Criptografía asimétrica

La Criptografía de clave pública o asimétrica, también denominada RSA por las siglas de los apellidos de sus inventores Rivest Shamir y Adelman, es por definición aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se llama clave pública y otra para descifrar que es la clave privada. El nacimiento de la Criptografía asimétrica ocurrió como resultado de la búsqueda de un modo más práctico de intercambiar las llaves simétricas

El esquema propuesto en RSA se explica así:

Mediante un programa de cómputo cualquier persona puede obtener un par de números, matemáticamente relacionados, a los que se denominan llaves. Una llave es un número de gran tamaño, que usted puede conceptualizar como un mensaje digital, como un archivo binario, o como una cadena de bits o bytes. Las llaves, públicas y privadas, tienen características matemáticas, su generación se produce siempre en parejas, y se relacionan de tal forma que, si dos llaves públicas son diferentes, entonces, las correspondientes llaves privadas son diferentes y viceversa. En otras palabras, si dos sujetos tienen llaves públicas diferentes, entonces sus llaves privadas son diferentes. La idea es que cada individuo genere un par de llaves: pública y privada. El individuo debe de mantener en secreto su llave privada, mientras que la llave pública la puede dar a conocer.

El procedimiento de firma de un documento digital, por ejemplo, implica que, mediante un programa de cómputo, un sujeto prepare un documento a firmar y su llave privada (que sólo él conoce). El programa produce como resultado un mensaje digital denominado firma digital. Juntos, el documento y la firma, constituyen el documento firmado.

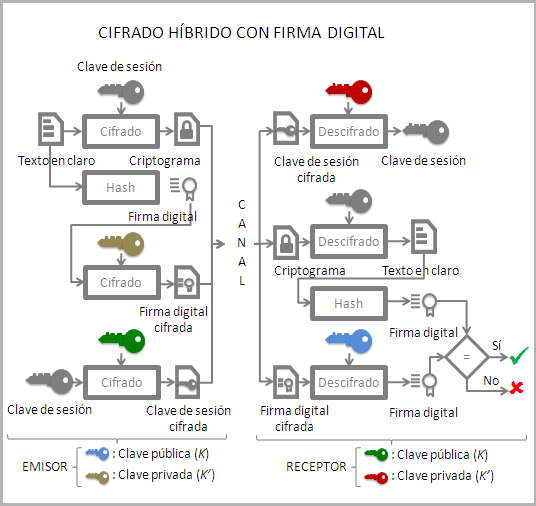
Es conveniente señalar que, a diferencia de la firma autógrafa, si dos documentos son diferentes entonces la firma digital también es diferente. En otras palabras, la firma digital cambia de documento a documento, si un sujeto firma dos documentos diferentes producirá dos documentos firmados diferentes. Si dos sujetos firman un mismo documento, también se producen dos documentos firmados diferentes.

El proceso de autentificación se efectúa de la siguiente forma:

Dos puntos I y II mantienen comunicación, conociendo I la llave pública de II. Desde el punto II, se envía un documento firmado digitalmente y un criptograma asociado que sólo es posible hacerse utilizando su clave privada. Entonces I, utilizando la llave pública de II genera un criptograma reflejo, compara ambos criptogramas y, si son iguales, el documento es auténtico.  
Si alguna parte del documento o parte de la firma se modifica, aunque sea ligeramente, entonces, el procedimiento de autentificación indicará que el documento no es auténtico. Si una llave pública autentifica un documento firmado, entonces el documento fue firmado con la correspondiente llave privada, es decir, si un individuo tiene asociada la llave pública que autentifica el documento, entonces, el documento fue efectivamente firmado por ese individuo.

A diferencia de la firma autógrafa, que es biométrica, y efectivamente prueba el acto personal de firma, la firma digital sólo prueba que se utilizó la llave privada del sujeto y no necesariamente el acto personal de firma. En consecuencia, no es posible establecer con total seguridad que el individuo firmó un documento, sino que sólo es posible demostrar que es el individuo es el responsable de que el documento se firmara con su llave privada. En otras palabras, si un documento firmado corresponde con la llave pública de un sujeto, entonces el sujeto, aunque no lo haya hecho, debe de reconocer el documento como auténtico.

Por lo tanto, el sujeto debe cuidar de mantener su llave privada en total secreto y no revelársela a nadie, porque de hacerlo es responsable de su mal uso.



Tecnicas de HASH

Las técnicas hash se establecen como métodos que mediante una ecuación fueron creados para generar posiciones en una tabla (arreglo) que será la que contendrá datos. Surge, por tanto, la necesidad de comprender las diferentes funciones como: SHA-1, SHA-3, SHA-256

Dentro del mundo de las estructuras de datos existe un sinfín de temas que conllevan diferentes métodos, funciones y aplicaciones para explotar en el contexto de programación; con el objetivo de innovar con soluciones que den soluciones a actividades de la cotidianidad

Al hablar de hashing estamos refiriéndonos a una tabla que almacena tanto registros como objetos, para después realizar una búsqueda de la cual su prioridad es tener un constante tiempo de recuperación en base a 0 y 1 sin tomar en cuenta qué cantidad de elementos puedan están dentro de una table

La manera correcta para poder lograr ese objetivo es crear una tabla de gran medida para abarcar cada elemento que se pueda almacenar y luego guardar cada objeto dentro de una posición con el valor clave del objeto.

Las técnicas hashing o tablas de dispersión se han creado para crear mediante una ecuación y una clave de entrada, como parte fundamental, un dato que será una posición en un arreglo

La función hash cumple con una operación fundamental y es que, si queremos buscar el objeto que guardamos en “x posición”, mediante la clave y la ecuación, podremos obtener el archivo guardado, sin importar si los elementos en arreglo están ordenados o no, y sin importar cuál sea el tamaño del arreglo, ya que las técnicas hashing son unos de los métodos de búsqueda más rápido, lo cual es una gran ventaja. Es posible que ocurra que a la hora de generar una posición en el arreglo o a la hora de buscar un elemento, la posición generada ya existe o nos devuelva un dato no deseado, en caso de la búsqueda, esto se conoce como colisiones. Importante conocer que dada dos claves diferentes k1 y k2 nos deberían dar resultados diferentes.

UTILIZACIÓN DEL HASH

Las diferentes funciones Hash que existen son utilizadas más que nada para resguardar la integridad de los archivos de grandes empresas, para certificación que las páginas web, proteger los derechos de autor de libros, películas, y otros contenidos que se encuentran en internet. Un ejemplo claro del uso de Hash es en las contraseñas, ciertos servicios en línea generan una función hash cuando el usuarios crean sus contraseñas, estos servicios en línea no guardan en texto plano las contraseñas de sus usuarios ya que esto significaría un problema grande en caso de que sufran de algún ataque a sus Base de Datos, generando una función Hash de la contraseña de los usuarios será más difícil de descifrar cuál será la contraseña en texto plano brindando mayor seguridad a los usuarios resguardando su información.

De acuerdo a lo analizado, las empresas que quieran mantener su información a salvo tendrán que cambiarse a las mejoras del SHA-1 que son: SHA-3 Y SHA-256.

SHA-3, SECURE HASH ALGORITM, fue creado a partir del SHA-2 como una actualización para solventar errores que se encontraban dentro de ese método. Debido a que los navegadores como Google Chrome, Internet Explorer entre otros utilizan el método SHA-1 tiene una baja seguridad que estos diseñadores demoraron solo 10 días en descubrir, Google informó que su navegador cambiaría a SHA3 durante el año 2017 y de igual manera lo realizan otras empresas como Microsoft

SHA 256, son nuevas funciones hash que utilizan palabras de 32 bits a 64 bits, la función SHA 256 pertenece a la familia del SHA-2. Esta función participa para la autenticación de software, y para la firma de mensajes

