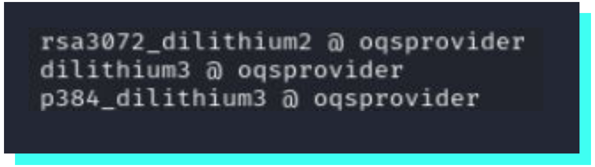
educaciónIT
CODE YOUR FUTURE

Criptografía y Blockchain

Módulo 4 - Resolución del laboratorio

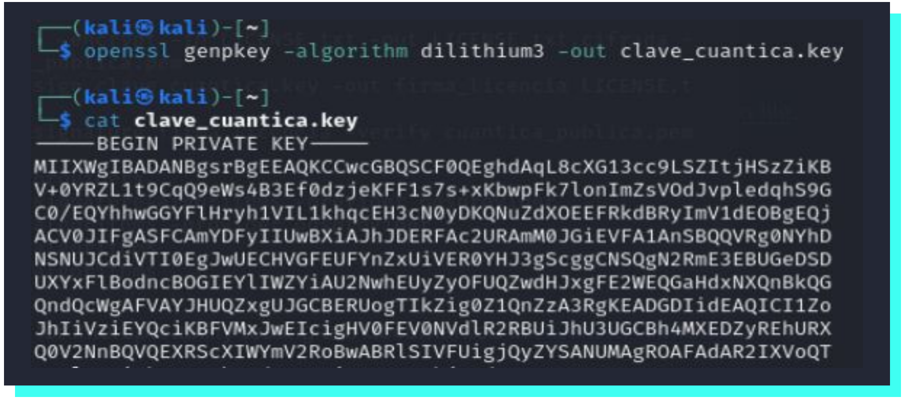
Resolución del ejercicio 1

2.



```
rsa3072_dilithium2 @ oqsprovider
dilithium3 @ oqsprovider
p384_dilithium3 @ oqsprovider
```

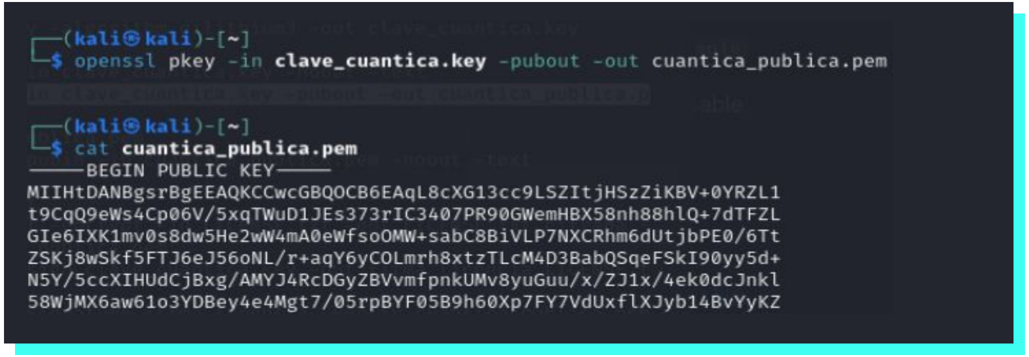
3.



```
┌──(kali㉿kali)-[~]
└─$ openssl genpkey -algorithm dilithium3 -out clave_cuantica.key

┌──(kali㉿kali)-[~]
└─$ cat clave_cuantica.key
-----BEGIN PRIVATE KEY-----
MIIXWgIBADANBgsrBgEEAQKCCwcGBQSCF0QEghdAqL8cXG13cc9LSZItjHSzZiKB
V+0YRZL1t9CqQ9eWs4B3Ef0dzjeKFF1s7s+xKbwpFk7lonImZsVOdJvpledqhS9G
C0/EQYhhwGGYFlHryh1VIL1khqcEH3cN0yDKQNuZdXOEEFRkdBRyImV1dEOBgEQj
ACV0JIFgASFCAmYDFyIIUwBXiAJhJDERFAc2URAmM0JGiEVFA1AnSBQQVRg0NYhD
NSNUJCdiVTI0EgJwUECHVGFEUFYnZxUiVER0YHJ3gScggCNSQgN2RmE3EBUGeDSD
UXYxFlBodncBOGIEYlIWZYiAU2NwhEUyZyOFUQZwdHJxgFE2WEQGaHdxNXQnBkQG
QndQcWgAFVAYJHUQZxgUJGCBERUogTIkZig0Z1QnZzA3RgKEADGDIidEAQICI1Zo
JhIiVziEYQciKBFVMxJwEIcigHV0FEV0NVdlR2RBUiJhU3UGCBh4MXEDZyREhURX
Q0V2NnBQVQEXRScXIWYmV2RoBwABRlSIVFUigjQyZYSANUMAgROAFAdAR2IXVoQT
```

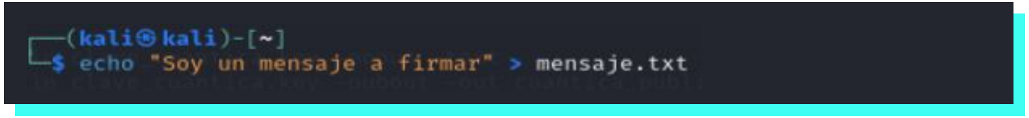
4.



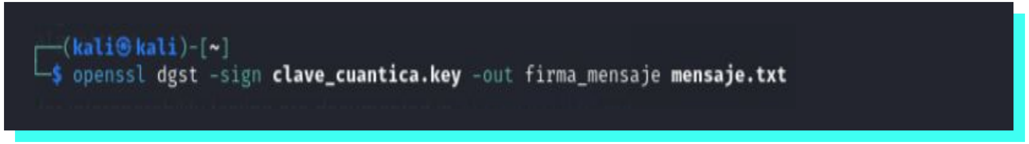
```
┌──(kali㉿kali)-[~]
└─$ openssl pkey -in clave_cuantica.key -pubout -out cuantica_publica.pem

┌──(kali㉿kali)-[~]
└─$ cat cuantica_publica.pem
-----BEGIN PUBLIC KEY-----
MIIHtDANBgsrBgEEAQKCCwcGBQOCB6EAqL8cXG13cc9LSZItjHSzZiKBV+0YRZL1
t9CqQ9eWs4Cp06V/5xqTWuD1JEs373rIC3407PR90GWemHBX58nh88hlQ+7dTFZL
GIe6IXK1mv0s8dw5He2wW4mA0eWfsoOMW+sabC8BiVLP7NXCRhm6dUtjbPE0/6Tt
ZSKj8wSkf5FTJ6eJ56oNL/r+aqY6yCOLmrh8xtzTLcM4D3BabQSqeFSkI90yy5d+
N5Y/5ccXIHUdCjBxg/AMYJ4RcDGyZBVvmfpnkUMv8yuGuu/x/ZJ1x/4ek0dcJnkl
58WjMX6aw61o3YDBey4e4Mgt7/05rpBYF05B9h60Xp7FY7VdUxflXJyb14BvYyKZ
```

5.

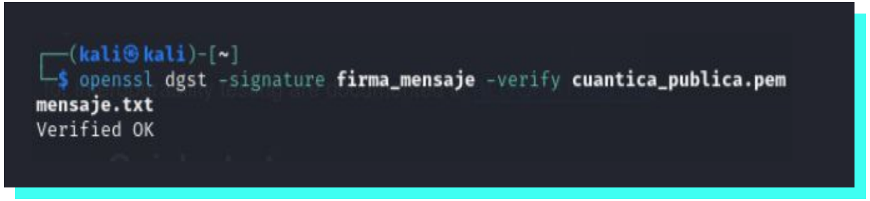


```
┌──(kali㉿kali)-[~]
└─$ echo "Soy un mensaje a firmar" > mensaje.txt
```



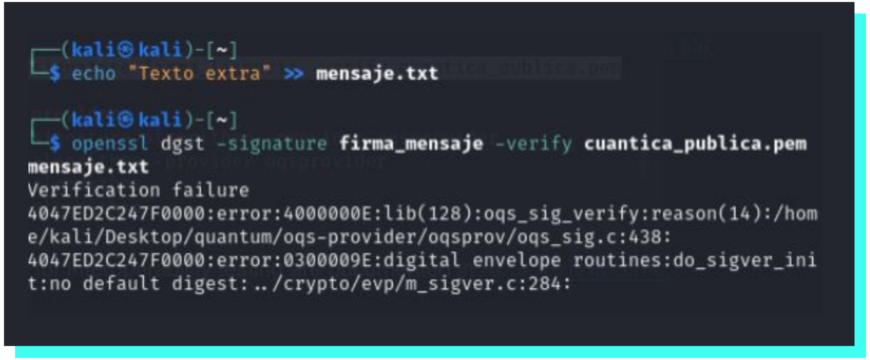
```
┌──(kali㉿kali)-[~]
└─$ openssl dgst -sign clave_cuantica.key -out firma_mensaje mensaje.txt
```

6.



```
┌──(kali㉿kali)-[~]
└─$ openssl dgst -signature firma_mensaje -verify cuantica_publica.pem
mensaje.txt
Verified OK
```

7.

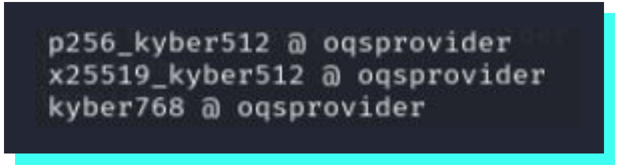


```
┌──(kali㉿kali)-[~]
└─$ echo "Texto extra" >> mensaje.txt

┌──(kali㉿kali)-[~]
└─$ openssl dgst -signature firma_mensaje -verify cuantica_publica.pem
mensaje.txt
Verification failure
4047ED2C247F0000:error:4000000E:lib(128):oqs_sig_verify:reason(14):/hom
e/kali/Desktop/quantum/oqs-provider/oqsprov/oqs_sig.c:438:
4047ED2C247F0000:error:0300009E:digital envelope routines:do_sigver_ini
t:no default digest:../crypto/evp/m_sigver.c:284:
```

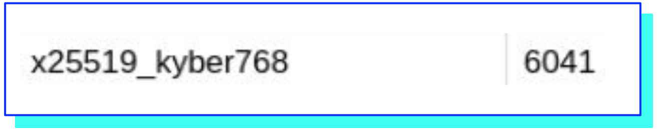
Resolución del ejercicio 2

2.



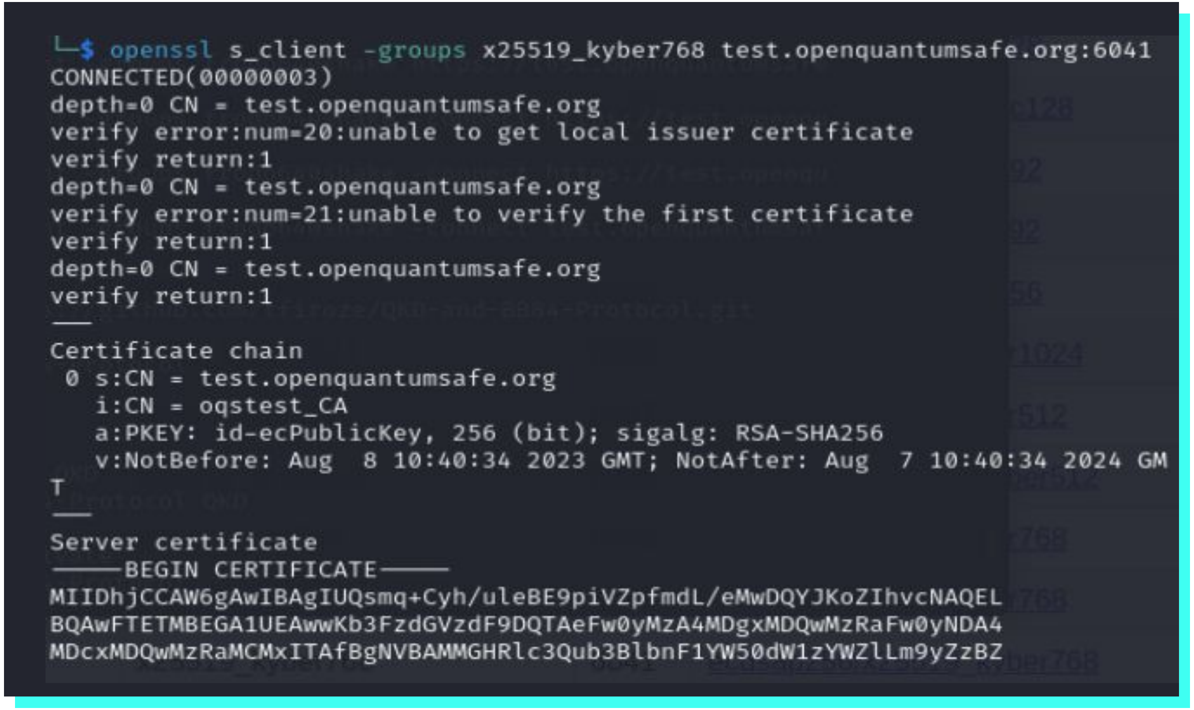
```
p256_kyber512 @ oqsprovider
x25519_kyber512 @ oqsprovider
kyber768 @ oqsprovider
```

3.



x25519_kyber768	6041

5.



```
└─$ openssl s_client -groups x25519_kyber768 test.openquantumsafe.org:6041
CONNECTED(00000003)
depth=0 CN = test.openquantumsafe.org
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN = test.openquantumsafe.org
verify error:num=21:unable to verify the first certificate
verify return:1
depth=0 CN = test.openquantumsafe.org
verify return:1
---
Certificate chain
 0 s:CN = test.openquantumsafe.org
   i:CN = oqstest_CA
   a:PKEY: id-ecPublicKey, 256 (bit); sigalg: RSA-SHA256
   v:NotBefore: Aug  8 10:40:34 2023 GMT; NotAfter: Aug  7 10:40:34 2024 GM
T
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDhjCCAW6gAwIBAgIUQsmq+Cyh/uleBE9piVZpfmdL/eMwDQYJKoZIhvcNAQEL
BQAwFTETMBEGA1UEAwwKb3FzdGVzdF9DQTAeFw0yMzA4MDgxMDQwMzRaFw0yNDA4
MDcxMDQwMzRaMCMxITAfBgNVBAMMGHRlc3Qub3BlbnF1YW50dW1zYWZlLm9yZzBZ
```

educaciónIT
CODE YOUR FUTURE

¡Sigamos trabajando!