02.Hashing

Hashing es una función de un único camino. En inglés *One Way Function*. O huella dactilar.

Una función hash debe cumplir dos requisitos mínimos

1. Debe producir un *valor único* y *repetible* por cada entrada
2. La salida no entrega pistas sobre la entrada que los produce

MD5 no debe ser usado para ninguna operación de seguridad

Confidencialidad: Ningún sujeto puede *leer* el mensaje sin autorización
Integridad: Ningún sujeto puede *modificar* el mensaje sin autorización

Digests son como huellas dactilares, son una pequeña cantidad de datos que expresan la identidad de un documento.

Digest MD5 crean un número que siempre es de **16 bytes** de memoria.

Python distingue entre cadenas Unicode y cadenas de byte crudos. En términos prácticos se deben usar bytes.

Se transforman cadenas de texto en bytes usando el operador `b'` sobre la cadena objetivo.

Hash o Función Hash siempre se refiere al hahs criptográfico.

Funciones Hash están fundamentalmente intentando mapear un enorme (incluso infinito) número de entidades en un conjunto más pequeño de entidades. No importa que tan grande es el archivo o el documento, siempre terminará como una cadena de números de 16 bytes.

En términos matemáticos discretos, esto quiere decir que el *dominio* de una función hash es mucho mayor que su *rango*.

Dado un gran número de documentos, existen chances de que producirán el mismo hash.
