Primero veamos los comando posibles.

```
MacBook-Air:Downloads gfilippa$ openssl help
openssl:Error: 'help' is an invalid command.

Standard commands
asn1parse         ca                certhash          ciphers
crl               crl2pkcs7         dgst              dh
dhparam           dsa               dsaparam          ec
ecparam           enc               errstr            gendh
gendsa            genpkey           genrsa            nseq
ocsp              passwd            pkcs12            pkcs7
pkcs8             pkey              pkeyparam         pkeyutl
prime             rand              req               rsa
rsautl            s_client          s_server          s_time
sess_id           smime             speed             spkac
ts                verify            version           x509

Message Digest commands (see the `dgst' command for more details)
gost-mac          md4               md5               md_gost94
ripemd160         sha1              sha224            sha256
sha384            sha512            streebog256       streebog512
whirlpool

Cipher commands (see the `enc' command for more details)
aes-128-cbc       aes-128-ecb       aes-192-cbc       aes-192-ecb
aes-256-cbc       aes-256-ecb       base64            bf
bf-cbc            bf-cfb            bf-ecb            bf-ofb
camellia-128-cbc  camellia-128-ecb  camellia-192-cbc  camellia-192-ecb
camellia-256-cbc  camellia-256-ecb  cast              cast-cbc
cast5-cbc         cast5-cfb         cast5-ecb         cast5-ofb
chacha            des               des-cbc           des-cfb
des-ecb           des-ede           des-ede-cbc       des-ede-cfb
des-ede-ofb       des-ede3          des-ede3-cbc      des-ede3-cfb
des-ede3-ofb      des-ofb           des3              desx
rc2               rc2-40-cbc        rc2-64-cbc        rc2-cbc
rc2-cfb           rc2-ecb           rc2-ofb           rc4
rc4-40
```

Generando una huella digital sobre un archivo

$ openssl dgst -md5 <<nombre de archivo>>

$ openssl dgst -md5 redes2_unl.txt
MD5(redes2_unl.txt)= d41d8cd98f00b204e9800998ecf8427e

modificamos el archivo y vemos nuevamente el hash
$ echo 5 > redes2_unl.txt
$ cat redes2_unl.txt

5
$ openssl dgst -md5 redes2_unl.txt
MD5(redes2_unl.txt)= 1dcca23355272056f04fe8bf20edfce0

vemos que el HASH es distinto al primer archivo y con esto vemos que fue modificado el archivo orginal.

Cifrando datos (encriptando/desencriptando)

OpenSSL permite varios métodos de clave simétricas, por ejemplo blowfich, DES, 3DES, AES, etc.

Encriptando
$ openssl bf -e -in redes2_unl.txt -out redes2_unl.bf
enter bf-cbc encryption password:
Verifying - enter bf-cbc encryption password:
$ cat redes2_unl.bf
Salted__ï¿½dï¿½ï¿½8[qï¿½ï¿½{ys5#

Desencriptando
$ openssl bf -d -in redes2_unl.bf -out redes2_unl_decript.txt
enter bf-cbc decryption password:
$ cat redes2_unl_decript.txt
5

Creando claves Privadas y Públicas
$ openssl genrsa -out redes2_2022.pem 1024
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
$ cat redes2_2022.pem
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQClS5WcS7okbMctNd8y+V2pqIul/3ccxUU8S+Lq+1cnLdt0srJp
UfLIFiNwptpcWBt/ST3sCWQMYoXcgY9WnObesZldwxjODEBPtq4itSpnWPjZRh2m
t5FgppKkz5/gjnjlf/0TzVmvd2iDy9KWSrzxEbOxKaEu63i0kUpZ/PJWJwIDAQAB
AoGAKVVRQBgfn+QjmkaSXajFpxsicIwFOQiLW5yOTbwz+vQYoIHe4z8+upHuosjW
aakOlzG1bkSa5A3u80jikwIBKN+bEaJ4KX/AVsq38i1+k1PLESj8NKuOcxb7GYEj
LJ1A0ypDEKqwChq69U6gtH0c7nEdlp4ypt5hmdsRXAUIByECQQDcF5JbpQUpfwNq
X/1KjnbK9Ec11sOhGjtqpe3eu61ys+p1JiJAf7tBzeT5O0Sd92AoQA8S6/1wzEWk
A7TNUqIVAkEAwENaWF2KZwGuGfZXUbp7W94gpyf+ZbW2vRviDT+2YdrYAK6oWmpI
BUljv/Bvo6B1AwHqQw1XtCb2UiN7CLHySwJBAJ/LRWngT/Um0HYFJ0NgWANWg/Uk
7ngjMYxm2GNkY7PpyIoxm6C0nGJUeLAzRchi+J+AkvEsAaBJzy4busNwAVkCQENC
jMWjG7sDZHPisRN/aI5v+/5eSGoukto/eepmophDJhO/BlhzG/T1grbwFy4oASdn
MRv5+/ejNcLwdKdLEVcCQB6ygjQv0Vb4ojYMEdB8emoeZyRcJBl5un/gicvymVAH
MIzbnjvUNSOxpPlWLerPH04QsBSISNwIBB/4RO7luX4=

-----END RSA PRIVATE KEY-----

ahora extraemos la clave pública de la llave privada.

$ openssl rsa -in redes2_2022.pem -pubout -out redes2_2022_pub.pem
writing RSA key
$ cat redes2_2022_pub.pem
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQClS5WcS7okbMctNd8y+V2pqIul
/3ccxUU8S+Lq+1cnLdt0srJpUfLIFiNwptpcWBt/ST3sCWQMYoXcgY9WnObesZld
wxjODEBPtq4itSpnWPjZRh2mt5FgppKkz5/gjnjlf/0TzVmvd2iDy9KWSrzxEbOx
KaEu63i0kUpZ/PJWJwIDAQAB
-----END PUBLIC KEY-----

Ahora vamos a encriptar con la clave pública un archivo.

$ openssl rsautl -encrypt -inkey redes2_2022_pub.pem -pubin -in redes2_unl.txt -out redes2_unl_pri_pub.rsa
MacBook-Air:Downloads gfilippa$ cat redes2_unl_pri_pub.rsa
o7��{�bD�
*	�"�'�;�x�w������*
�+v�Ė��l�"ajo�MaN�>a��1t8�◂R�e��"��WwK��un�S��q�U(ZR ◆|*
���?��B'◆lCU-$95z��A◆

ahora desencriptamos con la clave privada
$ openssl rsautl -decrypt -inkey redes2_2022.pem -in redes2_unl_pri_pub.rsa -out redes2_unl_decrypt_pub_pri.txt
$ cat redes2_unl_decrypt_pub_pri.txt
5
$