Beneficios de la implementación de seguridad SHA-2 en la creación de firmas electrónicas avanzadas

Diana Dolores De la Cruz Arias, José Ney Garrido Vázquez, José Ángel Jesús Magaña, Alejandro Hernández Cadena, José Manuel Gómez Zea

Tecnológico Nacional de México Campus Villahermosa, Cd. Industrial; Departamento de Postgrado e Investigación; Carretera Villahermosa Frontera, Km. 3.5, Cd. Industrial, Villahermosa Tabasco, CP: 86010

Resumen

Las funciones hash son técnicas que se utilizan para crear valores que representan un conjunto de datos. También se le conoce como hash al resultado de dicha función, estas se utilizan para diversas aplicaciones, entre ellas:

- Verificar la autenticidad de archivos.
- Firmas electrónicas.

Hay una variedad extensa de funciones hash que pueden ser utilizadas, sin embargo, las más conocidas son MD5, SHA-1 y SHA-2.

La firma electrónica es un método criptográfico a la cual se le asocia la identidad de un sujeto a un mensaje, asegurando la integridad de dicho mensaje o documento.

Para que esto sea posible, se debe calcular el hash del mensaje, encriptar el resultado con la llave privada del sujeto, y posteriormente se adjunta al documento con el certificado, esto sin la llave privada, únicamente con la pública.

Finalmente, para autenticar la firma electrónica del documento, se debe verificar la fecha de validez, que la entidad certificadora sea de confianza, etc. Se obtiene el hash encriptado y se desencripta con la llave pública, se calcula el hash del documento y se comprueba que ambos hashes sean iguales.

Abstract

Hash functions are techniques are used to create values that represent a data set. The result of this function is also known as a hash, these are used for various applications, including:

- Verify the authenticity of the files
- Electronic signatures

There are a wide variety of hash functions that can be used, however, the best known are MD5, SHA-1, and SHA-2.

An electronic signature is a cryptographic method to which the identity of a subject is associated with a message, ensuring the integrity of message or document. to make this possible, the message hash must be calculated, the result must be encrypted with the subject's private key, and subsequently attached to the document with the certificate, without the private key, only with the public key.

Finally, to authenticate the electronic signature of the document, the validity date must be verified, the certifying entity is trustworthy, etc. The encrypted hash is obtained and decrypted with the public key, the document hash is calculated and it is verified that both hashes are equal.

Palabras clave: SHA-2, Firma electrónica avanzada, Llave pública, Llave privada.
Keywords: SHA-2, Advanced Electronic Signature, Public Key, Private Key.

1 INTRODUCCIÓN

La utilización de documentos digitales supone un importante desafío que es determinar la autenticidad del mismo, la firma electrónica puede dar solución a este desafío, ya que está basada en procedimientos criptográficos.

Su función es similar a la firma autógrafa, ser un sello irrefutable que permita autenticar la identidad de una entidad.

El receptor podrá comprobar que la firma en el documento es auténtica y que este no haya sufrido alguna alteración.

El sistema de la firma electrónica avanzada está conformado por dos partes:

Un método que no permita alterar la firma y otro que permita comprobar que la firma pertenece al firmante.

Cualquier entidad puede adquirir mediante un algoritmo un par de número matemáticamente relacionados, los cuales son denominados llaves o claves.

Una llave se puede definir como un mensaje o una cadena de bits. Cada sujeto tiene una llave pública que puede ser proporcionada a cualquiera y una privada que debe mantenerse en secreto para evitar mal uso de la firma electrónica.

Estas llaves están relacionadas de modo que todo lo que se encripte con una de ellas, solo podrá ser desencriptada por la otra.

Para poder firmar un documento se aplica sobre él mismo una función hash que permite obtener un valor hash, es decir, el resumen del documento.

La creación la firma electrónica se produce mediante un algoritmo que combina los caracteres de la llave pública con los caracteres que conforman al documento.

Para validar que un documento firmado sea válido, el receptor del mismo debe crear un valor hash del documento y desencriptar la firma electrónica con la llave pública del firmante, una vez que se obtengan los valores hash, se deben comparar para verificar la autenticidad del documento.

Si existe alguna alteración en el documento o la firma, el procedimiento de autenticación indicará que el documento firmado no es auténtico.

Si se desea que la firma electrónica tenga validez legal, se debe conocer la llave pública del o los firmantes, para que puedan autenticar los documentos firmados y existir de por medio un marco legislativo, de lo contrario se tendrá que suscribir un acuerdo formal utilizando la firma autógrafa, donde se reconozcan y acepten sus respectivas llaves públicas.

2 FIRMA ELECTRÓNICA AVANZADA

El término "Firma digital" erróneamente se utiliza a menudo para definir lo mismo que "Firma electrónica avanzada".

Según un artículo publicado por la Secretaría de la Función Pública la Firma Electrónica Avanzada (conocida en México como FIEL) es un conjunto de datos que se adjuntan a un mensaje electrónico, cuyo propósito es identificar al emisor del mensaje como autor legítimo de éste; como si se tratara de una firma autógrafa (Secretaría de la Función Pública, 2013).

Por sus características, la FIEL brinda seguridad a las transacciones electrónicas de los contribuyentes, con su uso se puede identificar al autor del mensaje y verificar que no haya sido modificado.

Los documentos en lo que se plasma una firma autográfa pierden valor legal al momento de ser digitalizados, ya que, estas pueden ser editadas, alteradas, reemplazadas o falsificadas por terceros.

ISSN: 2007-4786

Por ello, en la tabla 1, se muestran las características clave que representan el uso de la Firma Electrónica Avanzada a diferencia de la Firma autógrafa.

Si bien las firmas digitales comunes pueden usar una variedad de métodos para autenticar a los firmantes, como la dirección de correo electrónico, la identificación de la compañía o la verificación por teléfono, las firmas electrónicas avanzadas usan un método específico, como una identificación digital basada en un certificado.

La identificación electrónica avanzada incluye un certificado con una clave privada y una clave pública. La clave privada se usa para crear una firma basada en un certificado. Los certificados son credenciales que se aplican automáticamente a los documentos firmados.

Las firmas electrónicas avanzadas en los documentos pueden ser muy útiles ya que no pueden modificarse ni editarse sin comprometer la validez de la firma.

Con el uso de la firma electrónica avanzada las transacciones son más seguras ya que permite reconocer quien es el autor del mensaje y comprobar que este no haya sufrido algún cambio.

Anteriormente se mencionó que el diseño de la firma electrónica se basa en estándares de infraestructura de claves, en los cuales se hace uso de las llaves pública y privada para el envío de mensajes:

La llave privada es conocida únicamente por el titular de la firma electrónica avanzada ya que sirve para cifrar datos.

La llave privada únicamente puede cifrar los mensajes.

Una llave privada puedes cifrar y descifrar, sin embargo, esto último no es de suma importancia. El destinatario envía su llave pública y con ella se cifra la información que recibirá. Las llaves permiten que los usuarios puedan validar su identidad frente a otros usuarios y utilizar los certificados que le permitirán cifrar y descifrar mensajes, utilizar su firma digital, etc.

La idea de resguardar las comunicaciones mediante el cifrado de mensajes se remonta a la antigüedad, sin embargo, los esquemas de firma electrónica se hicieron realidad en el año de 1970 con el desarrollo del encriptamiento de la clave pública.

Consecuentemente, para comprender el funcionamiento de la firma electrónica avanzada, en primer lugar, se debe tener conocimiento de términos básicos como la función hash, la criptografía de la llave pública y privada.

Características	Firma electrónica	Firma autógrafa
Puede ser utilizada en documentos digitales y transacciones	Si	No
El proceso de validación de la firma electrónica se puede automatizar	Si	No
La firma permite encontrar cambios en un documento	Si	No
Tiene validez legal	Si	Si

Tabla 1. Comparación de la firma electrónica avanzada y la firma autógrafa.

ISSN: 2007-4786

3 FUNCIÓN HASH

Uno de los principales elementos de un sistema de firma digital es el hash. Este involucra la conversión datos de cualquier tamaño en valores de tamaño fijo. El valor resultante producido por la función hash se denomina valor hash o resumen de mensaje.

Cuando se combina con el cifrado, se puede usar una función hash criptográfica para generar un valor hash (resumen) que se puede usar como una huella digital única. Es decir, que, si surge algún cambio en los mensajes, esto da como resultado un valor hash.

Debido a eso las funciones criptográficas hash son muy utilizadas para validar que los datos digitales sean auténticos.

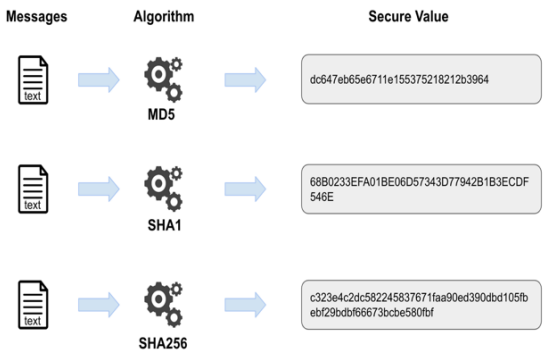

Figura 1. Tabla hash

En las funciones hash se utiliza un algoritmo de cifrado para generar un certificado y una clave de autenticación para usar entre el servidor y el cliente, y para cifrar la contraseña de autenticación de la base de datos. En este proceso, decidimos qué algoritmo cifra los datos. Existen algoritmos como MD5, SHA1 y SHA2 en el algoritmo de cifrado.

La siguiente figura muestra el resultado del método de cifrado: SHA1 es más complicado que MD5 y SHA256 es más complicado que SHA1.

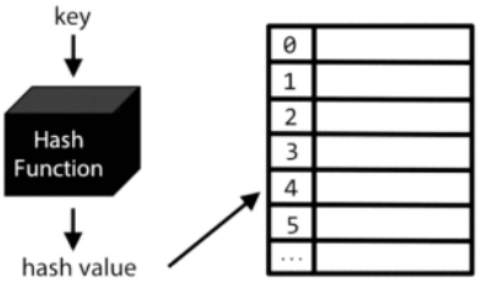

Figura 2. Resultado de método de cifrado.

3.1 FUNCIÓN SHA-2

En el año 2005 la National Institute of Standards and Technology (NIST) prohibió el uso de las funciones basadas en SHA-1 para generar firmas electrónicas y otras aplicaciones que requieren resistencia a colisiones debido a la vulnerabilidad en su funcionamiento para replicar firmas en diferentes archivos. Por ello la NIST recomienda el uso de las funciones basadas en SHA-2.

SHA-2 (es decir, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 y SHA-512/256): las agencias federales pueden usar estas funciones hash para todas las aplicaciones que emplean algoritmos hash seguros. NIST alienta a los diseñadores de aplicaciones y protocolos a implementar SHA-256 como mínimo para cualquier aplicación de funciones hash que requiera interoperabilidad (National Institute of Standards and Technology, 2015).

Según el equipo de soporte de SSL, SHA-2 (Algoritmo de hash seguro 2) se refiere a una familia de funciones de hash criptográficas que pueden convertir cadenas de datos arbitrariamente largas en resúmenes de un tamaño fijo (224, 256, 384 o 512 bits). SHA-2 de 256 bits, también conocido como SHA-256, es la versión más utilizada. El resumen se muestra comúnmente como un número hexadecimal de valor fijo. SHA-256, por ejemplo, devuelve un código de 64 caracteres (SSL, 2015).

Actualmente sha-2 es la función de cifrado más utilizado y adoptado en la mayoría de los campos.

Tiene la ventaja de una alta velocidad de salida. Además, es imposible descifrar con un método de cifrado unidireccional. Aunque el nivel de protección efectivo puede ser inferior a SHA-384, 512 o SHA-3, hasta el momento no existen deficiencias significativas en los problemas de estabilidad, y debido a su velocidad, se usa ampliamente para certificados, Blockchains, etc.

Todas las versiones existentes del algoritmo de hash seguro se crearon de acuerdo con el principio de Merkle-Damgard.

En criptografía, la construcción Merkle-Damgard o la función hash Merkle-Damgard es un método para construir funciones hash criptográficas resistentes a colisiones a partir de funciones de compresión unidireccionales.

Figura 3. Método de encriptación sha-2.

3.1.1 PARÁMETROS TÉCNICOS

Este protocolo es para datos divididos en partes, cada volumen es de 64 bytes. Este algoritmo proporciona integración donde aparece el código de 256 bits. La tecnología de cifrado se basa en una ronda relativamente simple y el ciclo es de 64 veces.

- Tamaño de bloque de 64 bytes
- La longitud máxima de un código cifrado es de 33 bytes.
- La opción de resumen del mensaje es de 32 bytes.
- El tamaño de palabra predeterminado es de 4 bytes.

- El número de iteraciones en un solo ciclo es 64.
- La velocidad del algoritmo es de 140 Mbps.

Como se mencionó anteriormente, el protocolo SHA-2 se basa en el concepto Merkle-Damgard. Esto significa que la división se realiza primero con bloques, luego solo con las palabras rotas.

Una serie de información pasa por una serie de iteraciones (64 u 80). Cada ciclo va acompañado de un bloque de conversión de palabras. El código hash resultante se genera sumando los valores originales.

4 INFRAESTRUCTURA DE LLAVE PÚBLICA (PKI)

La criptografía de llave pública es un sistema de cifrado que hace uso de un par de llaves que son: una llave púbica y una llave privada

Ambas claves están relacionadas matemáticamente y se pueden usar tanto para el cifrado de datos como para las firmas electrónicas.

La infraestructura de la llave pública puede cifrar los mensajes ocupando la llave pública y solamente puede descifrar los datos con su llave privada correspondiente, sin embargo, los sistemas antigüos utilizan una sola llave para cifrar y descifrar.

Es decir, que, está implícito el hash de datos digitales mediante la llave privada del firmante.

El receptor del mensaje puede usar la clave pública provista por el firmante para verificar que la firma sea válida.

En ciertas situaciones, las firmas digitales pueden incluir cifrado, pero este no es siempre el caso. Por ejemplo, la cadena de bloques de Bitcoin usa PKI y firmas digitales, pero al contrario de lo que muchos creen, el proceso no incluye cifrado.

5 LÍMITE

Los principales desafíos que enfrentan los esquemas de la firma electrónica provienen de tres requisitos mínimos.

- **Algoritmos:** Debido a la vulnerabilidad en la seguridad de las firmas electrónicas, se debe elegir una función hash que sea confiable.
- **Implementación:** Para que un sistema de firmas electrónicas no tenga fallas, el algoritmo debe ser óptimo.
- **Clave privada:** La clave privada no debe filtrarse o ser comprometida bajo ninguna circunstancia, ya que los atributos de autenticidad ya no serán válidos.

CONCLUSIONES

Las partes primordiales de los sistemas de firma electrónica son las funciones hash y la criptografía de la clave pública ya que actualmente son utilizadas en una amplia gama de aplicaciones.

ISSN: 2007-4786

Si estas son implementadas de la manera correcta, las firmas electrónicas pueden sugerir un gran aumento en cuanto a seguridad, integridad y permitir la validación y autenticación de cualquier tipo de datos.

Muchas burocracias actuales todavía se basan en el papeleo, pero a medida que avanzamos hacia sistemas más digitalizados, se adoptarán más esquemas de firma electrónica.

La firma electrónica implica seguridad y confianza y hoy en día el algoritmo SHA-1 ya no es seguro y por ello la NITS recomienda el uso del algoritmo SHA-2.

Las firmas electrónicas se han utilizado desde hace muchos años, sin embargo, aún hay mucho por explorar en este tema.

REFERENCIAS

[1]. (2018). Resultado de método de cifrado. [Figura]. Recuperado de https://www.keycdn.com/support/sha1-vs-sha256
[2]. Aoki, K., Guo, J., Matusiewicz, K., Sasaki, Y., & Wang, L. (2009, December). Preimages for step-reduced SHA-2. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 578-597). Springer, Berlin, Heidelberg.
[3]. Bellare, M., Boldyreva, A., Desai, A., & Pointcheval, D. (2001, December). Key-privacy in public-key encryption. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 566-582). Springer, Berlin, Heidelberg.
[4]. Carmona, I., & Eric, C. (2015). El reto de la firma electrónica notarial: su posible uso para autorizar todos los instrumentos notariales. Revista IUS, 9(36), 303-329.
[5]. Enciso, L. I. (2011). La implementación de la Firma Electrónica en México. Economía, 369.
[6]. Merkle, R. C. (1987, August). A digital signature based on a conventional encryption function. In Conference on the theory and application of cryptographic techniques (pp. 369-378). Springer, Berlin, Heidelberg.
[7]. Merkle, R. C. (1989, August). A certified digital signature. In Conference on the Theory and Application of Cryptology (pp. 218-238). Springer, New York, NY.
[8]. National Institute of Standards and Technology. (05 de Agosto de 2015). Hash Functions. Obtenido de Computer Security Resource Center: https://csrc.nist.gov/Projects/Hash-Functions/NIST-Policy-on-Hash-Functions
[9]. Nohe, P. (2018). Metodo de encriptación sha-2. [Figura]. Recuperado de https://www.thesslstore.com/blog/difference-encryption-hashing-salting/
[10]. Preneel, B. (1994). Cryptographic hash functions. European Transactions on Telecommunications, 5(4), 431-448.
[11]. Rogaway, P., & Shrimpton, T. (2004, February). Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In International workshop on fast software encryption (pp. 371-388). Springer, Berlin, Heidelberg.
[12]. Rosas, O. (2017). Tabla hash. [Figura]. Recuperado de https://compilandoconocimiento.com/2017/01/19/tablas-hash/
[13]. SSL, E. d. (10 de Noviembre de 2015). SSL. Obtenido de What Is SHA-2?: https://www.ssl.com/faqs/what-is-sha-2/

Correo electrónico autor: m19301420@villahermosa.tecnm.mx