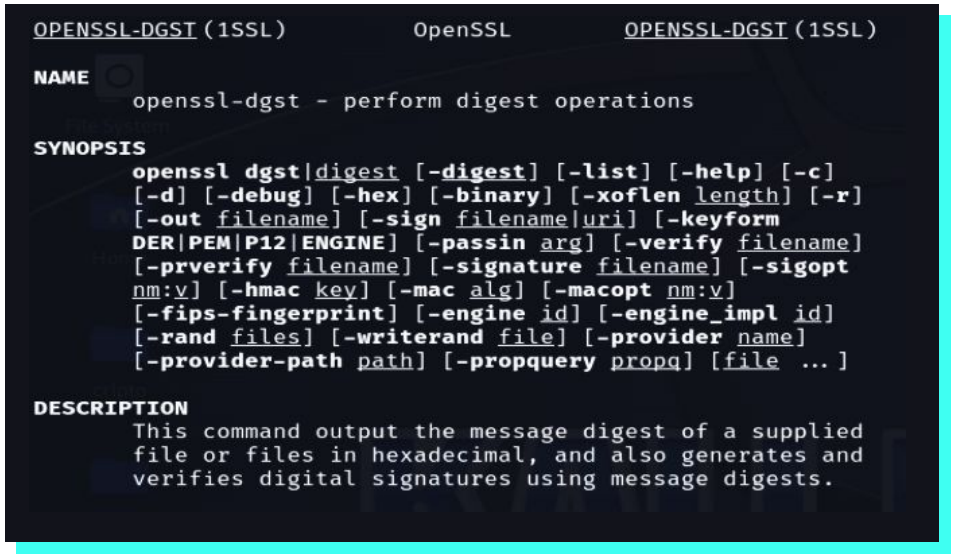
educación IT
CODE YOUR FUTURE

# Criptografía y Blockchain

## Módulo 3 - Resolución del laboratorio

# Resolución del ejercicio 1

1.



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

NAME
       openssl-dgst - perform digest operations

SYNOPSIS
       openssl dgst|digest [-digest] [-list] [-help] [-c]
       [-d] [-debug] [-hex] [-binary] [-xoflen length] [-r]
       [-out filename] [-sign filename|uri] [-keyform
       DER|PEM|P12|ENGINE] [-passin arg] [-verify filename]
       [-prverify filename] [-signature filename] [-sigopt
       nm:v] [-hmac key] [-mac alg] [-macopt nm:v]
       [-fips-fingerprint] [-engine id] [-engine_impl id]
       [-rand files] [-writerand file] [-provider name]
       [-provider-path path] [-propquery propq] [file ...]

DESCRIPTION
       This command output the message digest of a supplied
       file or files in hexadecimal, and also generates and
       verifies digital signatures using message digests.
```

2.

```
-$ seq 20000 > muestra.txt
```

3.

```
└─$ openssl dgst -list
Supported digests:
-blake2b512               -blake2s256               -md4
-md5                      -md5-sha1                 -ripemd
-ripemd160                -rmd160                   -sha1
-sha224                   -sha256                   -sha3-224
-sha3-256                 -sha3-384                 -sha3-512
-sha384                   -sha512                   -sha512-224
-sha512-256               -shake128                 -shake256
-sm3                      -ssl3-md5                 -ssl3-sha1
-whirlpool
```

4.

```
└─$ openssl dgst -sha3-256 muestra.txt
SHA3-256(muestra.txt)= 658656e129914052546af527ba8cf573ab27fb47551a0682ffcf
00eeaf56d32b
```

# Resolución del ejercicio 2

1.

```
$ hashcat --help
hashcat (v6.2.6) starting in help mode

Usage: hashcat [options]... hash|hashfile|hccapxfile [dictionary|mask|directory]...

- [ Options ] -

 Options Short / Long          | Type | Description                                    | Exam
ple
=============================+======+================================================+======
=================
 -m, --hash-type               | Num  | Hash-type, references below (otherwise autodetect)   | -m 1
```

2.

```
┌──(kali㉿kali)-[~/Desktop/cripto]
└─$ hashcat -a 0 -m 3200 hashes.txt Passwords/xato-net-10-million-passwords-10000.txt --force

hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 4.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO
, POCL_DEBUG) - Platform #1 [The pocl project]
```

3.

```
┌──(kali㉿kali)-[~/Desktop/cripto]
└─$ hashcat -a 0 -m 3200 hashes.txt Passwords/xato-net-10-million-passwords-10000.txt --show

$2y$10$TYau45etgP4173/zx1usm.uO34TXAld/8e0/jKC5b0jHCqs/MZGBi:password
$2y$10$qQVWugep3jGmh4ZHuHqw8exczy4t8BZ/Jy6H4vnbRiXw.BGwQUrHu:hotdog
$2y$10$DuZ0T/Qieif009SdR5HD5OOiFl/WJaDyCDB/ztWIM.1koiDJrN5eu:password1
$2y$10$0ClJ1I7LQxMNva/NwRa5L.4ly3EHB8eFR5CckXpgRRKAQHXvEL5oS:88888888
$2y$10$LIWMJJgX.Ti9DYrYiaotHuqi34eZ2axl8/i1Cd68GYsYAG02Icwve:hello123
```

educación IT
CODE YOUR FUTURE

# ¡Sigamos trabajando!