Criptografía Simétrica y Asimétrica

OpenWebinars

¡BIENVENIDOS!

Soy Luis Javier Marquina

Profesor en Ciclos Formativos y Bachillerato

OpenWebinars

ÍNDICE

¿ Qué es Criptografía?

- Mensajes ininteligibles para receptores no autorizados
    - Aplicando un algoritmo

- Garantizar la Confidencialidad de la información

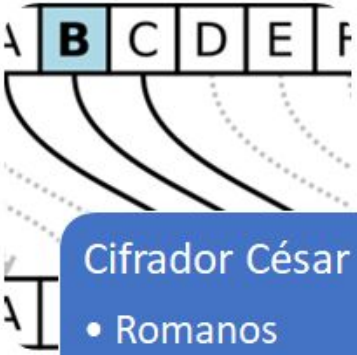
Historia de la Criptografía

Jeroglíficos

- Egipcios
- Sustitución

Escítala

- Espartanos
- Transposición



Cifrador César

- Romanos
- Sustitución

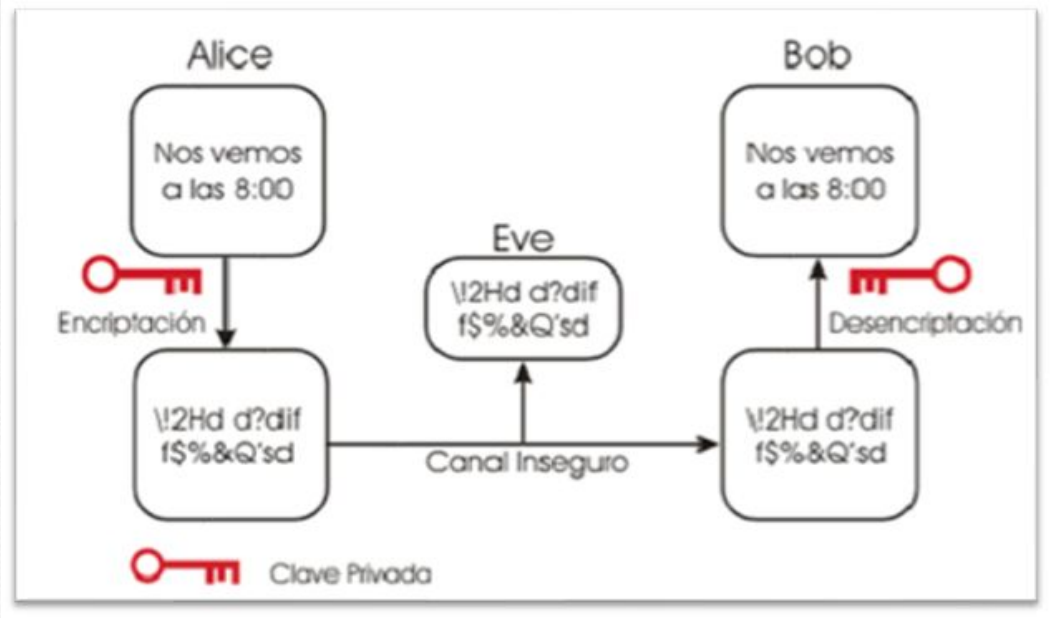
Criptografía actual

- Criptografía Simétrica o de Clave Privada

- Criptografía Asimétrica o de Clave Pública

Criptografía Simétrica

- Receptor y emisor conocen la clave para cifrar/descifrar el mensaje



Criptografía Simétrica

- Ventajas

  - Eficiente en grupos reducidos
  - Sencillos de utilizar
  - Eficientes (poco tiempo cifrar/descifrar)

- Desventajas

  - Posible intercambio de claves por medios no seguros
  - Gran cantidad de claves a memorizar/almacenar

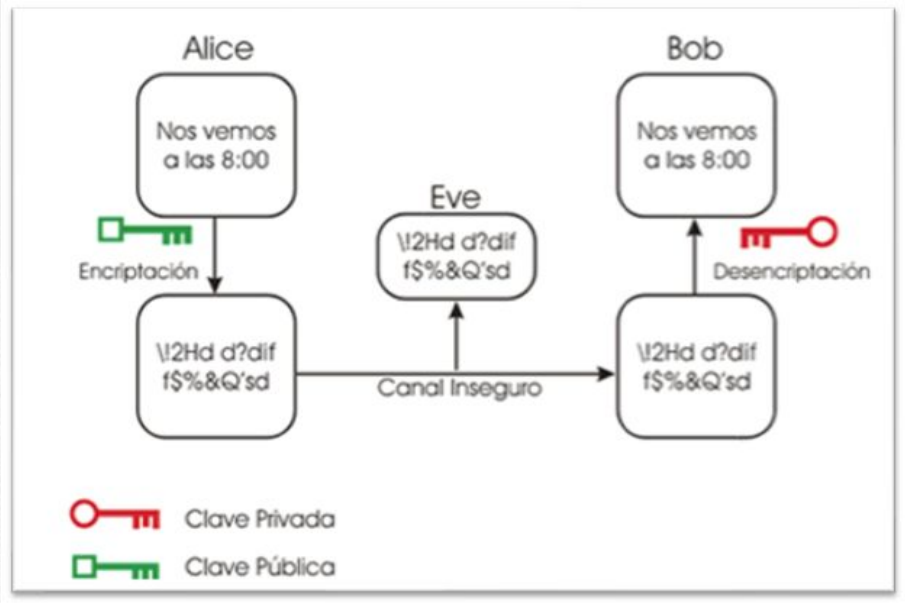
Criptografía Simétrica

- Cifrado simétrico con GnuPG sobre Linux

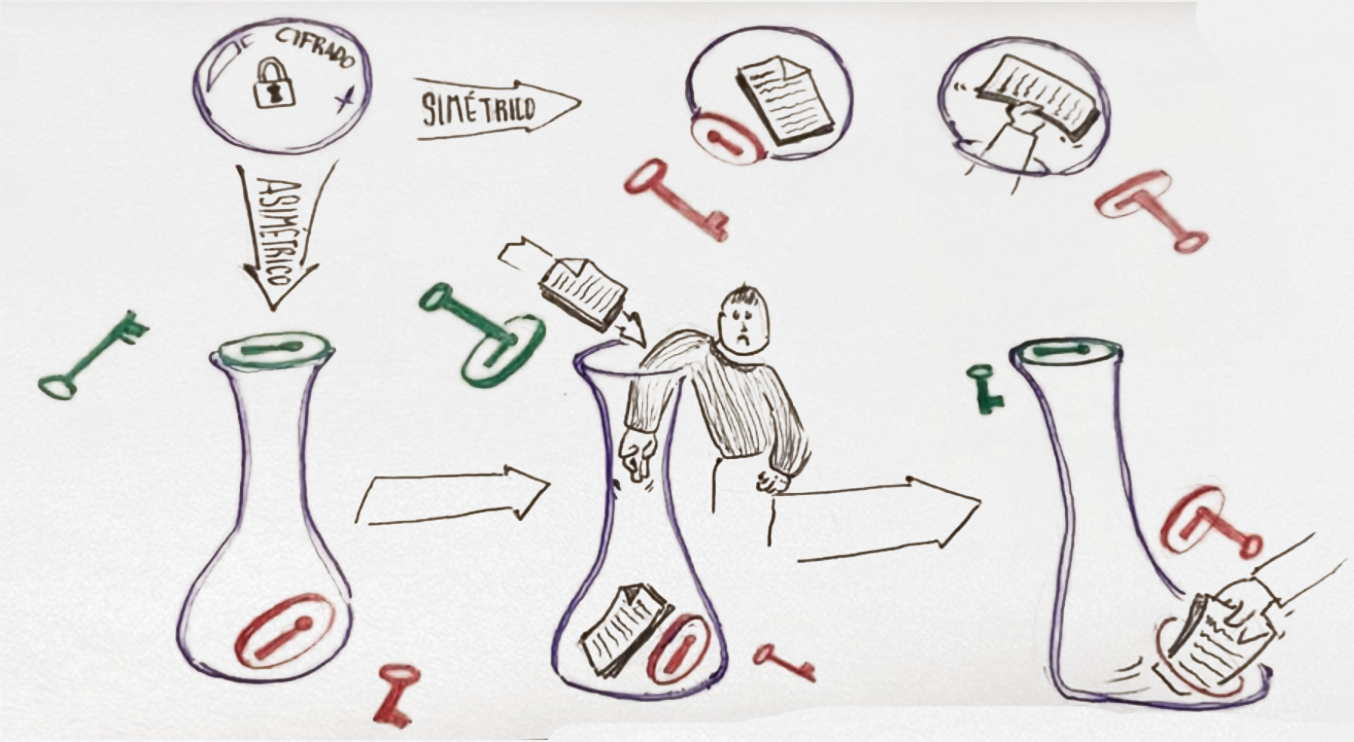
- Cifrado simétrico con IZArc sobre Windows

Criptografía Asimétrica

- Receptor y emisor disponen de una clave pública y otra privada para cifrar/descifrar el mensaje



Criptografía Asimétrica



Criptografía Asimétrica

- Clave matemáticamente relacionadas
- Lo que cifras con una solo lo puedes descifrar con la otra
- Imposible deducir la clave privada con la pública

Criptografía Asimétrica

- Ventajas

  - Menor número de claves
  - Utilización medios no seguros
  - Firma digital (no repudio)

- Desventajas

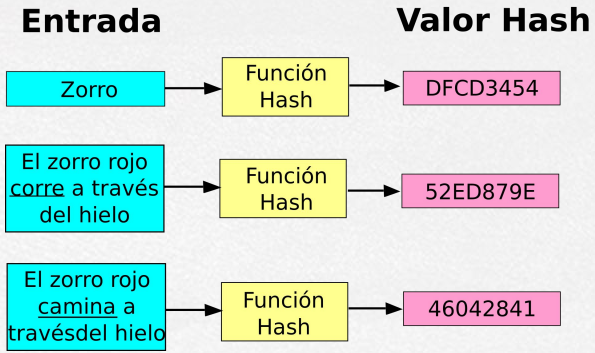
  - Poco eficientes
  - Proteger clave privada (con criptografía simétrica)
  - Importante backup de la clave privada

Criptografía Asimétrica

- Cifrado asimétrico con GnuPG sobre Linux

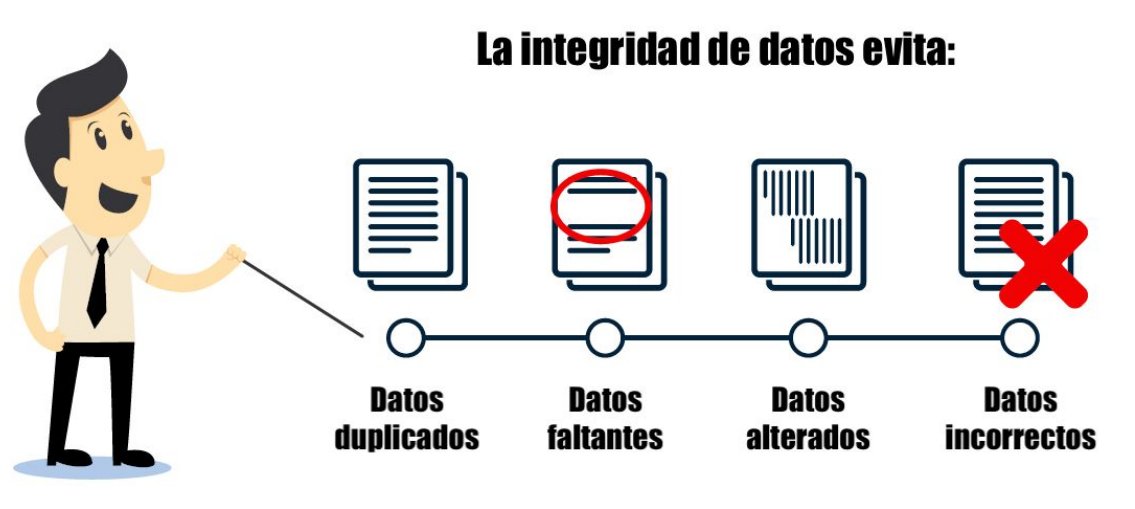
Criptografía Función Hash

- Algoritmo (operaciones matemáticas, lógicas,...)
- Transforma unos datos en una serie de caracteres con longitud fija
    - Genera un valor a partir de una cadena de texto utilizando una función matemática
    - Identifica de forma única a un fichero, disco duro,...



Criptografía Función Hash

- Protege la integridad de los datos



Criptografía Función Hash

- Principales Algoritmos
  - MD5, SHA
- Reglas
  - Números generados con un mismo método tienen igual tamaño
  - Imposible reconstruir texto base a partir del Hash
  - Computacionalmente sencillo de calcular

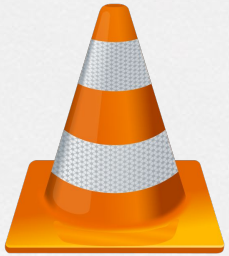
Criptografía Función Hash

- Ejemplo
  - Código ASCII
  - Agrupar de 3 en 3
  - Función matemática (1º - 2º) * 3º

E	n		u	n		l	u	g	a	r		d	e	
69	110	32	117	110	32	108	117	103	97	114	32	100	101	32
-1312			224			-927			-544			-32		-2591
l	a		M	a	n	c	h	a		d	e		c	u
108	97	32	77	97	110	99	104	97	32	100	101	32	99	117
352			-2200			-485			-6868			-7839		-17040
														-19631

Criptografía Función Hash

- Comprobación Hash
  - VLC y Hash Generator



Downloading VLC 3.0.11 for Windows 64 bits

Thanks! Your download will start in few seconds...

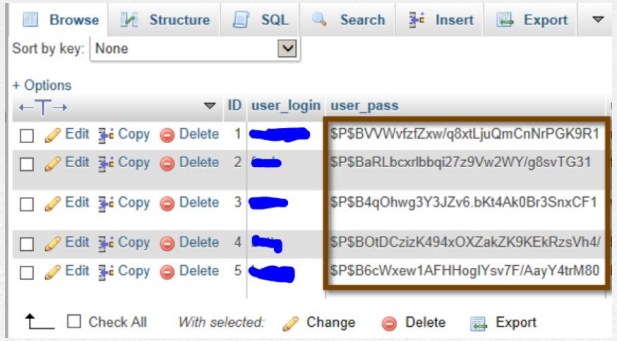
If not, click here. SHA-256 checksum: 2e41f1959ad77c34746715da5027c5ed554c35361397c9984a9ef78bc0b5e937

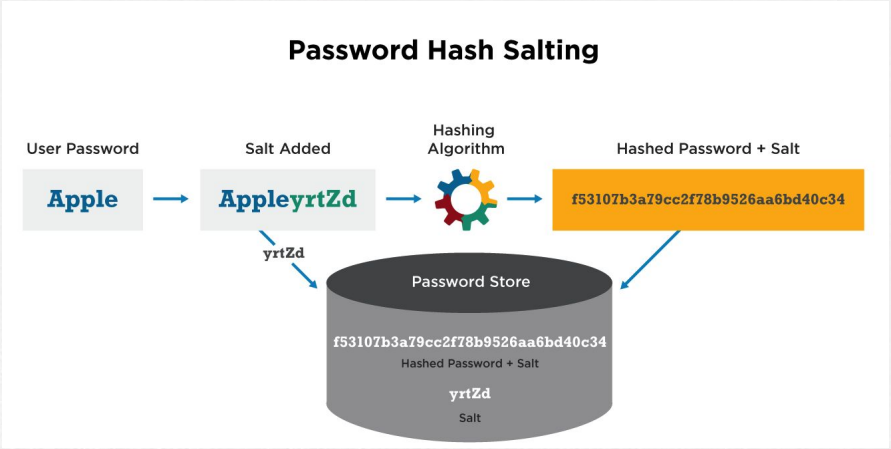
Criptografía Función Hash

- Crear Hash
  - WinMD5 en Windows
  - MD5sum en Linux

Criptografía Función Hash

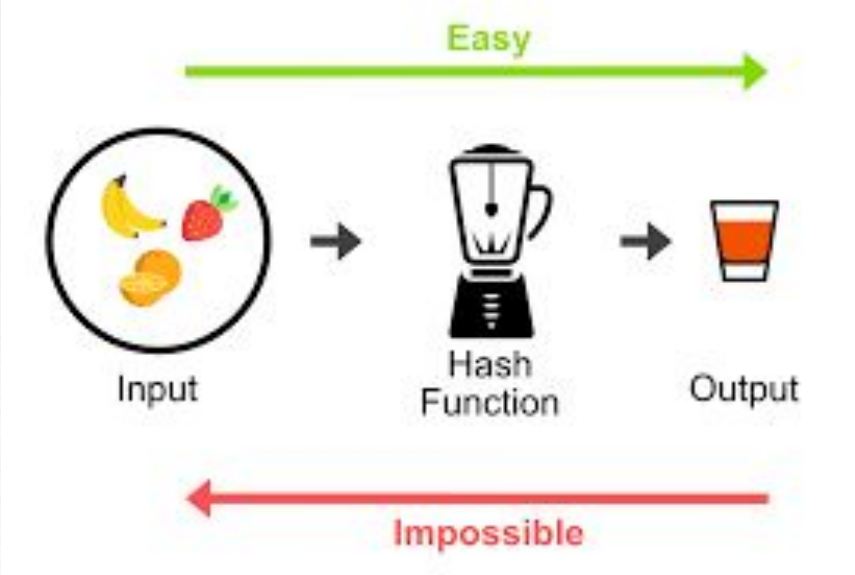
- Reverse Hashing
  - Password Hasheadas





Criptografía Función Hash

- Reverse Hashing
  - https://md5hashing.net/hash

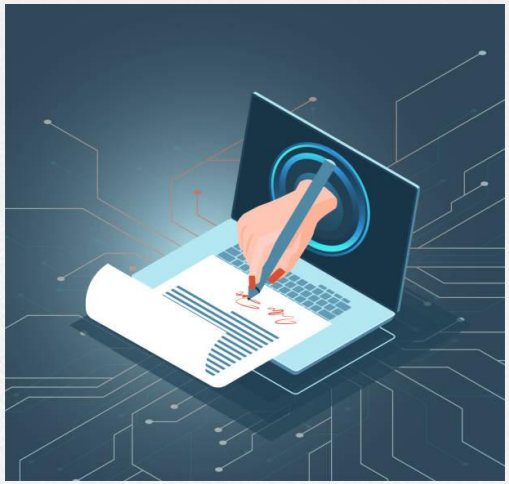


Criptografía Función Hash

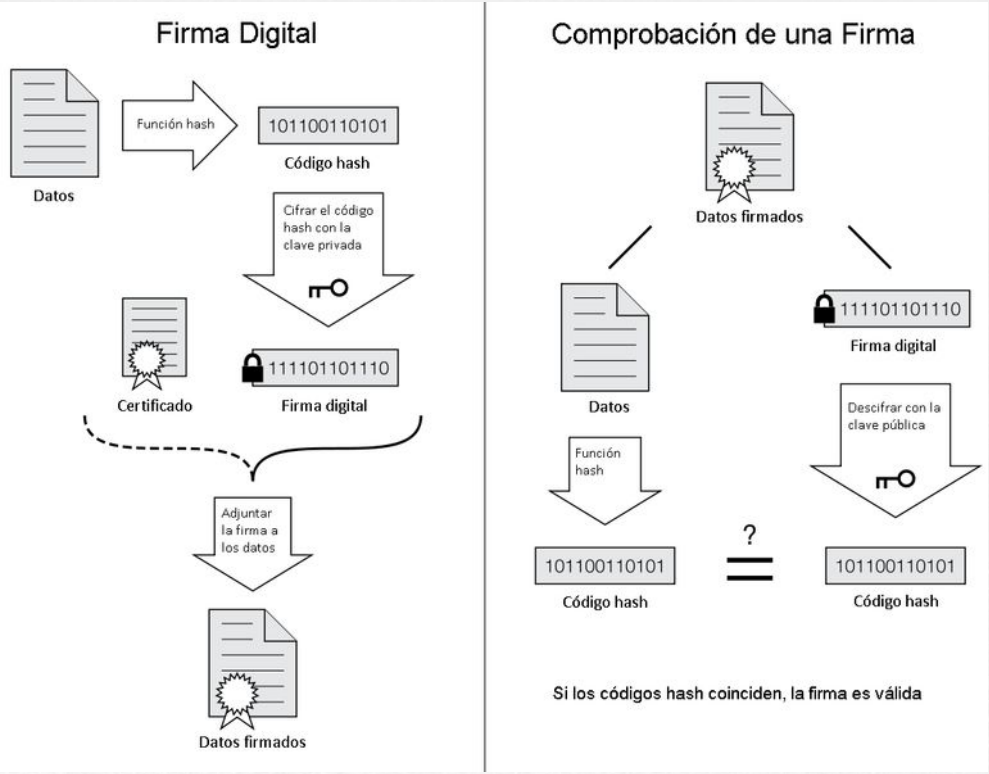
- Son ataques de diccionario

Criptografía Firma Digital

- Método criptográfico
  - Asocia la identidad de una persona/equipo informático a un mensaje/documento
  - Certificado digital



Criptografía Firma Digital



Criptografía Firma Digital

- Firma digital con GnuPG sobre Linux

- Firma digital con Gpg4win sobre Windows

Criptografía Cuántica

- Futuro de la criptografía
  - Cómo mandar un mensaje secreto con criptografía cuántica (https://www.youtube.com/watch?v=7R7dnT2043M)