Actividad 14. Uso de funciones Hash

Una **función** criptográfica **hash** es **un algoritmo** matemático que **transforma cualquier dato entrante en una serie de caracteres de salida, con una longitud fija** o variable, dependiendo del algoritmo hash que estemos utilizando. En los algoritmos de hash con longitud de salida fija, esta longitud será la misma independientemente del tamaño de los datos de entrada. Los algoritmos hash que están específicamente diseñados para proteger contraseñas, suelen ser variables.

Utilización de las funciones Hash

1. **proteger las contraseñas y no guardarlas en texto claro en una base de datos**
   Para comprobar que hemos introducido correctamente una contraseña que está guardada en una base de datos (se almacena el hash de la clave), lo que se hace es aplicar el algoritmo hash a la contraseña introducida y compararla con la almacenada, si es igual, la clave es correcta, si es diferente, la clave es incorrecta. Este procedimiento se utiliza en todos los sistemas operativos, webs con autenticación de usuario/clave etc.

2. **Asegurar la integridad de datos transmitidos**
   La manera de usarlas para este fin es **comprobar los hashes creados antes y después de la transmisión de datos**, de esta manera, si los hashes son totalmente idénticos significará que la comunicación ha sido segura y que los datos no han sido alterados, de lo contrario, algo ha fallado de por medio y los datos obtenidos al **final de la comunicación no son los mismos que los que se emitieron al inicio.**

3. **Para introducirlos en listas negras**
   Por ejemplo, se pueden usar para detectar diferentes canciones o películas protegidos por derechos de autor.
4. **Para detectar Malware**
   En algunos sistemas antimalware, se compara el valor hash de un malware conocido con la información almacenada en un disco.
5. **Para la firma digital**
   Al realizar la firma de un documento, se hace un hash del mismo. Al revisar el documento, se le aplica de nuevo la función hash y si no coincide, indica que ha sido modificado.

Propiedades de buen algoritmo de hash

- **Determinismo:** Siempre le brinda una salida de tamaño idéntico, independientemente del tamaño de la entrada con la que comenzó, esto significa que, si está codificando una sola oración, la salida resultante debe ser del mismo tamaño que la que obtendría al codificar un libro completo.
- **Resistencia previa a la imagen:** No es factible invertir un valor hash para recuperar el mensaje de texto sin formato de entrada original, por lo tanto, el concepto de hash es irreversible, tiene funciones unidireccionales.
- **Resistencia a la colisión:** Una colisión ocurre cuando dos objetos chocan. Bueno, este concepto se traslada a la criptografía con valores hash, si dos muestras únicas de datos de entrada dan como resultado resultados idénticos, se conoce como colisión. Esta es una mala noticia y significa que el algoritmo que está utilizando para codificar los datos no funciona y, por lo tanto, es inseguro, básicamente, la preocupación aquí es que alguien podría crear un archivo malicioso con un valor hash artificial que coincida con un archivo genuino (seguro) y hacerlo pasar por real porque la firma coincidiría, por lo tanto, un algoritmo hash bueno y confiable es aquel que es resistente a estas colisiones.
- **Efecto de avalancha:** Cualquier cambio realizado en una entrada, sin importar cuán pequeño sea, dará como resultado un cambio masivo en la salida.
- **Velocidad hash:** Los algoritmos hash deben funcionar a una velocidad razonable, en muchas situaciones, los algoritmos hash deberían calcular los valores hash rápidamente, esto se considera una propiedad ideal de una función hash criptográfica.

Tipos de algoritmos de hash más utilizados

MD5

Es una función hash popular y ampliamente usada, diseñada a principios de la década de 1990 como una función hash criptográfica. Trabaja con bloques de 512 bits y genera resúmenes de hash de 128 bits (128/4 = 32 caracteres hexadecimales). MD5 fue publicada en 1992, y aunque durante estos años fue usada y adoptada en forma generalizada, se han descubierto varias vulnerabilidades durante los últimos años por lo que actualmente se recomienda usar algoritmos más seguros.

SHA-1

Secure Hash Algorithm (SHA) . Los algoritmos de hash seguro son una familia de funciones de hash criptográficas publicadas por el Instituto Nacional de Estándares y Tecnología (NIST) como un estándar federal de procesamiento de información (FIPS) de EE. UU; que incluyen: SHA-1, SHA-2 y SHA-3

SHA-1 trabaja con bloques de 512 bits y genera un resumen hash de 160 bits. Se utiliza en protocolos como TLS/SSL, PGP SSH y en IPsec.

Fue diseñado por la Agencia de Seguridad Nacional (NSA) para ser parte de Digital Signature Algorithm. Se descubrieron debilidades criptográficas en SHA-1, y el estándar ya no fue aprobado para la mayoría de los usos criptográficos después de 2010.

SHA-2

Se compone de una familia de dos funciones hash similares, con diferentes tamaños de bloque, conocidas como SHA-256 y SHA-512 . Se diferencian por el tamaño de las palabras; SHA-256 usa palabras de 32 bytes (256/8) donde SHA-512 usa palabras de 64 bytes (512/8). De SHA-2, también hay versiones truncadas de cada estándar, conocidas como SHA-224 , SHA-384 , SHA-512/224 y SHA-512/256 . Estos también fueron diseñados por la NSA.

Las funciones hash SHA-2 están implementadas en una gran variedad de aplicaciones y protocolos de seguridad, como por ejemplo: TLS y SSL, PGP, SSH, S/MIME, PPCoin y IPsec.

La moneda criptográfica Bitcoin depende en gran medida en un doble uso del SHA-256.

A finales de 2013, los mejores ataques públicos consiguieron romper las 46 de las 64 iteraciones del SHA-256 y 46 de las 80 iteraciones del SHA-512.

SHA-3

Es una función hash anteriormente llamada Keccak , elegida en 2012 después de una competencia pública entre diseñadores que no pertenecen a la NSA. Admite las mismas longitudes de hash que SHA-2 y su estructura interna difiere significativamente del resto de la familia SHA.

SHA-3 es muy diferente al actual SHA-2, sin embargo el NIST afirma que este nuevo algoritmo no pretende sustituir de momento al actual SHA-2, quien no ha demostrado por el momento ninguna vulnerabilidad, sino que simplemente pretende ser un salvoconducto por si ocurre algo con el estándar actual. Los investigadores de seguridad afirman que se tardan años en crear un nuevo estándar, y por ello han querido estar preparados para el futuro desarrollando y estandarizando este nuevo algoritmo que, sin duda, protegerá de la mejor forma posible la información de los usuarios.

Herramientas para generar hash online

File Checksum

Es una sencilla herramienta web que permite la generación de hashes. Tan solo es necesario arrastrar el archivo desde la ubicación en donde está, hasta el sitio web. O bien, puedes hacer clic en el cuadro donde dice «Drop File Here» y subes el archivo. No solamente puedes generar hashes en SHA2-256 sino también con otras funciones hash que existen. Específicamente, 29 algoritmos de hash tanto para Hashes de Archivos como de texto plano. Una ventaja importante es que no necesitas realizar registro previo, sólo accede a la web y ya podrás utilizarlo.

HTML5 File Hash Online Calculator

Es otro sitio web que no necesita de registro previo para generar hashes de archivos. Los algoritmos que soporta son MD5, SHA-1, SHA-256, SHA-384 y SHA-512. También cuenta con un algoritmo que se describe como la implementación más rápida de los algoritmos SHA (WebCryptoAPI), el cual se aplica para archivos de menos de 512 GB de peso.

Defuse Online Text & File Checksum Calculator

Otra herramienta más que puedes encontrar en Internet para generar hashes. Es compatible con texto tipo ASCII o UNICODE y en cuanto a archivos, no tiene limitaciones en cuanto a formato, pero sí de tamaño (5 MB). Una de sus ventajas es que ni los datos ni los hashes que se generan son almacenados en el servidor del sitio.

Herramientas para generar hash

QuickHash

QuickHash se trata de una una herramienta de hashes de datos de código abierto para los sistemas operativos Linux, Windows y Apple Mac OS, cuenta con una interfaz gráfica de usuario muy amigable y fácil de utilizar. Esta herramienta actualmente soporta los siguientes algoritmos hash: MD5, SHA1, SHA-3 (256 bits), SHA2-256, SHA2-512, xxHash, Blake2B (256 bits) y Blake3, por tanto, es una herramienta realmente completa. Por si todo esto fuera poco, debemos indicar que es totalmente gratuita, y su desarrollo se sostiene gracias a las donaciones de las personas que la usan.

HashMyFiles

Es un programa portable que permite la generación de hashes en forma masiva. Es decir, puedes seleccionar más de un archivo a la vez para que pueda generar los hashes para cada uno. Soporta los algoritmos SHA (todas sus variantes) y CRC32. Es posible crear un acceso a HashMyFiles en el menú contextual para que cada vez que selecciones archivos o incluso carpetas, puedas contar con este programa para poder importarlos a este y crear los hashes. Es compatible con Windows a partir de la versión 2000.

MultiHasher

Consiste en otra herramienta super compacta y sencilla de usar. Se especializa en generar hashes masivamente, por carpetas y subcarpetas e incluso, indicando la ruta de lo que queremos generar. Soporta todos los algoritmos conocidos.

MD5 & SHA Checksum Utility

Es un software gratuito que genera tipos de hash SHA-512, SHA-1, MD5, SHA-256 a partir de un archivo determinado. También verifica la integridad del archivo. Para la verificación del hash, o para generar un hash, debe seleccionar el archivo deseado, luego seleccionar uno de estos dos hashes SHA-1 o MD5. Después de eso, debe hacer clic en verificar o copiar para verificar la integridad del archivo o generar el hash.

MD5 Hash Check

Práctico programa, también gratuito, para generar y verificar valores hash de archivos MD5, Whirlpool, CRC16, Panama, Tiger, RIPEMD320, RIPEMD 256, RIPEMD160, SHA512, SHA384, SHA256, SHA224, SHA1, CRC32. Con la ayuda de este software, puede verificar fácilmente la integridad de dos archivos. Se puede agregar fácilmente al menú contextual y, además, compara fácilmente los valores hash de dos archivos proporcionados.

Hash Generator

Genera rápidamente hashes de la familia MD5, MD2, MD4, CRC32, ADLER32, WHIRLPOOL, RIPEMD 160, HAVAL256-4 y SHA. Este software ayuda a verificar la integridad del archivo. El principal inconveniente de este programa es que no se pueden comparar hashes con él. También está disponible en una versión portable.

Se pide:

1. Descarga una de las aplicaciones indicadas para hacer Hash
2. Calcula el Hash con varios algoritmos de los siguientes textos:
   - Seguridad informática
   - Utilizamos cookies opcionales para mejorar tu experiencia en nuestros sitios web, como a través de conexiones en redes sociales, y para mostrar publicidad personalizada en función de tu actividad en línea. Si rechazas las cookies opcionales, solo se utilizarán las cookies necesarias para prestarte nuestros servicios. Puedes cambiar tu selección si haces clic en 'Gestionar cookies' al final de la página.
   - Gr5!Q4$tkZAfB05N
3. Calcula el Hash con varios algoritmos de los archivos subidos a la plataforma
4. Busca en Internet algún archivo para descargar (Imagen iso, pdf, etc.) que tenga un hash para comprobarlo. Descarga el archivo, aplica el hash y comprueba que no se ha modificado.