Crypto

Ver hash de archivo

Comprobar el hash de un fichero o programa nos puede servir para confirmar que no se ha modificado por ejemplo en una descarga.

creamos archivo con contenido

```
echo 'hola' > fichero.txt
```

md5

```
md5sum fichero.txt
```

modificamos el contenido del fichero

```
nano fichero.txt

# cambiamos hola por adios
# guardamos
ctrl + o
# cerramos
ctrl + x
```

otra forma de cambiar el contenido

```
echo 'adios' > fichero
```

comprobamos de nuevo el hash y comprobamos que ha cambiado

```
md5sum hash
```

sha1 y sha256

Al igual que podemos obtener el hash md5 de un fichero podemos obtener otro tipo de hashes como sha1 y sha256

```
# sha1
sha1sum fichero.txt

# sha256
sha256sum fichero.txt
```

Identificar tipo de hash

hash-identifier

Esta herramienta entre otras nos permite identificar el tipo de hash.

Con los hashes obtenidos anteriormente podemos hacer la prueba.

```
hash-identifier hash

# Ejemplo
hash-identifier 916f4c31aaa35d6b867dae9a7f54270d
```

Codificación

Usaremos la herramienta Decodify, utilizada para la decodificación de textos.

```
# descargamos
git clone https://github.com/UltimateHackers/Decodify

# nos movemos al directorio generado
cd Decodify

# instalamos
make install
```

Codificamos texto en base64 con openssl

```
echo 'esto es un texto para codificar' | openssl enc -a -e

-e --> le indicamos que codifique
```

```
-a --> le indicamos que el output sea en base64
enc --> se debe utilizar para el cifrado
```

Descodificamos con openssl

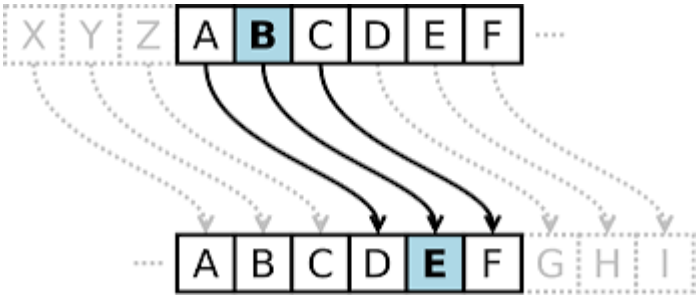
```
echo 'ZXN0byBlcyB1biB0ZXh0byBwYXJhIGNvZGlmaWNhcgo=' | opens
sl enc -a -d

-d --> indicamos que descodifique
```

con dcode(decodify) descodificamos la cadena generada anteriormente

```
dcode ZXN0byBlcyB1biB0ZXh0byBwYXJhIGNvZGlmaWNhcgo=
```

cifrado cesar

consiste en sustituir cada letra del abecedario por una letra desplazada un número determinado de posiciones




```
dcode 'bpgkta xh qtiitg iwpc sr' -rot all
```

Cifrado simétrico

ciframos

```
echo "texto de cifrado simetrico" | openssl enc -aes-256-cb
c -a -e

# al ejecutarlo le  indicamos una password
```

desciframos

```
echo 'U2FsdGVkX19pSL7wzN0tFqozr5nFvw7qkSJpuMnTo8oOQS/HlKrMh
3W2CmI2X1d5' | openssl enc -aes-256-cbc -a -d
```