Criptografía, Firma Digital y Seguridad de la Información v. 1.5

Juan Rodrigo Anabalón R.

http://deoxy.spaces.live.com

jranabalon@yahoo.es

Resumen:

El presente artículo busca introducir al lector en el concepto de criptografía firma digital y seguridad de la información.

El concepto de criptografía es esencial para comprender el funcionamiento de la firma electrónica ya que todos los documentos que son firmados para los distintos trámites que se realicen, deben ser confiables, para así, asegurar el buen funcionamiento del sistema, y proteger la confidencialidad de los datos entregados, evitar la suplantación de usuarios. No obstante muchas personas pensarán que con el solo hecho de encriptar sus mensajes están protegidos, pero la seguridad debe ser una actitud de vida y no depende solo de la criptografía.

Palabras Clave:

Criptografía, seguridad de la información, Firma digital.

Copyleft

Versiones

v.1.0	03/2005	Primera versión web publicada en IT Pro Chile
v.1.5	10/2006	Primera revisión con cambios y correcciones

Formatos y Fuentes

PDF http://es.geocities.com/jranabalon/criptopaper.pdf

Cita

Juan Rodrigo Anabalón R. (2006) Criptografía, Firma Digital y Seguridad de la Información. v1.5 url: http://es.geocities.com/jranabalon/criptopaper.pdf.

1. CONCEPTOS RELACIONADOS CON LA CRIPTOGRAFIA.

El término criptografía viene del griego *kryptos* (ocultar) y *grafos* (escribir), literalmente escritura oculta, la **criptografía** es un arte y a la vez una ciencia para cifrar y descifrar datos utilizando las matemáticas. Esto se hace para intercambiar datos de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

La criptografía tiene como finalidad garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones etc.), y asegurar que la información que se envía es auténtica en un doble sentido, "que el remitente sea realmente quien dice ser" e impedir que el contenido del mensaje enviado (criptograma) sea modificado en el trayecto.

Otro método para ocultar el contenido de un mensaje **es ocultar que ha habido un mensaje**. Con esteganografía se puede ocultar un mensaje en un archivo de sonido, una imagen o incluso en reparto de los espacios usados para justificar un texto plano.

Normalmente aparte de ocultarlo el mensaje además se cifra.

Cabe hacer notar, que la palabra criptografía solo se refiere al uso de códigos, lo que no engloba las técnicas que se usan para romper esos códigos, esto último se conoce como *criptoanálisis*. El término *Criptología* se emplea para agrupar la *Criptografía* y el *Criptoanálisis*.

Entre las disciplinas que engloba la criptografía se pueden destacar la *Teoría de información*, la *Teoría de Números o Matemática Discreta*, que estudia las propiedades de los números enteros, y la *Complejidad Algorítmica*. Así que si pensaste que lo que te enseñaban en los ramos matemáticos no tenían ni una utilidad en informática, te puedo decir que estás rotundamente equivocado, pues si te has planteado la idea de ser un verdadero hacker o un cracker, debes empezar a desenpolvar tus cuadernos de Algebra que abandonaste una vez que habías aprobado los ramos en la Universidad.

Teniendo las cosas así, definiremos un Criptosistema como una quíntupla (M, C, K, E, D), donde:

- M representa el conjunto de todos los mensajes sin cifrar (texto claro) que pueden ser enviados.
- C representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.
- K representa el conjunto de claves que se pueden emplear en el criptosistema.
- E es el conjunto de *transformaciones* de cifrado o familia de funciones que se aplica a cada elemento de M para obtener un elemento C. Existe una transformación diferente E_k para cada valor posible de la clave *k.*
- D es el conjunto de transformaciones de descifrado, análogo a E.

Todo criptosistema ha de cumplir la siguiente condición:

$$D_k(E_k(m)) = m$$

Es decir, que si tenemos un mensaje m lo ciframos empleando la clave k y luego lo desciframos empleando la misma clave, obtenemos de nuevo el mensaje original m.

Existen principalmente dos tipos de criptosistemas:

- *Criptosistemas simétricos o de clave privada*: Estos son aquellos que emplean la misma clave k tanto para cifrar como para descifrar. Presentan el inconveniente de que para ser empleados en comunicaciones la clave k debe estar tanto en el emisor como en el receptor, lo cual nos lleva a preguntarnos cómo transmitir la clave en forma segura.
- *Criptosistemas asimétricos o de llave pública*: Estos emplean una doble clave (k_p, k_p). k_p se conoce como clave privada y k_p como clave pública. Una de ellas sirva para la transformación de E de cifrado y la otra para la transformación D de descifrado. En muchos casos son intercambiables, esto es, si empleamos una para cifrar la otra sirve para

descifrar y viceversa. Además se debe cuidar que la clave pública k_p no permita calcular la clave privada k_p.

Esto es debido a Shannon que propone una medida para la cantidad de información que aporta sobre una variable el conocimiento de otra. Así la cantidad de información de Shannon se define como la cantidad de información de una variable X sobre una variable Y como:

$$I(X,Y) = H(Y) - H(Y/X)$$

Esto quiere decir que la cantidad de información que nos aporta el echo de conocer X al medir la incertidumbre sobre Y es igual a la disminución de entropía que este conocimiento conlleva. Sus propiedades son las siguientes:

1) I(X,Y) = I(Y.X)

2) I(X,Y) >= 0

Entonces un criptosistema es seguro si la cantidad de información que nos aporta el echo de conocer el mensaje cifrado c sobre la entropía del texto claro m se hace cero, o sea:

$$I(C,M) = 0$$

Esto significa que la distribución de probabilidad que nos inducen todos los mensajes en claro, el conjunto M, no cambia si conocemos el mensaje cifrado.

2. Principios básicos de criptoanálisis.

Todo hacker o especialista en seguridad informática debe estar familiarizado con las técnicas de criptoanálisis.

2.1Criptografía de llave privada

2.1.1 Criptografía clásica

2.1.1.1 Cifrado Monoalfabético:

Aunque parezca básico para algunos lectores, es importante familiarizarse con los métodos clásicos de cifrado como el de *César* en el que se efectúa una *sustitución* carácter a carácter del texto, por ejemplo la A se sustituye por la D, y la B por la E, la C pasaría a ser la F y así con todo el abecedario.

Ej.

Texto claro: ESTAMOS CIFRANDO UNA CADENA

Texto cifrado: HVWDPR FLUDQGR XQD FDHGHQD

De forma general se puede decir que C=(M+3) mod 26 (considerando un alfabeto de 26 letras).

Este método se utilizaba en el siglo I a.C. y fácil de romper efectuando una relación entre letras que se repiten más habitualmente.

Para conseguir el texto original tendríamos que retroceder en el abecedario tres posiciones por cada letra para obtener el texto original.

Una solución posible, pero no definitiva, consiste en conseguir que distintas letras pueda ser cifrada con distintos pares. Por ejemplo sumar una posición a los lugares impares y dos en los impares, así la letra A se sustituye por B, la B por D, la C por D y así sucesivamente:

Ejemplo:

Texto claro: ESTAMOS CIFRANDO UNA CADENA

Texto cifrado: FUUCNQT DKGTBPEQ VPB DCEGOC

2.1.1.2 Cifrados de Transposición:

La *transposición* es otro método clásico., consiste en aplicar cambios de posición entre los elementos de texto, por ejemplo, el primer carácter por el segundo, el tercero por el cuarto, etc.

Texto claro: ESTAMOS CIFRANDO UNA CADENA

Texto cifrado: SEATOMC SFIARDNUO AN ACEDAN

Finalmente, para fortalecer el cifrado, se utiliza una combinación de ambos métodos, esto es, primero se hace una sustitución, y luego una transposición:

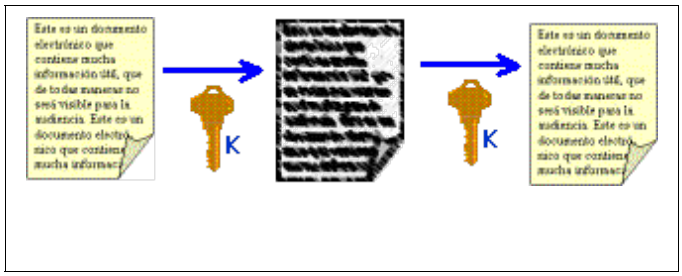
Ejemplo:

Texto claro: ESTAMOS CIFRANDO UNA CADENA

Sustitución: HVWDPR FLUDQGR XQD FDHGHQD

Transposición: VHDWRP LFDUGQX RDQ DFGHQHD

Para obtener el texto claro bastará con realizar la inversa, en primer lugar la transposición y posteriormente la sustitución.



Por tanto, si se sabe el método de cifrado, es cuestión de tiempo descubrir el texto original, sólo se necesita realizar un ataque apropiado, invirtiendo el algoritmo con el texto cifrado, someter el algoritmo a un ataque por fuerza bruta o diccionario.

La criptografía moderna está lejos de ser tan sencilla como la ya descrita, los criptosistemas actuales están concebidos principalmente en fundamentos matemáticos muy complejos, que hacen el proceso de romper una clave, una tarea mas difícil, pero no por eso, imposible.

2.1.2.1 Criptografía Asimétrica

Estos Algoritmos son de especial interés en redes de comunicación inseguras (Internet). Fueron propuestos por Whitfiel Diffie y Martín Hellman a mediados de los setenta. La principal novedad respecto a los métodos de criptografía simétrica es que las claves no son únicas, sino que forman pares.

Los Algoritmos asimétricos emplean generalmente longitudes de clave mucho mayores que simétricos. Por ejemplo, para algoritmos simétricos se considera segura una clave de 128 bits, para algoritmos asimétricos, excepto los de curvas elípticas, se recomiendan claves de 1024 bits, además los algoritmos asimétricos son más lentos que los simétricos debido ala complejidad de cálculo que estos demandan.

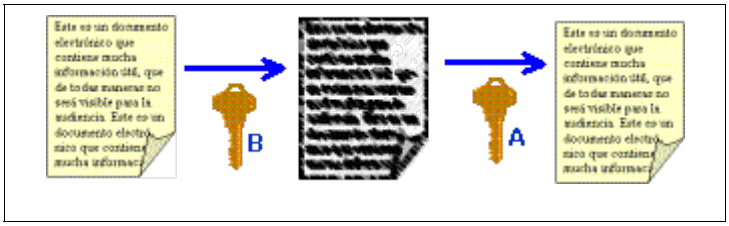
Los algoritmos asimétricos poseen dos claves diferentes en vez de una, k_p y k_p denominadas *clave privada* y *clave pública*. Una de ellas se usa para codificar y la otra para decodificar. Dependiendo del uso que le demos la clave privada será para cifrar o viceversa.

Otra aplicación de los algoritmos asimétricos es la autentificación de mensajes, lo que nos permite obtener una firma digital a partir de un mensaje.

En este tipo de cifrados no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Antes de iniciar una comunicación secreta, el remitente debe conseguir una copia de la clave pública del destinatario, y esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario.

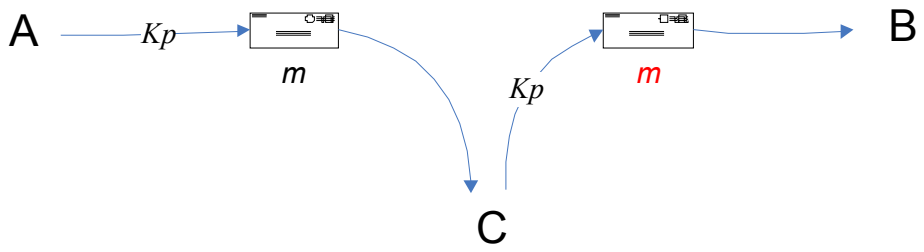
La idea del cifrado de clave pública es utilizar, por ejemplo, los números primos. Osea esto es una función en un solo sentido cuya computación es fácil, mientras que su inversión, resulta extremadamente difícil. Por ejemplo, es fácil multiplicar dos números primos y obtener uno compuesto, pero es difícil factorizar uno compuesto en sus componentes primos.

Los algoritmos de clave pública realizan una función parecida, si se considera una pieza de información, sería difícil computar el inverso.



En el diagrama anterior, vemos cómo un documento, es encriptada con una llave A, y desencriptada con una llave B. El proceso también funciona a la inversa: si se encripta el documento con la llave B, es posible desencriptarla con la llave A.

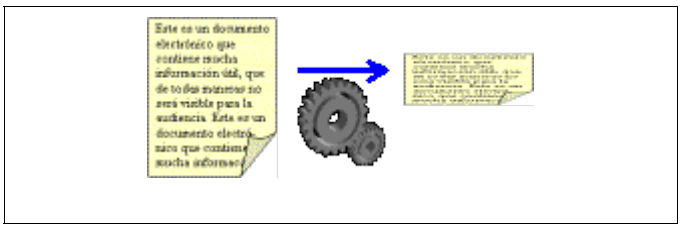
Pero todo esto igual puede presentar problemas. Por ejemplo C puede interceptar el mensaje *m* y se remplaza por otro mensaje *m*, esto causaría un mensaje corrupto con información dudosa, por ejemplo si tenemos la k_p de B se puede encriptar la información con esa misma clave y hacerle creer al receptor B que el mensaje fue realmente enviado por el remitente A.



A partir de esto ¿Cómo puede B estar seguro de que fue A quien envió la información?, ¿Cómo puede B estar seguro de que no hubo un agente C que halla modificado la información? ¿Cómo puede B asegurarse de que A no niegue que envió la información?.

3. FIRMA ELECTRÓNICA

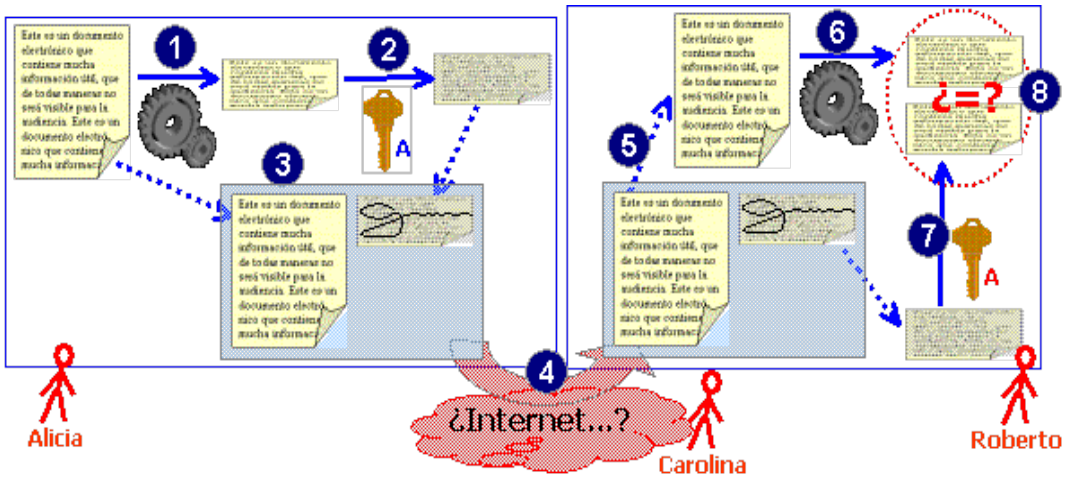
Para solucionar el problema anterior se puede generar un tipo de algoritmo criptográfico llamado Hashing, que es una secuencia de pasos que permite generar, a partir de un documento, un trozo de información (más pequeño). Si se cuenta solo con este pedazo de información no es posible generar el documento original.



Supongamos que M es un mensaje, h el hashing del mensaje (documento mas pequeño) y H la función que, a partir de M, da como resultado h. Podemos describirlo como h=H(M).

En la firma electrónica se combinan estos métodos de cifrado para generar una confiabilidad aceptable al proceso de entrega de información.

La siguiente figura muestra a: A (Alicia) envía un documento a B (Roberto).



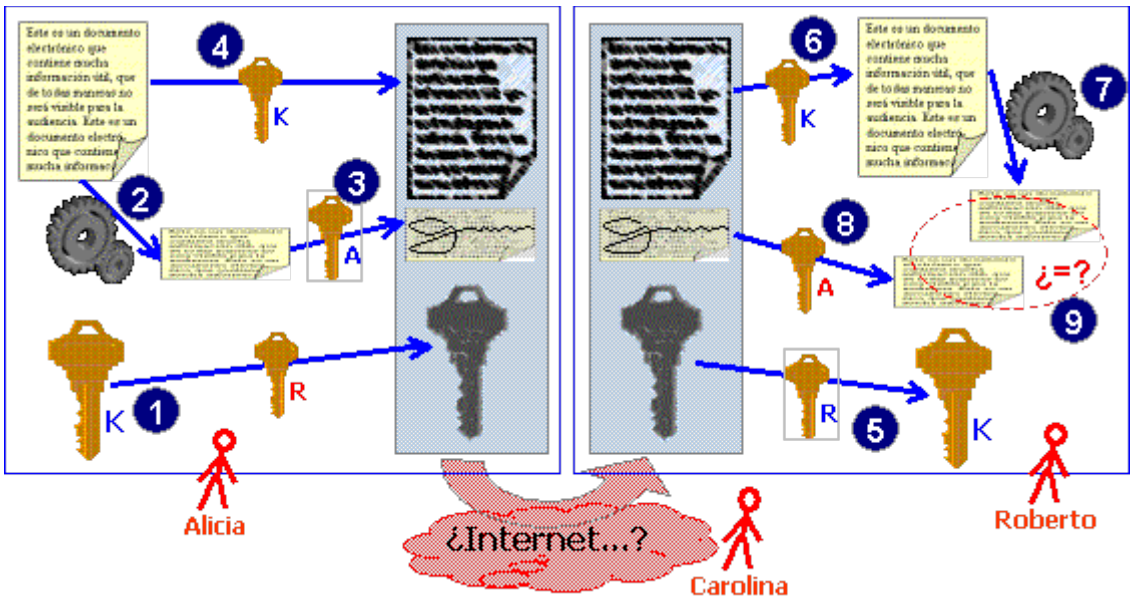
1	A toma el documento y, a través de un algoritmo de hashing, obtiene un message digest del documento.
2	A toma el message digest y lo encripta con su llave privada. El resultado es llamado fingerprint ("huella digital" del documento).
3	A toma el documento original y su fingerprint, y los mete dentro de una estructura que pueda contener archivos, como un archivo XML o un email multiparte.
4	A envía el documento a B, donde posiblemente puede interceptarlo C.
5	B recibe el archivo, y extrae el documento y el fingerprint.
6	B toma el documento y calcula a partir de él un message digest, con el mismo algoritmo que utilizó A.
7	B desencripta el fingerprint contenido en el archivo, con la llave pública de A (obteniendo, si todo está bien, el message digest del documento original).
8	Finalmente, B compara los message digest obtenidos independientemente en los dos pasos anteriores.

Si en el último paso, B compara los *message digest* y estos coinciden exactamente y son iguales, podemos tener la seguridad de que el documento proviene indudablemente de A. porque si B pudo desencriptar el fingerprint con la llave pública de A, esto nos asegura que el fingerprint fue encriptado con la llave privada de A. A no puede negar que envió el documento, por la misma razón anterior. C no modificó la información en el trayecto. Esto no es posible porque, si hubiese modificado el documento o el fingerprint, los message digest no hubiesen sido iguales.

Sin embargo volvemos atener problemas de confidencialidad de los datos, porque C puede observar la información contenida en el archivo.

3.1 Firma electrónica más encriptación

En el siguiente diagrama, también tomado de Cristian Bravo Lillo se muestra un esquema que combina la firma digital y la encriptación para solucionar el problema de confidencialidad.



1	A escoge una llave de sesión, que será una llave secreta que se usará sólo una vez, y que no necesita comunicar a B. Luego toma esta llave de sesión, la encripta con la llave pública de Roberto, y la introduce en un archivo contenedor (contenedor XML etc.).
2	A toma el archivo, le aplica un algoritmo y obtiene un Message Digest de la información.
3	Luego toma el Message Digest obtenido y lo encripta con su propia llave privada, obteniendo una firma electrónica del archivo. Luego introduce esta firma en el contenedor.
4	Finalmente, A toma la receta, la encripta con la llave de sesión, y la introduce en el contenedor; acto seguido, envía el archivo completo a B, donde pudiera estar observándolo C.
5	B recibe el archivo, extrae la llave de sesión encriptada y la desencripta con su propia llave privada.
6	Luego, B extrae la receta encriptada, y la desencripta con la llave de sesión que acaba de obtener en la paso anterior.
7	B toma la información que acaba de obtener, y calcula un Message Digest del documento, con el mismo algoritmo que utilizó A. Este será usado posteriormente para verificación.
8	B extrae la firma electrónica generada por A, y la desencripta con la llave pública de A. Obtiene entonces otro Message Digest, que usará para compararlo con el obtenido en el paso anterior.

9	Finalmente, B compara los message digest obtenidos en forma independiente en los dos pasos anteriores.

4. Precauciones

Las precauciones se deben tomar en todo orden respecto de la seguridad de los sistemas computacionales y la información, si bien el sistema criptográfico es "seguro", las deficiencias no están prácticamente relacionadas con la encriptación de la información, el problema radica más bien en el traspaso o intercambio de claves, pues el agente C puede intervenir y obtener estas claves de forma *"ilícita"*. Ya que A puede solicitar la clave publica a B por teléfono (por ejemplo) y nuestro agente C puede intervenirlo para escuchar la conversación que ambos mantienen, o bien suplantar identidades como hacerle creer a B que realmente está hablando con A y así engañarlo y lograr que le entreguen la clave.

Pero aunque todo esto se controle, la teoría de sistemas nos dice que todo sistema es parte de otro sistema así que aunque ya hallan intercambiado las claves y un hacker intenta un ataque a la confidencialidad de ellos, lo puede hacer con un simple *keylog*, así en vez de tratar de intervenir el mensaje desde dentro perfectamente se puede conseguir desde afuera. Es importante entonces mantener limpio el PC de todo tipo de amenazas y estar siempre atento y controlando nuestro sistema. La mayor seguridad que podamos dar a nuestros sistemas puede verse gravemente afectados simplemente por un descuido de nuestras llaves, no importa que tan protegidos estemos, un solo error puede comprometernos gravemente.

5. Referencias

- "Firma Digital y Certificados Digitales", Angel, José. HTML Web [visitado 25 Agosto 2003], http://www.htmlweb.net/seguridad/varios/firma_certificados.html

- Manual de Firma Electrónica, Ministerio Secretaría General de la Presidencia. Proyecto Reforma y Modernización del Estado
  Junio de 2004.
  Cristian Bravo Lillo.

- Criptografía y Seguridad en Computadores Tercera Edición (versión 1.14)
  Marzo de 2002.
  Manuel José Lucena López.