Práctica título:

Tema 5. Criptografía.

Título: Funciones hash.

Alumno: Carla García Parra

Sumario

Práctica título:

Objetivo.

Calcular y verificar la función resumen (hash de un fichero) de forma manual y automática. Se utilizará un fichero de texto y se verificará . Posteriormente se modificará el fichero y se comprobará que el hash no coincide.

También se utilizarán las funciones hash para verificar la integridad de una descarga .

El servidor Apache .	https://httpd.apache.org/download.cgi
La interfaz de desarrollo java Netbeans	https://netbeans.org/downloads/
El mapeador de redes nmap	https://nmap.org/book/install.html#inst-integrity
El analizador de tráfico	https://www.wireshark.org/download.html
El procesador de textos openoffice	https://www.openoffice.org/download/checksums.html
Oracle VirtualBox	https://www.virtualbox.org/wiki/Downloads

Fuentes bibliográficas.

Enlaces a las fuentes documentales.
https://www.redeszone.net/2010/11/09/criptografia-algoritmos-de-autenticacion-hash/
https://www.maketecheasier.com/check-sha1-sha256-sha512-hashes-on-linux/
https://www.redeszone.net/2016/07/09/descubre-los-mejores-mas-seguros-algoritmos-hash-conoce-los-no-recomendables-hoy-dia/?utm_source=related_posts&utm_medium=widget

juicio crítico
https://pthree.org/2016/06/28/lets-talk-password-hashing/

Algunas utilidades para el cálculo de hashes :
https://www.blq-software.com/FileChecksumUtility/index-EN.html
https://www.softzone.es/2017/05/06/generar-hash-archivos-file-checksum-utility/
http://www.winmd5.com/

Material necesario.

Todo lo realizado en la práctica ha sido desde Ubuntu 20 (virtualbox) y programa VokoScreen desde Windows 10

Dificultades e imposibles.

– obligatorio –

Indicar si:

No han habido dificultades
Dificultades encontradas y solucionadas
Dificultades encontradas y no solucionadas.

Cuestiones.

Si las hay en el enunciado del libro o bien han surgido durante la realización de la práctica.

Práctica título:

Investigación.

Qué se podría haber hecho y no se ha hecho.
Qué novedades han surgido que nos interesan.

Echad un vistazo a este artículo que habla de la utilización de las funciones hash en criptomonedas y haced un resumen de 5 líneas .
https://www.oroyfinanzas.com/2014/01/aplicacion-funciones-hash-unidireccionales-bitcoin/

En criptografía a este tipo de funciones que generan resúmenes se les denomina funciones hash. Son funciones que convierten una cantidad de bits de tamaño arbitrario a un conjunto reducido de bits denominado resumen, típicamente 128 ó 160 bits.
los algoritmos estándar de funciones hash desarrollados y utilizados desde la década de los 90, como MD5 o SHA-1, hoy en día o están rotos o significativamente amenazados. Bitcoin no se basa en ninguno de ellos porque utiliza SHA-256 como función hash principal y ECDSA junto a RIPEMD-160 en el proceso de creación de direcciones.

Realización y resultados.

Procedimiento y pasos realizados. Resultados obtenidos. – obligatorio –

1. Leed el artículo del enlace https://www.redeszone.net/2010/11/09/criptografia-algoritmos-de-autenticacion-hash/ para conocer las funciones hash que hay . Haced un resumen .

Un hash es un algoritmo matemático que lo que hace es transformar cualquier dato que entra en una serie de caracteres de salida, con una longitud de salida fija, esta longitud tiene que ser la misma aunque el tamaño de los datos de entrada cambien.
Se utilizan para proteger las contraseñas y no guardarlas en texto claro de una base de datos. Al aplicar hash a las contraseñas, ya sea para almacenarlas en el disco o para crear claves de cifrado, se deben utilizar criptográficas basadas en contraseñas, diseñadas específicamente para el problema a tratar. No se deben utilizar funciones hash de propósito general de ningún tipo, debido a su velocidad. Además, no deberían implementar su propio algoritmo de «estiramiento de claves», como el hash recursivo de su resumen de contraseña y salida adicional.

2. Cómo calcular los hashes en Ubuntu https://www.maketecheasier.com/check-sha1-sha256-sha512-hashes-on-linux/ .

   gtkhash
   md5sum documento documento_copia > documento_final
   md5sum documento documento_copia > documento_final

3. Usad md5 para calcular y verificar el hash de un fichero. ¿ Qué procedimiento de verificación utilizas ? , descríbelo .

-md5sum documento > documento_final
-md5sum -c documento_final

He utilizado el comando md5sum para crear el md5 del fichero y la salida de ese comando la metí en un numero documento para comprobar la integridad de ese hash con el mismo documento utilizando el parámetro -c

Práctica título:

Necesitamos que los documentos estén la misma ubicación para que la comprobación pueda funcionar

4. Idem pero la verificación ha de hacerse automáticamente

-md5sum -c documento documento_final
Utilizamos el comando -md5sum -c hash para verificar automáticamente
Necesitamos añadir los dos ficheros en uno, en el comando md5sum y utilizar el parámetro -c del comando para que se realice su comprobación

Verifica la integridad de las siguientes descargas (hay varios algoritmos) :

5. El servidor Apache . https://httpd.apache.org/download.cgi

   sha256sum httpd-2.4.51.tar.bz2 > apache
   sha256sum -c apache

   sha512sum httpd-2.4.51.tar.bz2 > apache2
   sha512sum -c apache2

6. La interfaz de desarrollo java Netbeans https://netbeans.org/downloads/

   sha512sum netbeans-12.5-source.zip > netbeans
   sha512sum -c netbeans

7. El mapeador de redes nmap https://nmap.org/book/install.html#inst-integrity

   md5sum nmap-7.92.tar.bz2 > mdnmap
   sha1sum nmap-7.92.tar.bz2 > sha1nmap
   sha224sum nmap-7.92.tar.bz2 > sha224nmap
   sha256sum nmap-7.92.tar.bz2 > sha256nmap
   sha384sum nmap-7.92.tar.bz2 > sha384nmap
   sha512sum nmap-7.92.tar.bz2 > sha512nmap

   md5sum -c mdnmap
   sha1sum -c sha1nmap
   sha224sum -c sha224nmap
   sha256sum -c sha256nmap
   sha384sum -c sha384nmap
   sha512sum -c sha512nmap

8. El analizador de tráfico https://www.wireshark.org/download.html

   sha256sum Wireshark-win64-3.4.9.exe > wire256
   sha1sum Wireshark-win64-3.4.9.exe > wire1

   sha256sum -c wire256
   sha1sum -c wire1

9. El procesador de textos openoffice https://www.openoffice.org/download/checksums.html

   sha256sum Apache_OpenOffice_4.1.11_Linux_x86-64_install-deb_es.tar.gz > libresha256

Práctica título:

sha256sum -c libresha256

sha512sum Apache_OpenOffice_4.1.11_Linux_x86-64_install-deb_es.tar.gz > libre512
sha512sum -c libre512

10. Oracle VirtualBox https://www.virtualbox.org/wiki/Downloads

    sha256sum virtualbox-6.1_6.1.26-145957~Ubuntu~eoan_amd64.deb > virtual256
    sha256sum -c virtual256

    md5sum virtualbox-6.1_6.1.26-145957~Ubuntu~eoan_amd64.deb > virtualmd5
    md5sum -c virtualmd5

11. ¿ Porqué el autor de los ficheros descargados proporciona los hashes con distintos algoritmos ?

Utilizan varios algoritmos para tener más seguridad y así es menos probable que se puedan alterar.