educación IT
CODE YOUR FUTURE

Criptografía y Blockchain

Módulo 3 - Resolución del laboratorio

Resolución del ejercicio

1.

```
OPENSSL-KDF(1SSL)      OpenSSL      OPENSSL-KDF(1SSL)

NAME
       openssl-kdf - perform Key Derivation
       Function operations

SYNOPSIS
       openssl kdf [-help] [-cipher] [-digest]
       [-mac] [-kdfopt nm:v] [-keylen num] [-out
       filename] [-binary] [-provider name]
       [-provider-path path] [-propquery propq]
       kdf_name

DESCRIPTION
       The key derivation functions generate a
       derived key from either a secret or
       password.

OPTIONS
       -help
           Print a usage message.

       -keylen num
           The output size of the derived key. This
           field is required.

       -out filename
           Filename   to   output   to,   or   standard
           output by default.
```

2.

```
└─$ openssl rand -hex 16
4749d6b518462e7ea5ac0a3d7218126b
```

3.

```
┌──(kali㉿kali)-[~]
└─$ openssl kdf -keylen 32 -kdfopt 'pass:SuperPa$$w0rd'
 -kdfopt hexsalt:4749d6b518462e7ea5ac0a3d7218126b -kdfo
pt n:65536 -kdfopt r:8 -kdfopt p:1 SCRYPT
2E:C7:45:ED:9C:8B:B4:41:1B:86:DE:63:32:ED:F0:91:49:69:4
A:85:C3:11:1A:8B:C4:16:7E:BD:6D:6C:A5:10
```

educación IT
CODE YOUR FUTURE

¡Sigamos trabajando!