educación IT
CODE YOUR FUTURE

Criptografía y Blockchain

Módulo 3 - Resolución del laboratorio

Resolución del ejercicio

1.
```
┌──(kali㉿kali)-[~]
└─$ seq 20000 > muestra.txt
```

2.
```
└─$ openssl genpkey -algorithm EC -pkeyopt
ec_paramgen_curve:secp521r1 -out ec_privada
.pem
```

3.
```
└─$ openssl pkey -in ec_privada.pem -pubout
 -out ec_publica.pem
```

4.

```
└─$ openssl pkeyutl -sign -digest sha3-512
-inkey ec_privada.pem -in muestra.txt -rawi
n -out muestra.txt.signature
```

6.

```
┌──(kali㉿kali)-[~]
└─$ cksum muestra.txt*
3231941463 108894 muestra.txt
3371777690 137 muestra.txt.signature
```

7.

```
┌──(kali㉿kali)-[~]
└─$ openssl pkeyutl -verify -digest sha3-51
2 -inkey ec_privada.pem -in muestra.txt -ra
win -sigfile muestra.txt.signature
Signature Verified Successfully
```

8.

```
┌──(kali㉿kali)-[~]
└─$ echo "algo mas" >> muestra.txt
```

9.

```
┌──(kali㉿kali)-[~]
└─$ openssl pkeyutl -verify -digest sha3-51
2 -inkey ec_privada.pem -in muestra.txt -ra
win -sigfile muestra.txt.signature
Signature Verification Failure
```

educación IT
CODE YOUR FUTURE

¡Sigamos trabajando!