# SGSSI-22.InformeLaboratorio6 (Alexandra)

## Actividad 1.

Lenguaje de programación utilizado: Python

## Actividad 0

Tras realizar varios intentos para arreglar el error del programa en Java obtenido en el laboratorio 5, no he conseguido hacer que obtenga un fichero con las características mencionadas, aunque sí comprueba que el hash comience por un '0':

```
Digest: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
Wrong digest.
File Result.txt emptied.

Digest: 0cdedf13a8f8872bd6b9ba2e36321a0360e7d97f3a0bce982807473ba1c647ce
Digest found! Check file 'Result.txt'
PS C:\Users\Aleina\Documents\Uni\4º\SGSSI\Sha256>
```

El error está en que el fichero 'Result.txt' se está sobreescribiendo en vez de vaciarse, como se puede observar en el comentario 'File Result.txt emptied.'. Le he dado muchas vueltas y comprobado varias dudas en Stackoverflow (y más), pero nada…

Al final, le pedí ayuda a un compañero, Gorka Arzanegi (16GROD) y me presentó su versión, que es en Python. Con su consentimiento, trabajé sobre dicha versión, la cual funciona conforme los requisitos del laboratorio 5.

Resultado obtenido:

```
Inserta el nombre del fichero: SGSSI-22.CB.02.txt
El primero fichero de salida será  SGSSI-22.CB.02.APEL.txt
Nuevo record: 1, intentos: 12
Nuevo record: 2, intentos: 20
Nuevo record: 3, intentos: 2325
Nuevo record: 4, intentos: 6897

Intentos totales: 18266
Hexadecimal generado: f3f5a94f G26
SHA256 generado: 0000d0ceeb0bebe655e77118c47aa71c76bfe112af68a6c81347ca0d75218e9e
```

## Actividad 1

Al comprobar si los ficheros cumplen las condiciones en la actividad 1.1, tengo como resultado lo siguiente:

```
PS C:\Users\Aleina\Documents\Uni\4º\SGSSI\Lab 5> & C:/msys64/mingw64/bin/python.exe "c:/Users/Aleina/Documents/Uni/4º/S
GSSI/Lab 5/L6_APEL.py"
Inserta el nombre del primer fichero: SGSSI-22.CB.02.txt
Inserta el nombre del segundo fichero: SGSSI-22.CB.02.APEL.txt
El segundo fichero es válido (su hash tiene como prefijo una secuencia de 0's mayor a 3)
PS C:\Users\Aleina\Documents\Uni\4º\SGSSI\Lab 5>
```

La implementación:

```python
from collections import deque
import hashlib, os, secrets

def sha256gen(filename):···

def rdn_hex_gen():···

if __name__ == '__main__':

    f1 = input("Inserta el nombre del primer fichero: ")
    f2 = input("Inserta el nombre del segundo fichero: ")

    with open(f1, 'r') as fp:
        txt = fp.read()

    with open(f2, 'r') as fp:
        x = len(fp.readlines())-1
        txt2 = deque(f2, x)

    if(txt == txt2):
        print("El contenido de ficheros son iguales (excepto última línea del segundo)")

    sha = sha256gen(f2)

    cont = 0
    i = 0

    while(i < (len(sha) - 1) and sha[i] == '0'):
        cont = cont + 1
        i = i + 1

    if(cont >= 3):
        print("El segundo fichero es válido (su hash tiene como prefijo una secuencia de 0's mayor a 3)")
```

El error está en comprobar el contenido, lo cual no conseguí arreglar en el periodo de tiempo del laboratorio.