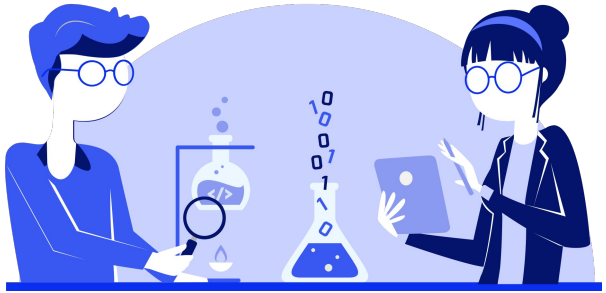
educación IT
CODE YOUR FUTURE

Criptografía y Blockchain

Módulo 3 - Laboratorio adicional

Para poder realizar este laboratorio, se recomienda:

- Revisar contenidos previos.



Ejercicio

Sigue las consignas para **firmar y verificar con *OpenSSL*:**

1. Con el comando **`seq`** genera un archivo ***muestra.txt*** con los números de 1 al 20.000.
2. Genera un par de claves ECDSA a partir de una curva ***NIST B-571***.
3. Para firmar, utilizaremos el subcomando **`openssl pkeyutl`** con las opciones ***sign***, ***digest***, ***inkey***, ***in***, ***rawin***, ***out***, ***sigfile***.
4. Guarda el archivo firmado con el nombre ***muestra.txt.signature***.
5. Consulta el manual (**`man openssl-pkeyutl`**) ante cualquier duda.
6. Compara el tamaño del archivo y su firma con el comando **`cksum muestra.txt.*`**. Los resultados se verán en la segunda columna.
7. Verifica la firma cambiando el ***sigfile*** y la opción ***sign*** por ***verify***.
8. Modifica el archivo con el comando **`echo “algo mas” >> muestra.txt`**.
9. Comprueba que la verificación ahora falla.

¡Sigamos trabajando!