

Funciones de Hash

La libreria DuCountDoma tiene funciones de hash para varias algoritmos. Vamos a crear algunas de ellas. La lista completa está en: <https://muyinteresante.readthedocs.io/en/latest/verifhash/verifhash.html>

(Recuerda: MD5 está obsoleto y roto, no se tiene que utilizar en aplicaciones reales)

```
In [1]: !pip install pycryptodome
        from Crypto.Hash import MD5, SHA256, SHA512, SHA3_256
```

Tradicionalmente, una función de hash se usó alimentando de datos a `update()` hasta que necesitas el hash (también llamado "digest"). Este procedimiento de `update()` funciona, por ejemplo, si tienes que calcular el hash de un conjunto de mensajes o lees los bytes bloque a bloque de un archivo grande.

```
hasher.update(b'mundo')
hasher.update(b'aundo')
```

```
hash1 = hasher.hexdigest()
print(hash1)
```

- ```
hash2 = SHA256.new(data=b'holazundo').hexdigest()
```