

## PRÁCTICA 2: Criptografía (Parte 4)

Seguridad de la Información  
Curso 2018-2019

Lenguajes y Ciencias de la Computación.  
E.T.S.I. Informática, Universidad de Málaga

### RELACIÓN DE EJERCICIOS:

---

1. (7.5 puntos) En base a la siguiente documentación:

- Manejo de ficheros
  - <https://www.datacamp.com/community/tutorials/reading-writing-files-python>
  - <https://www.pythonforbeginners.com/files/reading-and-writing-files-in-python>
  - <https://docs.python.org/3/tutorial/inputoutput.html>
- Hash y HMAC en PyCryptodome
  - <https://pycryptodome.readthedocs.io/en/latest/src/hash/hash.html>

Se pide lo siguiente:

- a. (2.5 puntos) Crear un documento de texto (.txt, editable en el Notepad) que contenga en la primera línea tu nombre, y en la segunda línea tus apellidos. A continuación, calcular utilizando Python y PyCryptodome el hash SHA512 de dicho fichero de texto.
- b. (2.5 puntos) Utilizando el fichero de texto del apartado anterior, usar Python y PyCryptodome para calcular el HMAC-SHA512 de dicho fichero, con la clave `b'S3cr3tK3y'` (S3cr3tK3y en binario) Posteriormente, comprobar la validez de dicho HMAC-SHA512.
- c. (2.5 puntos) Crear un documento de Word (.docx)<sup>1</sup> que contenga en la primera línea tu nombre, y en la segunda línea tus apellidos. A continuación, calcular utilizando Python y PyCryptodome el hash SHA3-256 de dicho fichero. Para ello, leer el fichero de 4KB en 4KB

*NOTA:* En los ficheros binarios, la función `read()` devuelve `b''` si no se han podido leer más elementos del fichero.

2. (2.5 puntos) En la librería PyCryptodome, no todos los algoritmos de hash pueden utilizarse para calcular un HMAC. De todos los algoritmos indicados en <https://pycryptodome.readthedocs.io/en/latest/src/hash/hash.html>, indicar cuales pueden utilizarse para calcular un HMAC y cuáles no, y por qué.

*NOTA:* Para este apartado, más que probar todos los algoritmos de hash uno por uno, se aconseja ejecutar el apartado 1.b (cálculo del HMAC) con el hash SHA3-256, y comprobar el error de ejecución "AttributeError". Ese error indicará por qué SHA3-256 no puede utilizarse para calcular un HMAC, y dará la pista necesaria para responder a esta pregunta solamente mirando la documentación<sup>2</sup>.

---

<sup>1</sup> En caso de que no dispongas de Microsoft Word en tu ordenador personal, se aconseja utilizar los equipos del laboratorio para crear dicho documento.

<sup>2</sup> Para más información sobre las causas por las que PyCryptodome no permite que SHA3-256 y otros algoritmos no se utilicen para calcular un HMAC, ver <https://crypto.stackexchange.com/a/17928>