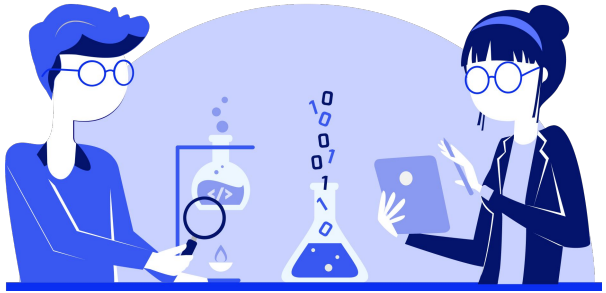
educación IT
CODE YOUR FUTURE

Criptografía y Blockchain

Módulo 3 - Laboratorio adicional

Para poder realizar este laboratorio, se recomienda:

- Revisar contenidos previos.



Ejercicio

Sigue las consignas para **derivar una clave de cifrado de 256 *bits* partir de una contraseña** con *OpenSSL*:

1. Puedes consultar la documentación con el comando **`man openssl-kdf`**.
2. Genera una clave (sal criptográfica) de 128 *bits* hexadecimal con **`openssl rand`**.
3. Deriva la clave útil para cifrado simétrico con el comando **`openssl kdf`** y las opciones ***keylen*** y ***kdfopt*** para la contraseña, la sal, y los parámetros de *SCRYPT n=65536*, *r=8* y *p=1*.

¡Sigamos trabajando!