

## **Laboratorio #5**

### **Estudiante:**

Andrés Arias Medina

### **Curso**

Seguridad en los Datos

### **Profesor**

Javier Omar Contreras Rodriguez



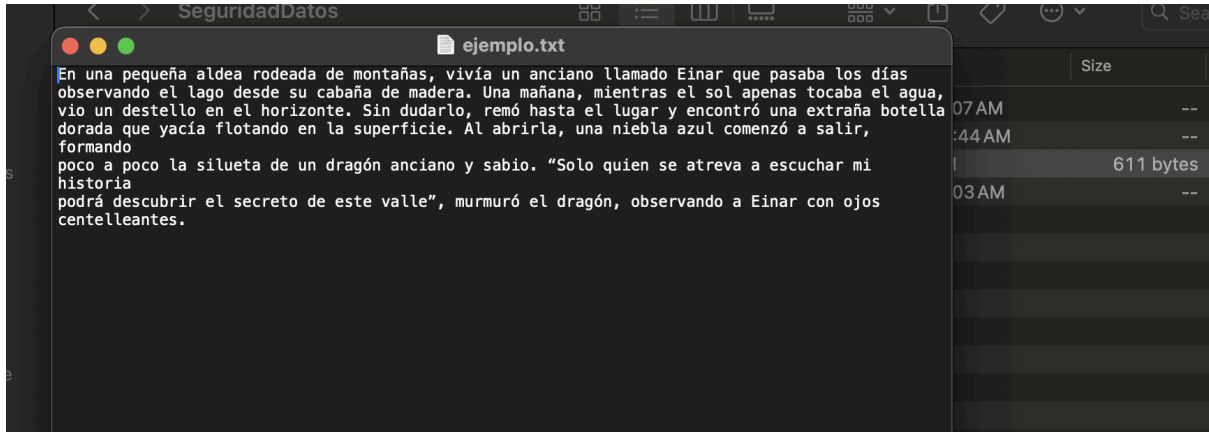
Universidad Pontificia Bolivariana

2 de noviembre de 2024

Medellín, Colombia

## Parte 1


Lo primero será crear un archivo aleatorio con los cinco renglones solicitados para la creación del archivo txt.



Guardamos el archivo y extraemos su hash usando un enlace compartido por el docente. El hash obtenido es el siguiente:

```
f7b5395fc60735587d953b723a7da91efa3633988bbc6a08c2313f689c9e1a0f
```

Select a file to hash from your system

Choose File  ejemplo.txt

2 Choose your hash function

☐ MD5 | 128-bit


☐ SHA-1 | 160-bit

☒ SHA-256 | 256-bit

☐ SHA-512 | 512-bit

3 Launch the hashing process

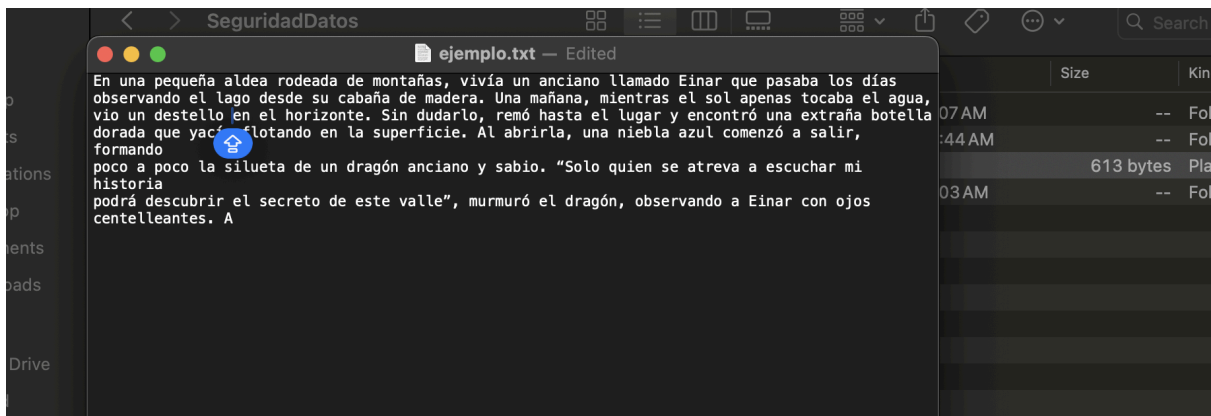
Launch hash process



Your file hash :

f7b5395fc60735587d953b723a7da91efa3633988bbc6a08c2313f689c9e1a0f

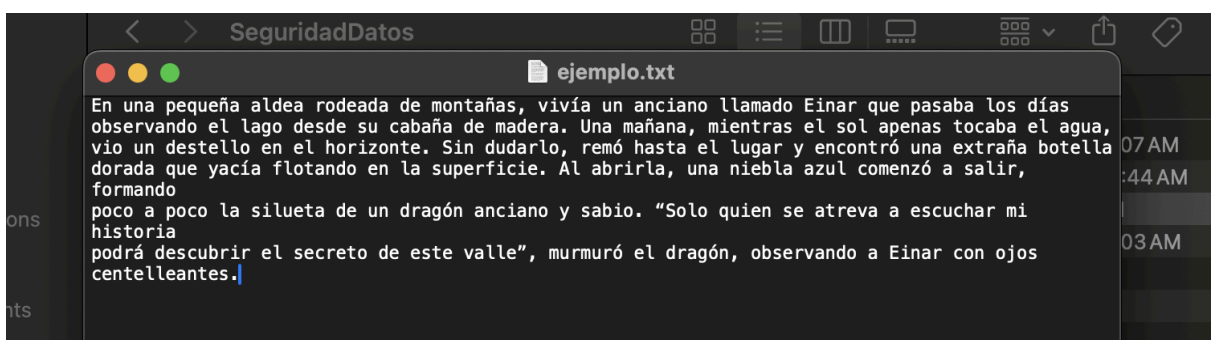
Ahora volvemos al editor y le agregamos al .txt un espacio y una letra mayúscula



Volvemos el enlace para recalcular el hash, que por teoría debería ser diferente al primero que se calculó.

A screenshot of a web-based hash calculator interface. The interface is dark-themed and has three main steps: 1. 'Select a file to hash from your system' with a 'Choose File' button and a file named 'ejemplo.txt' selected. 2. 'Choose your hash function' with four radio button options: 'MD5 | 128-bit', 'SHA-1 | 160-bit', 'SHA-256 | 256-bit' (selected), and 'SHA-512 | 512-bit'. 3. 'Launch the hashing process' with a 'Launch hash process' button. Below the button is a green progress bar. At the bottom, it says 'Your file hash :' followed by the hash value '3cc09a3148a6a2c579b80f97ac93f1ee9be85f80de753904f171b6aff9fbd52b'.


Efectivamente fue diferente, ahora se restaurará el archivo .txt suprimiendo el espacio y el carácter en mayúscula.



Se calcula nuevamente el hash que deberá ser idéntico al primero que se sacó.

Select a file to hash from your system

Choose File

 ejemplo.txt

2

 Choose your hash function

☐ MD5 | 128-bit

☐ SHA-1 | 160-bit

☒ SHA-256 | 256-bit

☐ SHA-512 | 512-bit

3

 Launch the hashing process

Launch hash process

Your file hash :

f7b5395fc60735587d953b723a7da91efa3633988bbc6a08c2313f689c9e1a0f

Resumen de los hash:

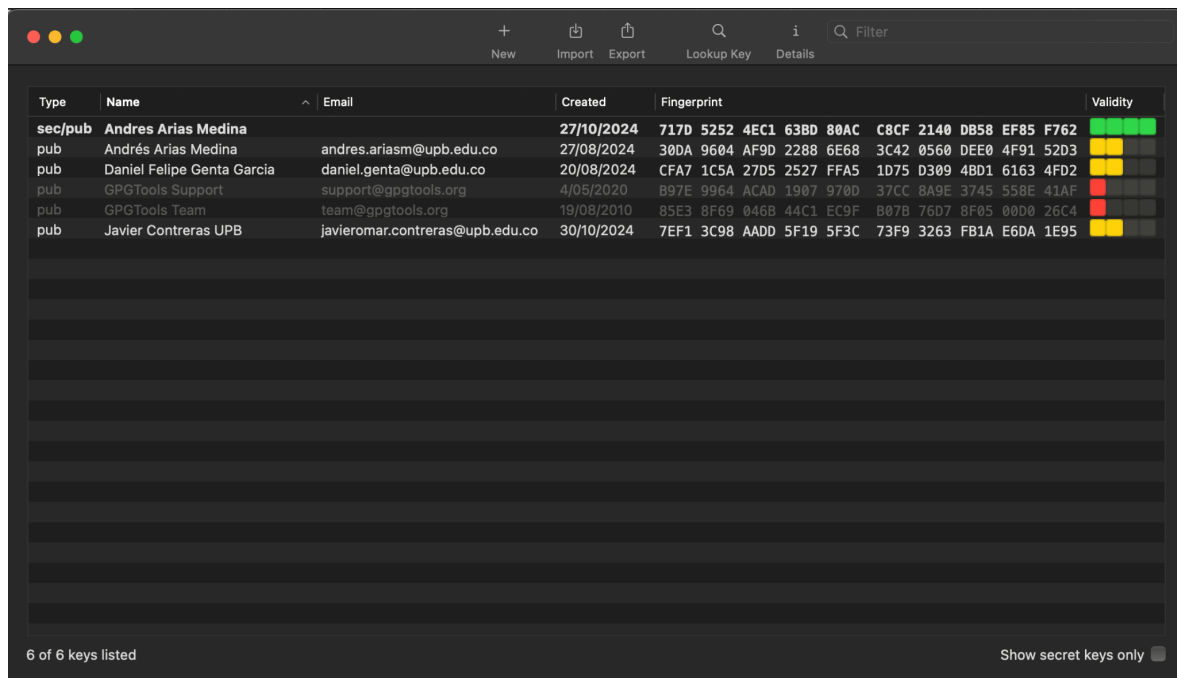
# de documento	Hash (SHA-256)
Documento base	f7b5395fc60735587d953b723a7da91efa3633988bbc6a08c2313f689c9e1a0f
Documento con cambios	3cc09a3148a6a2c579b80f97ac93f1ee9be85f80de753904f171b6aff9fbd52b
Documento con los cambios suprimidos	f7b5395fc60735587d953b723a7da91efa3633988bbc6a08c2313f689c9e1a0f

La propiedad involucrada es la de **"sensibilidad a cambios"** o **"efecto avalancha"**. Este efecto implica que cualquier modificación, incluso la de un solo carácter visible o no visible (espacio), produce un *hash* completamente diferente asegurando que los cambios mínimos en los datos originales resulten en resúmenes únicos. Esta propiedad es esencial en ciberseguridad para verificar la integridad de los datos: si el *hash* cambia, se sabrá que el archivo ha sido alterado.

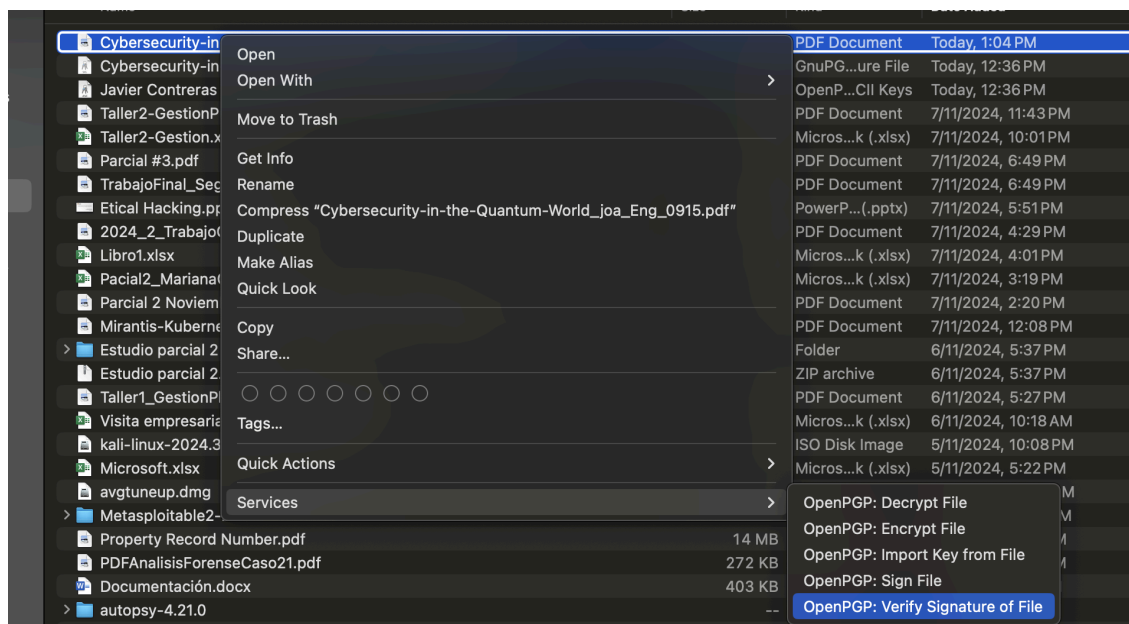
## Parte 2

Esta sección consta de verificar que el documento enviado por el docente cuente con una firma digital válida a través de la verificación por llaves.

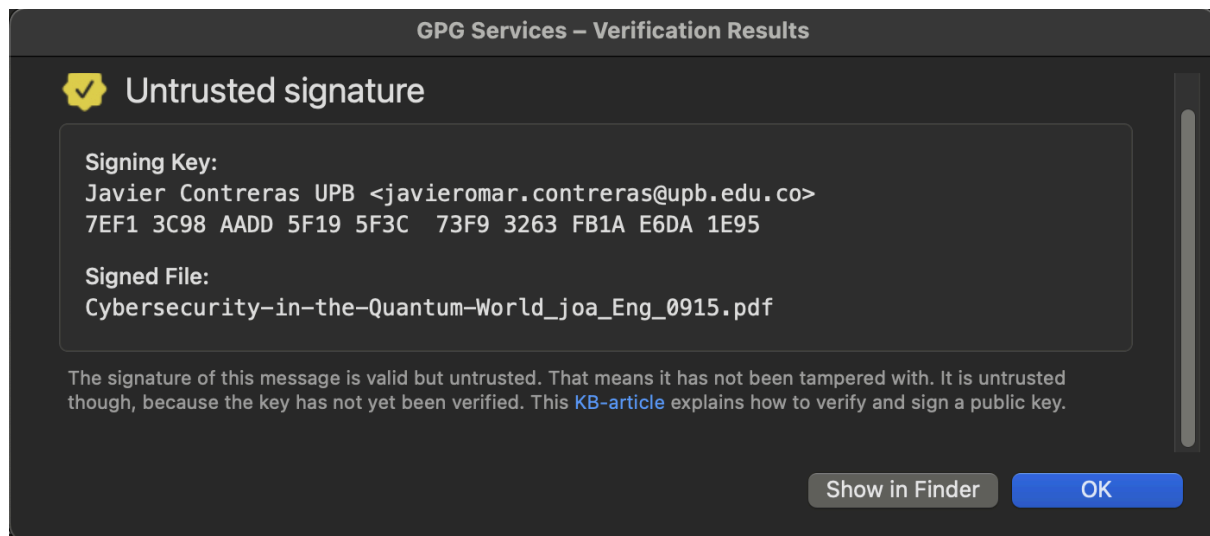
Lo primero será descargar la llave pública del docente y cargarla en GPG Keychain (Lo mismo que Kleoptara pero para macOS).



Una vez tengamos este paso se descarga el archivo pdf al que le verificaremos la firma digital. Lo seleccionamos y hundimos la opción de verificar.

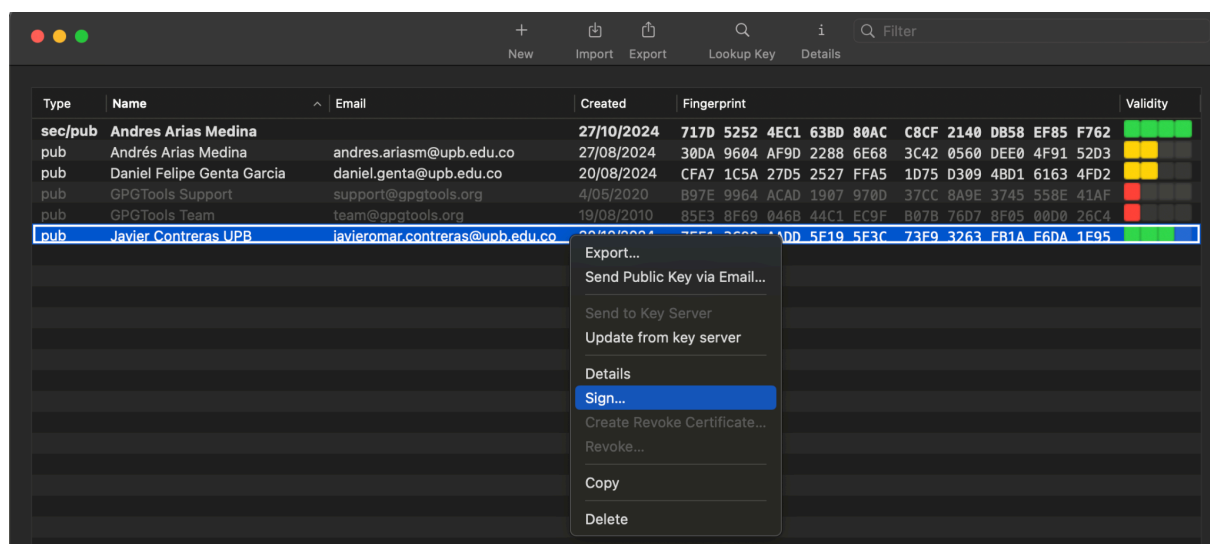


El resultado de la operación es que efectivamente se encuentra firmado el documento por el docente. Evidenciado gracias al uso de la llave pública compartida para dicho propósito.



El mensaje significa que la firma del mensaje ha sido verificada como válida, es decir, la integridad del mensaje se mantiene y no ha sido alterado. Sin embargo, la firma no es de confianza porque la clave pública utilizada para verificarla aún no ha sido confirmada o no es de confianza.

Para arreglar este problema debemos ir a GPG Keychain y certificar la llave pública del docente.



Seguimos los pasos que ahí nos indica e ingresamos la clave para verificación. Luego si intentamos verificar nuevamente la firma digital el resultado será muy distinto.

GPG Services – Verification Results



## Trusted signature

Signing Key:

Javier Contreras UPB <javieromar.contreras@upb.edu.co>  
7EF1 3C98 AADD 5F19 5F3C 73F9 3263 FB1A E6DA 1E95

Signed File:

Cybersecurity-in-the-Quantum-World\_joa\_Eng\_0915.pdf

Show in Finder

OK