Criptografía, Cifrando Sistemas Inteligentes

Mariano Esteban Romero Torres[*],
Miguel Alberto León Monterrosa[**]

Resumen

Este documento está enfocado en las firmas digitales y su proceso de elaboración. También se abordarán las funciones de resumen, su aplicación en las firmas digitales y sus principales problemas de seguridad (colisiones), así como de los desafíos en el uso de técnicas criptográficas para establecer la autenticidad de documentos electrónicos.

Palabras clave: clave pública, clave privada, certificado digital, criptografía asimétrica, criptografía simétrica, hash

Abstract

This paper is centered on digital signatures and the process of development. It also encompasses summary functions, its application in digital signatures, and its main security problems (collisions), as well as the mayor challenges in the use of cryptographic techniques to establish the authenticity of electronic documents.

Keywords: Private Key, Public Key, Digital Certificate, Asymmetric Cryptography, Symmetric Cryptography, Hash

* Ingeniero de Sistemas, Magister en Dirección Estratégica en Ingeniería de Software, Estudiante de Doctorado en Proyectos Universidad Nacional Abierta y a Distancia UNAD. Mariano.romero@unad.edu.co

** Ingeniero de Sistemas, Especialista en Redes y Telecomunicaciones, Estudiante Maestría en Seguridad Informática. Director de Software y Hardware Universidad del Sinú. miguelleon@unisinu.edu.co

Introducción

Uno de los principales desafíos que se plantea en la utilización de documentos electrónicos es establecer su autenticidad, es decir, la capacidad de asegurar si una determinada persona ha manifestado su conformidad con el contenido del documento electrónico. Este desafío es resuelto por lo que comúnmente se denomina como "firma digital", basada en procedimientos criptográficos. Su función respecto de los documentos digitales es similar a la de la firma de puño y letra en los documentos impresos: ser el sello irrefutable que permite atribuir a una persona algo escrito o su conformidad en un documento. El receptor, o un tercero, podrán verificar que el documento esté firmado, sin lugar a dudas, por la persona cuya firma aparece en el documento, sin que este haya sufrido alteración alguna. El sistema de firma digital consta de dos partes: un método que haga imposible la alteración de la firma y otro que permita verificar que la firma pertenece efectivamente al firmante.

Por su parte, los *hashs*, o funciones de resumen, son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija, que representa un resumen de toda la información dada. Esto quiere decir que, a partir de los datos de la entrada, se crea una cadena que solo puede volverse a crear con esos mismos datos.

Estas funciones tienen varios objetivos, diferentes a los de la criptografía simétrica y asimétrica; entre ellos, asegurar que no se ha modificado un archivo en una transmisión, hacer ilegible una contraseña o firmar digitalmente un documento.

Referente Teórico

La palabra criptografía viene del griego krypto, oculto, y graphéin, escribir. Hacer criptografía, entonces, puede entenderse como cifrar o codificar mensajes para evitar que su contenido pueda ser leído por un tercero no autorizado. El cifrado es el arte y la técnica de escribir con procedimientos o claves secretas, o de un modo enigmático, de tal forma que lo escrito sea inteligible solo para quien sepa descifrarlo o cuente con las herramientas o permisos para hacerlo.

Por otra parte, los sistemas inteligentes son un conjunto de elementos integrados mediante una estructura organizada con alta sensibilidad para responder adecuada, oportuna y eficientemente a los problemas derivados de su interacción con el entorno.

Figura 1. Sistemas Inteligentes

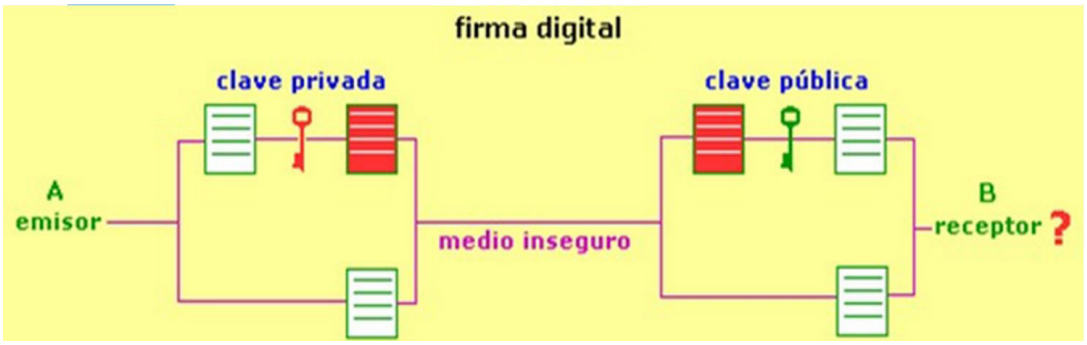
Fuente: Eadic, 2015.

Al hablar de criptografía, también se hace uso de conceptos importantes como el algoritmo MD5, los certificados y firmas digitales, cifrado simétrico y cifrado asimétrico y la aplicabilidad de estos conceptos al integrar a un sistema PKI. Para ello, se toma como entrada la necesidad de las organizaciones de asegurar y garantizar la privacidad, la integridad, la autenticación y el no rechazo.

La firma digital y las funciones hash

Una firma digital es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje. La firma digital no implica que el mensaje esté encriptado, es decir, que este no pueda ser leído por otras personas; al igual que cuando se firma un documento holográficamente este sí puede ser visualizado por otras personas. (Claudio Fernando, 2014).

Figura 2. Proceso de firma digital.



Fuente: Claudio Fernando, 2014.

Como se diagrama en la figura 2, el proceso de firma digital consta de dos partes bien diferenciadas. La primera de ellas es el proceso de firma, en el que el emisor encripta el documento con su llave privada, enviando al destinatario tanto el documento en claro como el encriptado. La segunda consiste en el proceso de verificación de la firma, en la que el receptor desencripta el documento cifrado con la clave pública de A y comprueba que coincide con el documento original, lo que atestigua de forma total que el emisor del mismo ha sido efectivamente A.

El esquema de firma digital mediante una función hash es el siguiente:

1. El emisor aplica una función hash conocida al documento, con lo que obtiene un resumen hash del mismo.

2. Encripta dicho resumen con su clave privada.

3. Envía al receptor el documento original plano y el resumen hash encriptado.

4. El receptor B aplica la función hash al resumen sin encriptar y desencripta el resumen encriptado con la llave pública de A.

5. Si ambos coinciden está seguro de que ha sido A el que le ha enviado el documento. Si no coinciden, está seguro de que no ha sido A o de que el envío ha sido interceptado durante el medio de envío y modificado.

Figura 3. Firma digital con resumen hash

Fuente: Claudio, 2014.

Las funciones hash y la firma digital son elementos indispensables para el establecimiento de canales seguros de comunicación, basados en los Certificados Digitales. Para que una función pueda considerarse como función hash debe cumplir con las siguientes condiciones

Unidireccionalidad. Dada la firma digital debe ser computacionalmente imposible recuperar el mensaje original.

Compresión. La firma digital debe ser de longitud fija, independientemente de la longitud del mensaje original.

Facilidad de cálculo. Dado el mensaje original, debe ser fácil calcular la firma digital de este.

Difusión. La firma digital debe ser una función compleja de todos los bits del mensaje, de tal forma que, si se modifica un solo bit, el hash resultante deberá cambiar al menos la mitad de sus bits aproximadamente.

Resistente a colisiones. Existen dos tipos:

- Colisión Simple. Dado el mensaje m_0, debe ser computacionalmente imposible obtener otro mensaje m_1, tal que el hash de m_0 sea idéntico al de m_1.
- Colisión fuerte. Será computacionalmente complicado encontrar un par (m_0, m_1) de forma que el hash de m_0 sea idéntico al de m_1.

Observando estas características se puede deducir, que un algoritmo hash no es un algoritmo de encriptación propiamente dicho, aun así, gracias a sus inestimables propiedades se ha hecho un hueco de relevancia en el mundo de la criptografía, y en particular, de la Seguridad Informática. (Torres, propiedades de las funciones hash, 2016)

Criptoanálisis de las funciones Hash

En el año 2004 salieron a la luz las primeras noticias sobre la ruptura de la función hash MD5, y desde ese momento la comunidad criptológica se ha cuestionado la seguridad que ofrecen los algoritmos hash a nuestros esquemas de cifrado.

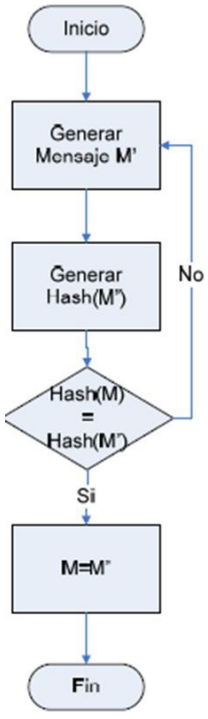
Según Benedicto (2010)

> el criptoanálisis es la ciencia encargada de buscar las vulnerabilidades de los criptosistemas. En el caso de las funciones hash la seguridad o fiabilidad está soportada sobre los pilares de las matemáticas más que sobre los de la informática o la telemática, de tal modo que las debilidades tienen más implicaciones matemáticas que computacionales. (Benedicto, 2010, p. 24)

A continuación, se muestran los tipos de ataque que se pueden realizar sobre una función hash.

Ataque del cumpleaños. Es un ataque por Fuerza Bruta que se basa en las implicaciones matemáticas. Básicamente este tipo de ataque consiste en generar cadenas aleatorias M', realizar Hash (M') y compararlas con Hash (M) original. Si coinciden se habrá encontrado la solución siendo M = M', en caso contrario se continúa generando nuevas cadenas. En el caso de SHA1 (160 bits) este ataque necesitaría generar 2^{160} mensajes para hallar la solución. (Benedicto, 2010, p. 24)

Figura 4. Diagrama ataque del cumpleaños.



Fuente: Rafael, 2010.

Ataque Wang-Yin-Yu o Ataque chino. Es un ataque por Fuerza Bruta simplificado. Ilustraremos este ataque con un ejemplo.

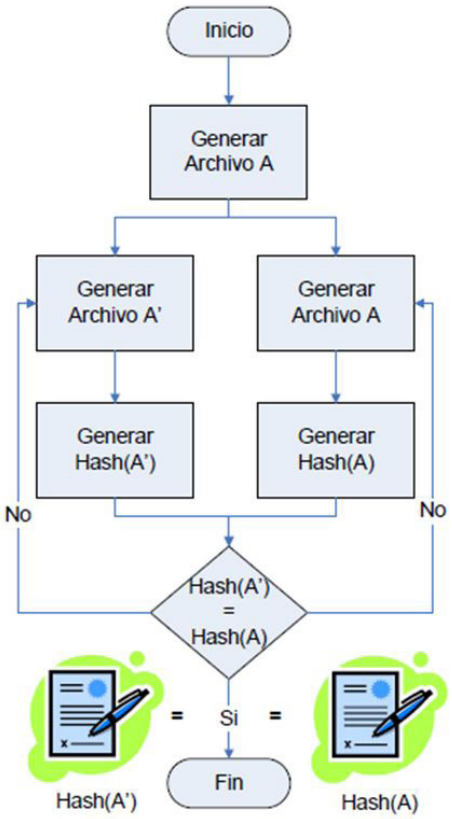
Imagine que quiere realizar la venta de un inmueble, para ello redacta un contrato de venta A, el cual contiene tanto el texto con los datos pertinentes, como imágenes de la vivienda.

Al mismo tiempo genera un contrato alternativo A' con las mismas fotos pero modificando el precio de venta a su favor. Por las propiedades vistas con anterioridad sería prácticamente imposible que Hash (A) = Hash (A').

Ahora bien, puede generar múltiples versiones de A y A' modificando tan sólo unos pocos bits de las imágenes (modifica sólo las imágenes para que no llame tanto la atención la trampa realizada) hasta conseguir que Hash (A) y Hash (A') sean idénticos. Ahora solo tendría que presentar al comprador el documento A, él aceptará las condiciones y lo firmará electrónicamente.

Luego cambia A por su variante A' y ya tiene un contrato legal de compraventa firmado con unas condiciones distintas de lo establecido. Gracias a este tipo de ataque, para romper un algoritmo hash SHA1, se pasa de generar 2160 mensajes, a tan solo 269. (Benedicto, 2010, p. 25)

Figura 5. Diagrama ataque Wang Yin-Yu.



Fuente: Rafael, 2010

Ataque por extensión de longitud. Este ataque se basa en que dado un hash Hash(m), en el que se conoce Hash(m) pero no el mensaje m, se puede generar nuevas huellas "válidas" que incluyan a la anterior aunque difieran de ella. Esto se realiza concatenando Hash (m)+m' para posteriormente realizar el hash a la totalidad dando como resultado Hash (Hash(m)+m'). (Benedicto, 2010, p. 27)

Figura 6. Diagrama ataque por extensión de longitud.

Fuente: Rafael, 2010.

Posibles soluciones

Colisiones en las funciones hash

Para autores como Gilbert y Hanschuh (2004), utilizar SHA-2 parece estar condenado si los ataques siguen avanzando sobre la arquitectura UFN (Unbalanced Feistel Network). La falla existe, pero aún no hay recursos para ponerla en evidencia.

Se sugiere utilizar 2 *hashings* distintos para el mismo mensaje, dado que nadie ha podido lograr colisiones simultáneas. Por ejemplo, si calculamos para un mensaje M los digestos concatenados h1 (M) || h2 (M), donde h1 y h2 indican dos funciones de *hashing* diferentes, encontrar una colisión implicaría que debe ser simultánea para ambas funciones, tarea computacionalmente imposible (Chabaud, 1998).

Para cambiar la arquitectura, hay que buscar el reemplazo de la plataforma UFN por nuevos algoritmos. Tal como el AES reemplazó al DES cambiando un FN (Feistel Network) por transformaciones basadas en las operaciones polinómicas de los cuerpos de Galois GF[2^8]. Con este objetivo, hay que buscar procesos fuertes e inmunes a las colisiones diferenciales.

Soluciones al problema de contraseñas

En primera instancia, hay que producir algoritmos de encriptación de contraseña que generen un número más largo de código, con ello la probabilidad de que se produzca una colisión o que una contraseña sea descifrada se reduce, dado que se des actualizarían las bases de datos para los códigos *hash* actuales y dejarían de ser, al menos por el momento, desconocidas.

Otra opción sería RIPEMD-160 que, como ya se ha dicho, crea un código *hash* de 160 bits RIPEMD (también llamados resúmenes RIPE del mensaje). Estas se representan típicamente como números de hexadecimal 40 dígitos (Wang, 2004).

El mayor problema consiste en la generación de claves de palabras incluidas en cualquier diccionario de lengua, dado que las bases para ataques se basan en sus palabras y combinaciones, para generar los códigos hash para ataques. Las buenas prácticas son unos de los mejores ejercicios; darlos a conocer y forzar este tipo de contraseñas puede llegar a ser una gran estrategia para reducir esta vulnerabilidad (Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, MICITT, 2015). A continuación, mencionaremos algunas de esas prácticas:

- Nunca revele el código de activación. Para ello mantenga en secreto la clave o pin utilizados

para acceder a sus dispositivos criptográficos (token o tarjetas inteligentes, *smart cards*)

- Utilice contraseñas, para la clave o pin, difíciles de deducir en el código de activación: nunca las escriba en algún papel que guarde junto con el dispositivo criptográfico.
- Cambie periódicamente las contraseñas, para la clave o pin de su dispositivo criptográfico.
- No entregue su dispositivo criptográfico a ningún desconocido, evite perderla de vista y retire el dispositivo criptográfico después de utilizarlos en el computador.
- Esté atento a la fecha de expiración. El certificado digital emitido por la Autoridad Certificadora posee una fecha de vencimiento, así que tenga la precaución de renovarla antes de esta fecha para evitar problemas con su uso.
- Reporte problemas o incidentes de seguridad directamente a la autoridad certificadora que le emitió el certificado. Si los problemas persisten, puede reportarlo a la DCFD.
- Reporte inmediatamente la pérdida, hurto o robo del dispositivo criptográfico (token o *smart card*), a través de los medios o servicios que la autoridad certificadora que emitió el certificado ha proporcionado para la revocación del certificado.
- Utilice antivirus actualizado en su computador y utilice software licenciado

Ataques Criptográficos

En criptografía se denomina 'ataque de fuerza bruta' a la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrarla. Dicho de otro modo, define al procedimiento por el cual, a partir del conocimiento del algoritmo de cifrado empleado y de un par texto claro-texto cifrado, se realiza el cifrado y descifrado respectivamente, de uno de los miembros del par, con cada una de las posibles combinaciones de clave hasta obtener el otro miembro del par.

Otro factor determinante en el coste de realizar un ataque de fuerza bruta es el juego de caracteres que se pueden utilizar en la clave. Esto hace referencia a que las contraseñas que solo utilicen dígitos numéricos serán más fáciles de descifrar que aquellas que incluyen otros caracteres como letras. La complejidad compuesta por la cantidad de caracteres en una contraseña es logarítmica (Wiki_seguridadinformatica, 2015).

Por otra parte, un ataque de diccionario es un método de cracking que consiste en intentar averiguar una contraseña probando todas las palabras del diccionario. Este tipo de ataque suele ser más eficiente que un ataque de fuerza bruta, ya que muchos usuarios suelen utilizar una palabra existente en una lengua como contraseña, para que sea fácil de recordar, lo que no es una práctica recomendable.

Los ataques de diccionario tienen pocas probabilidades de éxito con sistemas que emplean contraseñas fuertes con letras en mayúscula y minúscula, mezcladas con números o cualquier tipo de símbolos. Sin embargo, para la mayoría de los usuarios, recordar contraseñas tan complejas resulta complicado. Existen variantes que comprueban también alguna de las típicas sustituciones (determinadas letras con números, intercambio de 2 letras, abreviaciones) así como distintas combinaciones de mayúsculas y minúsculas (Seguridad Roberto, 19 de noviembre del 2016).

Otra solución habitual para no tener que memorizar un número elevado de contraseñas es utilizar un gestor de contraseñas. Estos programas también nos pueden ayudar a generar contraseñas seguras (asegurándonos que no se trate de un spyware).

Una forma sencilla de proteger un sistema contra los ataques de fuerza bruta o los ataques de diccionario es establecer un número máximo de tentativas, de esta forma se bloquea el sistema automáticamente después de un numero de intentos infructuosos predeterminados. Un ejemplo de este tipo de sistema es el mecanismo empleado en las tarjetas sim, que se bloquean automáticamente tras 3 intentos fallidos al introducir el código PIN.

Conclusión

Es muy importante resaltar que al igual que han aumentado las amenazas sobre los sistemas informáticos, debido al acelerado crecimiento de la tecnología, también han surgido y evolucionado nuevas estrategias y medidas de seguridad para la protección de los usuarios. En la red estamos expuestos a ser atacados en cualquier momento y uno de los puntos más vulnerables es la comunicación. Es por tal motivo que nace la necesidad de conocer e implementar mecanismos de seguridad para protegernos y a nuestra información de cualquier atacante o ataque.

Uno de los elementos de la seguridad informática que cobra gran importancia a la hora de transmitir información es la infraestructura de clave pública, ya que permite verificar la autenticidad del emisor y además cumplir con el principio de no repudio y de integridad referentes a la seguridad informática.

La importancia de conocer los temas bases y fundamentales en seguridad informática es indispensable, además de mantenerse actualizado de cada uno de los nuevos conceptos y conocimientos que surgen con el acelerado avance tecnológico, con el objetivo de estar preparado a dar soluciones efectivas ante la prevención o materialización de un ataque a un sistema inteligente.

Podemos comentar que el algoritmo MD5 ha dejado de considerarse seguro y dentro de poco quizá sea sustituido por otro más eficiente. Pero mientras eso pasa, nosotros como usuarios tenemos la responsabilidad de usar alternativas que ofrezcan mayor seguridad, y elegir contraseñas mejores, para proteger nuestros datos y los de nuestros sistemas. Una cadena siempre se rompe por el eslabón más débil.

La implementación del comando OpenSSL se puede tomar como una herramienta muy importante en el uso de:

- Creación de Certificados Digitales.
- Instalación de Certificados Digitales.
- Manejo de Certificados Digitales:
    - o Generar y Firmar Certificados
    - o Revocar Certificados
    - o Renovar un Certificado
    - o Visualizar un Certificado

Con la aplicación del concepto de criptografía a los sistemas inteligentes, se alcanza a mejorar la protección de la información, lo que produce confianza en las partes interesadas. De igual

forma, se logra minimizar los ataques a los sistemas inteligentes, fortaleciendo la seguridad informática en las comunicaciones electrónicas.

Es importante reconocer que el trabajo fundamental se debe desarrollar en el recurso humano, quien se debe concientizar y hacer parte de la cultura de la seguridad, aplicando siempre buenas prácticas.

Referencias

Benedicto, R. (2010). *Aplicación de metodologías de paralelización para la generación de Tablas Rainbow mediante la utilización de servidores de altas prestaciones en GNU/Linux*. (Titulación de ingeniero en Informática), Universidad de Almería. Recuperado de http://www.adminso.es/recursos/Proyectos/PFC/PFC_rafa.pdf

Chabaud F., Joux A. (1998) Differential collisions in SHA-0. In: Krawczyk H. (eds) Advances in Cryptology — CRYPTO '98. CRYPTO 1998. *Lecture Notes in Computer Science*, *1462*. 56-71. DOI: 10.1007/BFb0055720

Claudio Fernando. (2014) Criptología y Seguridad. Seguridad en Redes. Recuperado de http://slideplayer.es/slide/1652019/

Eadic (2015). Sistemas Inteligentes de Transporte. Recuperado de https://www.eadic.com/sistemas-inteligentes-de-transporte/

Gilbert H., Hanschuh H. (2004). Security Analysis of SHA-256 and Sisters. En: Matsui M., Zuccherato R.J. (eds) *Selected Areas in Cryptography. SAC 2003. Lecture Notes in Computer Science* (vol. 3006). Berlin, Heidelberg: Springer.

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) (2015). Buenas prácticas. Recuperado de http://www.firmadigital.go.cr/practicas.html

Seguridad Roberto. (19 de noviembre del 2016). Ataques de diccionario, ataques de fuerza bruta, programas, diccionarios [entrada de blog]. Recuperado de https://seguridadroberto.wordpress.com/2016/11/19/ataques-de-diccionario-ataques-de-fuerza-bruta-programas-diccionarios/

Torres, B. (2016). Métodos de cifrado. Disponible en: https://es.slideshare.net/BetsabethTorres_93/metodos-de-cifrado-69916762

Wang X., Feng D., Lai X., Yu H. (2004). Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD, (preprint - 17 Aug 2004) disponible on-line en: http://eprint.iacr.org/2004/199.pdf

Wiki_seguridadinformatica. (2015). Criptografía, Principios. Disponible en: https://sites.google.com/site/wikiseguridadinformatica/7-cro/7-1-principios