2021

Práctica 2

FRANCISCO JAVIER LÓPEZ CALDERÓN

UT 6. Criptografía y Sistemas Identificación

P6.2 – Cifrado Asimétrico Funciones HASH

Objetivo

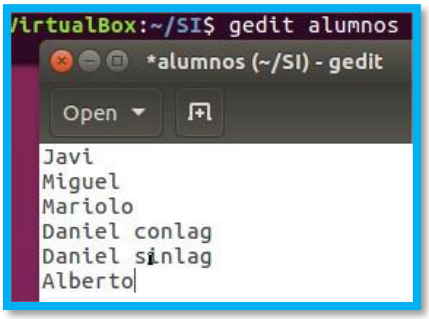
La integridad de un archivo, asegurar que su contenido no ha cambiado se puede comprobar mediante un **valor resumen** o **valor hash** calculado. Las funciones hash se utilizan para crear una cadena de longitud fija o resumen de mensaje a partir de una cadena de entrada de longitud variable.

Consideraciones previas

En el caso de GNU/Linux podemos emplear el comando **`md5sum nombredearchivo`** y nos calculará el valor resumen MD5 (Message Digest), pudiendo contrastarlo con el valor original

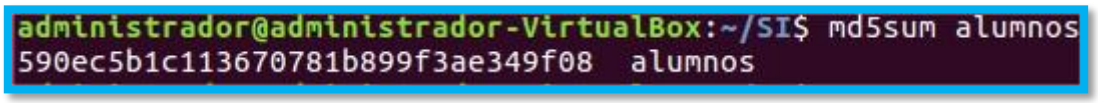
Desarrollo de la práctica

1. Calcula el valor MD5 de cualquier archivo plano que tengas o crea uno con los nombres y apellidos de los componentes del grupo de prácticas.



2. Modifica una única letra del archivo. Vuelve a calcular su valor MD5.

Tras cambiar una letra, procedo a utilizar md5sum



Podemos comprobar que el número identificador es diferente.

3. Compara los resultados y rellena la siguiente tabla:

TEXTO ORIGINAL	MD5
Javi Miguel Mariolo Daniel conlag Daniel sinlag Alberto	1816a2f7317620917aec391020ca24aa
TEXTO MODIFICADO	**MD5**
Javi Miguel Mariolo Daniel conlag Daniel sinlag AlbertA	590ec5b1c113670781b899f3ae349f08

Para verificar el resultado automáticamente, se puede guardar el resultado en un archivo con extensión.md5:

```
md5sum nombre_de_archivo > nombre_del_hash.md5
```

Las **comprobaciones** posteriores se realizan sobre el hash con la opción –c. El hash busca directamente el archivo de origen contenido en el propio hash.

```
md5sum  -c nombre_del_hash.md5
```

4. Calcula el valor resumen del archivo original y guárdalo.

```
administrador@administrador-VirtualBox:~/SI$ md5sum alumnos > VResumenalumnos.txt
administrador@administrador-VirtualBox:~/SI$ cat VResumenalumnos.txt
590ec5b1c113670781b899f3ae349f08  alumnos
```

5. Realiza la comprobación con la opción –c. ¿Qué mensaje nos da la comprobación?

```
administrador@administrador-VirtualBox:~/SI$ md5sum -c VResumenalumnos.txt
alumnos: OK
```

6. Modifica mínimamente el archivo (sin guardar el nuevo md5), y realiza una nueva comprobación. ¿Qué mensaje nos da ahora la comprobación?

Al modificar el archivo "*alumnos*" cuando se realiza la comprobación da error ya que la suma no es exacta.

```
administrador@administrador-VirtualBox:~/SI$ gedit alumnos
administrador@administrador-VirtualBox:~/SI$ md5sum -c VResumenalumnos.txt
alumnos: FAILED
md5sum: WARNING: 1 computed checksum did NOT match
```