

CAPÍTULO II

ELEMENTOS Y SEGURIDAD DE LA FIRMA ELECTRÓNICA

Hemos visto en el Capítulo I, que la firma electrónica está siendo utilizada en varios países del mundo, ya que la práctica ha demostrado que es un medio por el cual se puede autenticar mensajes de manera segura y económica, con la cual se cerciora la confidencialidad entre emisor y receptor, certificando la integridad del mensaje, dando como resultado un flujo comercial con mayor celeridad y confiabilidad, en razón de que la firma ológrafa queda en un segundo plano dentro de esta nueva Revolución Digital.

Ahora que ya tenemos claro el ámbito general de la firma electrónica, daremos paso a los elementos particulares de ésta, estableciendo las diferencias que existen entre los términos “firma electrónica” y “firma digital” ya que como veremos, estos no son similares, pasaremos por la criptografía y su importancia, para finalmente analizar el funcionamiento de la firma como tal.

1. FIRMA ELECTRÓNICA Y FIRMA DIGITAL

La *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos* (Ley 67) la cual rige al Ecuador desde el año 2002, establece que la firma electrónica “son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.”¹¹¹². Como se desprende de la simple lectura del concepto precitado, el campo de aplicación es sobradamente amplio, ya que se ha definido a la firma electrónica como el conjunto de datos verificativos, directamente vinculados con un mensaje electrónico, los cuales permiten de forma veraz e innegable, la relación entre

¹¹ *Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de datos*; R.O. #557 del 17 de abril de 2002.

un mensaje y su emisor, convirtiendo a este último como único responsable de la información enviada.

De esta manera queda claro el reconocimiento y validez jurídica que tiene la utilización de la firma electrónica, sin importar el método o técnica que se utilice como medio de seguridad, por cuanto la variedad y complejidad de métodos criptográficos es bastante extensa. Esto vendría a constituirse en un acierto por parte de nuestros legisladores, ya que a mi consideración ellos deben haber tomado muy en cuenta el hecho de que nos encontramos en avances experimentales y no nos podemos regir a un método restringido de comprobación de autoría, sin saber cual será el medio apropiado que se acople a nuestra sociedad y mas aún sabiendo que la tecnología es una ciencia que avanza a pasos agigantados donde las técnicas quedan obsoletas en poco tiempo.

En la mayoría de los textos, por no decir todos, que tratan el tema de la firma digital, determinan a la firma electrónica como un género y la firma digital como la especie, esto en razón de que la firma electrónica está caracterizada por ser todo modo de identificación de autoría basada en medios electrónicos, en donde el autor tiene el propósito de ligarse con el documento. Sarra también lo establece así diciendo que es el “... identificador que va adosado (*atachado*) o lógicamente asociado a un mensaje electrónico, documento o datos, y los propósitos para los cuales fue incluido implican el concepto jurídico de firma”¹², el problema radica en que la autoría queda únicamente supeditada al simple hecho de que el emisor tiene el “propósito” de relacionarse con el mensaje que ha enviado, no existe ninguna certeza técnica que nos asegure que el instrumento no ha sido modificado al momento de su envío, y de la misma manera no existe un nexo legal que determine que el emisor es en verdad quien dice ser. Estas atribuciones fundamentales son de la firma digital, como ya lo explicaré en párrafos posteriores.

Para mayor claridad de lo que es la firma electrónica, Apolonia Martínez¹³ explica que,

“Una firma electrónica sería simplemente cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita. este concepto amplio y tecnológicamente indefinido de firma (...) tendría cabida técnicas tan simples como un nombre u otro elemento identificativo incluido al final de un mensaje electrónico, y de tan escasa seguridad que plantean la cuestión de valor probatorio a efectos de autenticación, aparte de su nula aportación respecto a la integridad del mensaje...”

¹² SARRA, Andrea Viviana; *Comercio Electrónico y Derecho*; Ed. Astrea; Buenos Aires 2001; p. 389

¹³ MARTÍNEZ Nadal, Apolonia; *Comercio electrónico, firma digital y autoridades de certificación*; 2ª Ed. Colección Estudios de Derecho Mercantil; Civitas; Madrid 2000; p. 40

se entiende tan simple y poco segura a la firma electrónica que perfectamente puede concebirse como una firma manuscrita digitalizada utilizada al final de un mensaje, con la cual se liga al emisor con el texto.

Por su parte la firma digital o firma electrónica avanzada, como se la conoce en algunas legislaciones internacionales, es un método mucho más técnico, cuyo sistema radica en la utilización de criptografía, esto en razón de que el fin último de la firma digital es la protección e inviolabilidad de la información que se envía debiendo necesariamente recurrir a la encriptación la cual se define, según la Real Academia de la Lengua, como el arte de proteger la información, deviniendo el término criptografía, del griego *kriptos* que significa oculto y *graphe* que representa a la escritura, resolviendo en que es el arte de escribir con clave secreta o de un modo enigmático.

En otras palabras, la criptografía es la transformación de mensajes en textos aparentemente ilegibles en donde únicamente el emisor y receptor consiguen resolverlos a su forma original, alcanzando así que cualquier persona que no posea la clave le sea imposible descifrarlo, por lo general su creación es a través de algoritmos¹⁴. Para tener más clara esta idea, la firma digital se la entiende como el registro electrónico a través de *criptografía asimétrica de clave pública* donde el receptor del mensaje tiene la posibilidad de verificar si la información que recibió ha sido alterada en algún punto contado desde el envío hasta su recepción.

La diferencia entre estos dos métodos de autenticación electrónica de autoría radica en que al momento de utilizar la firma digital se aplican presunciones *juris tantum* sobre la identidad del emisor o firmante y la integridad del documento que él suscribió, es decir, son presunciones legales que se las mantienen hasta que se presenten otras situaciones que demuestren lo contrario o se las vuelvan controvertidas. Para dejar claras estas presunciones, un ejemplo de esto es la presunción de legitimidad de los actos administrativos, que pueden ser desvirtuados por el interesado demostrando que los mismos violan el orden jurídico.

Para esclarecer totalmente la diferencia entre estos dos elementos de identificación me permito citar al doctor Alfredo Reyes Krafft, el cual a mi parecer mejor define estas herramientas decretando a la firma electrónica como los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que

¹⁴ Un algoritmo según la Real Academia es el “conjunto ordenado y finito de operaciones que permite hallar la solución de un problema.” Es decir, es el proceso, por lo general de ámbito matemático, que se utiliza para despejar una incógnita o resolver cualquier tipo de problema.

puedan ser utilizados para identificar y/o vincular al firmante en relación con el mensaje de datos, en forma equivalente a la firma manuscrita, y la firma electrónica avanzada como a la firma electrónica que permite la identificación del firmante y ha sido generada bajo su exclusivo control, conocida también como firma digital, que vincula exclusivamente al mismo con el mensaje de datos al que se adjunta o se asocia, lo que permite que sea detectable cualquier modificación ulterior de éste¹⁵, nótese, como ya he repetido numerosas veces, en su primera definición se dice la posibilidad de vincular al signatario con el mensaje, esto podría ser cualquier símbolo, palabra o nombre que éste utilice con la única finalidad de identificador, dejando a un lado cualquier tipo de seguridad para el mensaje, resultando en un peligro de falsificación sencilla; y en su segunda definición se asevera el vínculo excluyente entre el firmante con el mensaje y brinda la tranquilidad del destinatario por cuanto cualquier modificación posterior al envío sería detectada.

Es normal la existencia de teorías contrapuestas en temas de relevancia, y ésta no es la excepción, existen juristas que sostienen que el calificativo de género-especie entre éstas dos es totalmente erróneo, planteando el hecho de que lo “electrónico” es más restrictivo que lo “digital” ya que el primero se vincula a una tecnología específica y lo “digital” es el nombre con el cual se ha acordado para este tipo de información; además de esto, jurisconsultos argentinos como Mauricio Devoto, a quien tengo gran respeto y agradecimiento por su obra *Comercio electrónico y firma digital* cuya lectura ha sido de gran ayuda pero lo cual no significa que no tengamos pensamientos opuestos en ciertos temas, manifiesta su desacuerdo, mencionando que la firma escaneada que puede ser depositada al final de cualquier documento, carece de los requisitos mínimos de seguridad para otorgarle valor jurídico lo cual se contrasta en la firma digital.

Personalmente respaldo la conexión que existe entre firma electrónica y firma digital de género-especie ya que ambas son vías de identificación de autoría de mensajes de datos, las dos coexisten en un mundo tecnológico el cual se lo realiza a través de computadoras y tanto la una como la otra son utilizadas por millones de personas las cuales persiguen un mismo objetivo; obviamente la distinción radica en la seguridad que brindan, pero por esto no dejan de ser género-especie, el género es la determinación de autoría del firmante y la especie es la determinación de autoría del firmante indudable, un ejemplo claro de esta relación es la de caballo como género y el caballo árabe de nombre Relámpago con doce

¹⁵ REYES KRAFFT, Alfredo; *La firma electrónica y las entidades de certificación*; Ed. Porrúa; México 2003; p. 164

años de edad cuyo propietario es Pedro Pérez como especie, la esencia viene a ser la misma.

1.1 Funciones de la Firma Digital

La firma digital debe garantizar a sus usuarios cuatro puntos básicos:

- *Autenticidad* del emisor del mensaje: es la primera y fundamental función de la firma digital, ya que con ésta se le imputa la autoría innegable a quien suscribe el documento, además de conferirle todos los efectos jurídicos que ésta acarrea, esto por cuanto la relación inseparable que se genera entre firma y documento volviendo a estos en uno solo para garantizar tanto al firmante como a quien recibe, la no alteración que podría existir al momento de su envío.
- *Confidencialidad* del mensaje de datos entre emisor y receptor: función imperiosa dentro del mecanismo en razón de la inmensa cantidad de riesgos que existen en la Red; cuando nosotros enviamos un correo electrónico, a pesar de que la recepción del mismo se da en cuestión de centésimas de segundo, la seguridad de nuestro mensaje es totalmente vulnerable ya que el documento viaja en su formato original, es por esto que dentro de la firma digital cada usuario posee dos claves, una privada y una pública, la primera la utilizamos para encriptar el mensaje que hemos escrito, para así enviarlo al destinatario especificando la clave pública de este (identificable públicamente) determinando que éste será la única persona que pueda abrir el mensaje con la clave pública del emisor y la clave privada del receptor la cual a su vez desencriptará el mensaje emitiendo de manera inmediata una notificación en la cual conste que no ha sido alterado el mensaje original, dando como resultado la confidencialidad deseada entre ambos; más adelante hablaremos con mayor detenimiento sobre este proceso.
- *Integridad* del mensaje firmado: el documento firmado digitalmente debe ser íntegro, por lo tanto se garantiza que el contenido que el receptor recibe, es exactamente el mismo que aquel que el emisor envió firmado, de esta manera se asegura que cualquier modificación por terceros que pueda darse será evitada y el mensaje original sin alteraciones será recibido.
- *No repudio* por parte del firmante: la persona quien envía un mensaje de datos con firma digital no puede aducir que no lo ha enviado ya que técnicamente se puede demostrar la identidad única e inequívoca del emisor, esto por cuanto existe un vínculo

jurídico entre el usuario y un tercero de confianza o *Entidad de Certificación* la cual ha sido constituida legalmente y se encuentra bajo la regulación del Consejo Nacional de Telecomunicaciones (CONATEL), lo cual hace del signatario el único y total responsable del uso que éste de a la firma digital; menciono esto nada más como un adelanto de lo que trataremos en capítulos posteriores. Este punto es de vital importancia para el aumento de las relaciones jurídicas y comerciales entre personas por medio del Internet, ya que se permite una disminución inmensa en los costos transaccionales y la celeridad necesaria que se busca. Además de esto, con la incursión de responsabilidades legales para los usuarios se otorga valor probatorio de autoría a la firma digital. De igual manera, no existe la posibilidad de repudio por parte del receptor del mensaje.

Ahora bien, habiendo explicado las bondades de la firma digital, a continuación se ilustra un cuadro comparativo entre la firma manuscrita y la digital, para demostrar que a pesar de ser la firma autógrafa el medio de uso común y obligatorio por varios siglos, ésta tiene falencias claras que las cubre la firma digital, como es el caso de la confidencialidad y el no repudio, el primero lógicamente porque nuestra firma personal queda a vista y paciencia de todo documento que suscribimos, dejando de manifiesto nuestros actos y apartando del camino la confidencialidad que pudimos haber deseado. En segunda instancia el no repudio es un hecho claro que no sucede con la firma manuscrita, cualquier texto firmado puede su supuesto autor aducir que él no ha sido quien firmó el documento, deslindándose de cierta manera de cualquier responsabilidad, a pesar de que existan exámenes grafológicos los cuales también pueden ser inexactos, cosa que no sucede con la firma digital como ya lo expliqué anteriormente.

	Firma Manuscrita	Firma Digital
Elementos personales		
La firma como signo personal	SI	SI
Voluntad de asumir el contenido del doc.	SI	SI
Elementos Funcionales		
Integridad	SI	SI
Autenticidad	SI	SI
Confidencialidad	NO	SI
No repudio	NO	SI

1.2 Efectos de la Firma Digital

Dentro de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas aprobada en la 85ª Sesión Plenaria de 2001, reza en su artículo sexto que “Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica...”¹⁶, dejando de esta manera claro el tratamiento igualitario que deberá darse a las firmas electrónicas en comparación con la firma manuscrita, dejando de lado cualquier restricción que pueda darse respecto de sus efectos jurídicos como firma.

Inspirado en este artículo, un año más tarde, dentro de nuestra ley de Comercio Electrónico se decide incorporar una norma similar en el artículo 14 la cual menciona que “La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba enjuicio.”, reiterando de esta forma el valor legal que debe darse a las firmas electrónicas y resaltando además el factor de valor probatorio que tienen éstas dentro de un proceso judicial, pero más que nada, la similitud entre firma manuscrita y digital ante los ojos de la ley.

Explicado esto, cabe establecer los efectos que tiene la firma electrónica, las cuales tienen relación directa con sus funciones:

- *Presunción de autenticidad*: aquella firma electrónica que haya cumplido con el requisito de estar bajo el control de una Entidad de Certificación se decretará como verídica, determinando el vínculo jurídico que existe entre firma y autor resultando en la voluntad manifiesta de obligarse.
- *Presunción de integridad*: el proceso de firma digital se realiza con posterioridad al documento que vamos a enviar, esto en razón de que una vez firmado digitalmente el escrito será imposible su alteración ulterior ya que los dos, tanto firma como documento, se convierten en uno solo, valiéndose del *certificado* que emite la Entidad correspondiente para verificar la integridad del mismo, en donde constará cualquier modificación en caso de haberla.

Lorenzetti menciona que “si se manda un correo electrónico firmado digitalmente, éste no puede abrirse y cambiarse su contenido sin afectar su vinculación con la firma certificada” añadiendo “si algo se altera, el certificado lo avisa”¹⁷.

- *Presunción de prueba*: como expliqué en el no repudio, cualquier negación respecto al envío o recepción de un documento firmado digitalmente no será tomado en cuenta,

¹⁶ <http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf>

¹⁷ LORENZETTI Ricardo; *Comercio Electrónico*; Abeledo Perrot, Buenos Aires, Argentina; p. 82.

esto gracias a la intervención de la Entidad Certificadora, convirtiendo de esta manera a la firma en un medio probatorio, correspondiendo a quien niegue su validez, probarlo.

- *Presunción de obligatoriedad:* Al contratar por medios electrónicos con sustento legal de firma electrónica, las partes intervinientes se obligarán legalmente con la simple aceptación de ambas, siendo esta firma manifestación de la voluntad y requisito de existencia de todo contrato, quedando como único motivo de ilegalidad la incursión de cualquiera de los vicios del consentimiento (error, fuerza y dolo) tipificados en el Código Civil.

1.3 Elementos

Dentro de la presente investigación encontré a tratadistas que hablan sobre la presencia de ciertos elementos necesarios para la existencia plena de la firma digital, haciendo un pequeño barrido de lo ya explicado y enumerando puntos claves como el hecho de que la firma digital se la realiza por medios electrónicos, la cual vincula al firmante con el texto, sin que esta conste dentro del propio instrumento como sí sucede en la firma autógrafa, sino que va anexa, transformándose en algo inseparable; que, a pesar de ser éste medio suficiente para demostrar la autoría, no se cumple con la seguridad suficiente para darle valor jurídico, por eso es necesaria la inclusión de criptografía; que, la firma electrónica debe estar bajo estricto control de su titular, ya que él será el único responsable de su uso; y que, el receptor debe estar en capacidad de verificar la autoría, obviamente a través de una Entidad de Certificación. Como vemos, son puntos que ya los he tratado, pero siempre son necesarios su enunciación para así dejar clara toda parte interviniente en este proceso. Lo que realmente me admira y sorprende es el hecho de que dos escritores de distintos países, con distintas fechas de edición, describen estos elementos con palabras textuales, siendo idénticos el uno del otro, dando a pensar que su conexión intelectual es algo asombroso, es por esto que me permito citar a ambos:

“Elemento objetivo-soporte: En un sentido negativo, el soporte no es escrito, y no hay una elaboración manual del autor. En un sentido positivo, la firma es cualquier símbolo procedimiento de seguridad usado por una persona que incluye medios eléctricos, digitales, magnéticos, ópticos, electromagnéticos o similares. Puede advertirse entonces que la firma electrónica no necesariamente debe ir anexa a un documento, como ocurre en el caso de la firma ológrafa sobre un documento escrito.

Elemento subjetivo: Los símbolos asentados en medios electrónicos tienen un propósito específico: se hacen para identificar a la persona e indicar su aprobación del contenido de un mensaje electrónico.

Con estos dos elementos puede haber firma electrónica, pero para que la ley asigne efectos de presunción, es decir, que cada vez que se vean esos signos se presuma que son de su autor, se requiere más seguridad.

Esfera de control del titular: Siendo un elemento de imputación de autoría, es lógico que se requiera que esté bajo el control del titular, ya que sólo él es quien decide qué declaraciones de voluntad son suyas. Por ello, es necesario que la firma pertenezca únicamente a su titular y se encuentre bajo su control exclusivo.

Derechos de verificación del receptor: Se requiere que los sistemas utilizados puedan ser verificados por el receptor para asegurarse de la autoría.¹⁸ y ¹⁹.

2. CRIPTOGRAFÍA

La criptografía no es un arte o ciencia que aparece conjuntamente con el nacimiento de las nuevas tecnologías, este es un método que se ha utilizado desde varios siglos atrás con la finalidad de proteger información de carácter confidencial de cualquier tipo de alteración, modificación o interceptación que pudiera existir, de esta manera se garantizaba la comunicación secreta entre dos personas o grupos.

Por lo general, ésta era usada durante campañas militares para enviar mensajes ocultos entre ejércitos aliados. Las tropas españolas de Felipe II utilizaron durante mucho tiempo un cifrado que consistía en un alfabeto de más de 500 símbolos que los matemáticos de este rey consideraban infranqueable. Cuando el matemático francés François Viète consiguió *criptoanalizar*, y por lo tanto descubrir aquel sistema para Enrique IV rey de Francia, el conocimiento mostrado por el rey francés acarreó una queja de la corte española ante del Papa Pío V acusando a Enrique IV de utilizar magia negra para vencer a sus ejércitos. De igual forma, en la Grecia Antigua, se utilizó una herramienta llamada *scytale*, la cual era un cilindro, de forma y dimensiones específicas, donde cada ejercito aliado tenía uno de ellos; alrededor de este objeto se enredaba una tira de cuero, de tal forma que el

¹⁸ LORENZETTI Ricardo; *Comercio Electrónico*; Abeledo Perrot; 2001; Buenos Aires-Argentina; p. 80.

¹⁹ PÁEZ Ribadeneira Juan José; *Manual de Firmas Electrónicas y Mensajes de Datos*; Corporación de Estudios y Publicaciones; 2005; Quito-Ecuador; p. 48.

cilindro quedará completamente cubierto y así escribir sobre éste el mensaje deseado. Finalmente se enviaba la tira de cuero con un mensaje aparentemente ilegible, llegando a su destino de manera segura.

Como se introdujo al principio de este capítulo, la criptografía consiste en la transformación de mensajes en textos aparentemente ilegibles en donde únicamente el emisor y receptor consiguen resolverlos a su forma original, alcanzando así que cualquier persona que no posea la clave le sea imposible descifrarlo, por lo general su creación es a través de algoritmos con los cuales se crean dos claves diferentes pero matemáticamente vinculadas entre sí, una de estas claves es utilizada para cifrar el mensaje o firmar digitalmente un documento, transformándolo en un texto ilegible, mientras que la segunda clave es utilizada para descifrar el mensaje o verificar la firma digital, transformando nuevamente al texto a su forma original. Este método se lo conoce como criptografía asimétrica de clave pública y es el de mayor uso en razón de las seguridades que brindan, pero no es el único, existe también la criptografía simétrica.

2.1 Características

Las características de la criptografía son muy similares a las funciones que tiene la firma electrónica, esto en razón de que la criptografía es necesaria para alcanzar los objetivos básicos de confidencialidad, integridad, autenticidad y no repudio que posee este tipo de firmas.

A continuación haré un pequeño recuento de estas características incluyendo una quinta la cual es propia de la criptografía.

- Conservar la *confidencialidad* de la información, es decir, el texto el cual ha sido enviado por medios telemáticos serán transformados en ilegibles para que únicamente emisor y receptor sean capaces de descifrar dicha información.
- Dar fe de la *autenticidad* tanto de emisor como receptor, asegurando de tal manera el vínculo inequívoco que debe existir entre emisor/receptor respecto del mensaje.
- Precautelar la *integridad* del mensaje, resguardando la información enviada de cualquier peligro de alteración o falsificación por terceras personas que pudiera existir dentro del lapso de transmisión.
- Garantizar el *no repudio* de la información, determinando irrefutablemente que las partes han enviado o recibido el mensaje.

- Permitir el *control de acceso* de información, garantizando así que solo usuarios autorizados puedan acceder al sistema de datos, teniendo disponibilidad de ellos cuando sean requeridos.

2.2 Criptografía Simétrica

También conocida como tradicional o de clave privada, la criptografía simétrica es aquel método de encriptación en el cual solamente existe una llave idéntica para cifrar y descifrar el mensaje, esto quiere decir que si deseamos utilizar a la criptografía simétrica como medio de autenticación, necesariamente la clave deberá ser conocida por el emisor y receptor, donde ambos tendrán que guardar el secreto.

La ventaja de este sistema radica en que su aplicación es mucho más rápida en comparación de la criptografía asimétrica, es decir, cuando existen textos muy extensos o grandes volúmenes de información al momento de cifrarlos mediante este método su aplicación se resolverá en poco tiempo.

La encriptación simétrica de mayor aplicación es *Data Encryption Standard* más conocida por su abreviatura *DES*, ésta fue desarrollada en los Estados Unidos en 1976 por la compañía de computación IBM; para su época este era un medio tan seguro que hasta fue usado por el gobierno estadounidense para proteger su información. Posterior a este sistema fueron apareciendo otros métodos como 3DES, Blowfish e IDEA, basando su peculiaridad en que poseían claves más extensas, pero igualmente descifrables en un tiempo relativamente mayor.

La rapidez del criptosistema simétrico consiste en la extensión del algoritmo de cifrado que utilizan (no pretendo extenderme en temas técnicos pero creo necesaria una explicación básica para mayor comprensión), por ejemplo, en el cifrado de DES se utiliza una clave de 56 Bits, *Bit* es el acrónimo de Binary Digit (dígito binario), en el cual únicamente se utilizan dos de los números binarios (0 y 1), por lo cual si hacemos el cálculo matemático de 2 elevado a 56 nos da como resultado 72.057.594.037.927.936 claves posibles. Aparentemente es un número muy extenso pero el alto desarrollo de los sistemas de computación hace descifrable a este método en un mediano plazo de tiempo volviendo vulnerable a nuestra información.

Por lo tanto, teniendo un mecanismo donde existe una clave idéntica para cifrar y descifrar el mensaje de datos enviado, existen algunos problemas:

- *Acceso a la clave*; necesariamente ambas partes deben estar en conocimiento de la clave para poder enviar y recibir el mensaje, y lógicamente su envío no puede hacerse a través de un simple correo electrónico. La situación se dificulta, debiendo el remitente contactarse con el destinatario o viceversa, lo cual traba la celeridad del acto, ya que deben recurrir a llamadas telefónicas o encuentros personales, pero ¿qué pasaría si están en distintos países? ¿O su único referente es el correo electrónico de una página Web? Es por esto que se pierde la facilidad que por esencia nos brinda la firma digital.
- *Secreto*; Al ser la clave un dato compartido entre ambas partes, la seguridad de sus mensajes radica en la confianza y sigilo que puedan tener los usuarios para que la información no se vea alterada por terceras personas. *El secreto mejor guardado es aquel que no se cuenta.*
- *Límite de usuarios*; esto va vinculado con el literal anterior; mientras más personas conozcan la clave, más vulnerable es esta. Su uso reside en la confianza de las partes.

2.3 Criptografía Asimétrica

A fin de que la firma electrónica cumpla con todas sus funciones, es necesaria la aplicación de criptografía asimétrica o también llamada de clave pública. Esta clase de criptosistema consiste en que cada usuario tenga un par de claves, una pública la cual podrá ser conocida por todos, y una privada, en donde el propietario deberá guardarla y él será el único que la posea sin que necesariamente la conozca, ya que esta clave privada se podrá encontrar dentro de un dispositivo de memoria individual, dentro del propio ordenador o mejor aún, se podrá acceder a través de un dispositivo de lectura de huella digital, los cuales en la actualidad ya vienen incorporados en algunas computadoras portátiles o como hardware adicional.

Este método fue creado como solución a los problemas que existen dentro de la criptografía simétrica, ya que los riesgos por el intercambio de claves eran altos, basándose únicamente en la confianza de uno a otro. Aquí únicamente se requiere obtener la clave pública del destinatario y enviar el documento firmado.

El cifrado asimétrico tiene sus bases de seguridad en la utilización de números primos (números únicamente divisibles por si mismos y por 1) en donde su encriptación se da aplicando lo que matemáticamente se conoce como *función trampa* (función que se aplica en un solo sentido) esto las convierte en fáciles de cifrar pero difíciles de descifrar, es

decir, multiplicar dos números primos grandes es sencillo, mientras que encontrar los componentes del resultado es excesivamente difícil, donde además existe una *trampa* que consiste en un dato adicional desconocido, volviéndolo mas complicado aun si se llegara a conocer uno de los dos números.

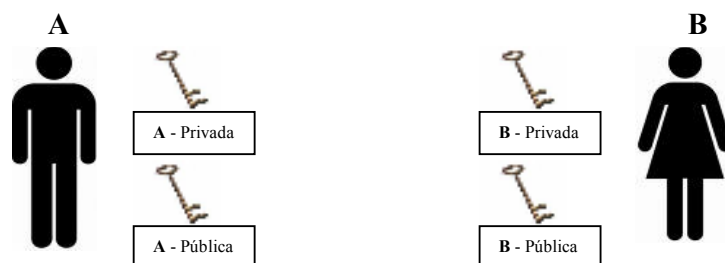
“El criptosistema (o familia de funciones) de cifrado asimétrico o de clave pública, utiliza un par de claves. Una es pública y la otra es secreta o privada. Cada clave efectúa una transformación unívoca sobre el mensaje y es función inversa de la otra, de modo que cada par de claves puede descifrar sólo lo que su par correspondiente cifró.”²⁰

Como vimos, cada usuario estará en posesión de dos claves, publica y privada, la primera será de conocimiento general, mientras que la otra se mantendrá en secreto, ambas claves son usadas para cifrar o descifrar un mensaje, por ejemplo, si tenemos dos sujetos (A y B), donde A quiere enviar un mensaje firmado digitalmente a B, A deberá utilizar la clave pública de B (Kpu) para encriptar el mensaje que ha escrito y lo enviará a B quien mediante su clave privada (Kpr), será el único capaz de descifrar dicho mensaje, pudiendo verificar la identidad del firmante mediante la Kpu del emisor, es decir de A. Por lo tanto, el mensaje fue encriptado por A con la Kpu de B y fue descifrado por B con su propia clave privada.

Lo mismo sucederá a la inversa, en el caso de que A desee enviar un documento digitalmente firmado, lo puede encriptar con su Kpr, para que B lo descencripte con la Kpu de A.

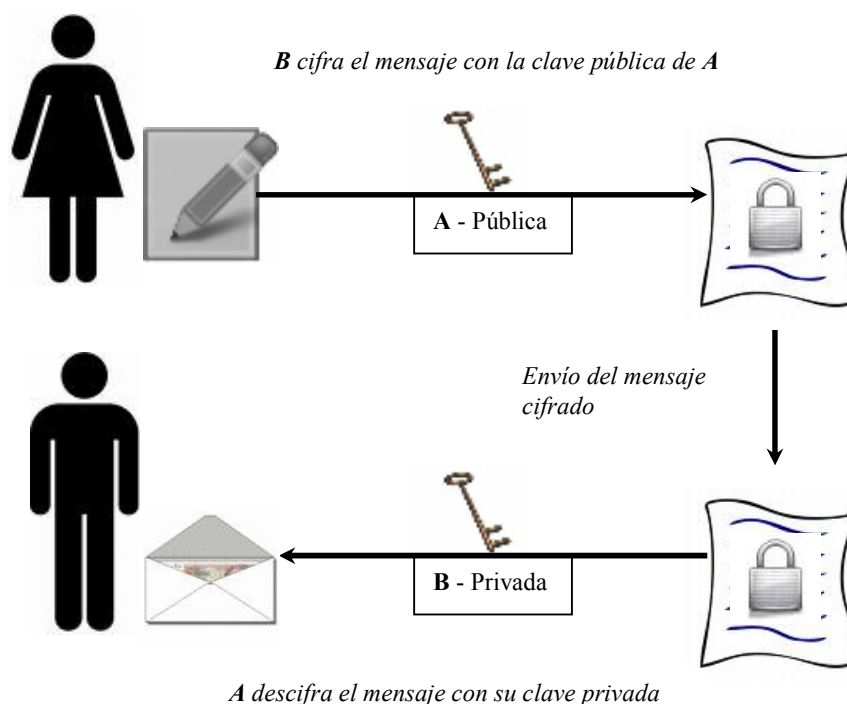
Para mayor entendimiento a continuación se grafica lo explicado:

- **Gráfico 1:**



²⁰ SARRA, Andrea Viviana; *Comercio Electrónico...* p. 60

- **Gráfico 2:** (Proceso)



2.4 Función Hash

Es necesario enfatizar en el hecho de que los algoritmos usados en la criptografía asimétrica de llave pública son significativamente más lentos que los de encriptación simétrica. Por tal razón se utiliza varias encriptaciones las cuales aceleran el proceso, estableciendo la eficacia requerida.

Este cifrado adicional se lo conoce como función hash (*hash function*), cuyo objetivo consiste en obtener un resumen o digesto del texto original. Al hash se lo puede establecer como “un número que se obtiene haciendo una operación matemática sobre todos los datos del mensaje, de tal manera que si el mensaje variara aunque sea en un *bit*, el *hash* sería totalmente diferente”²¹.

Esta función se caracteriza por lo siguiente:

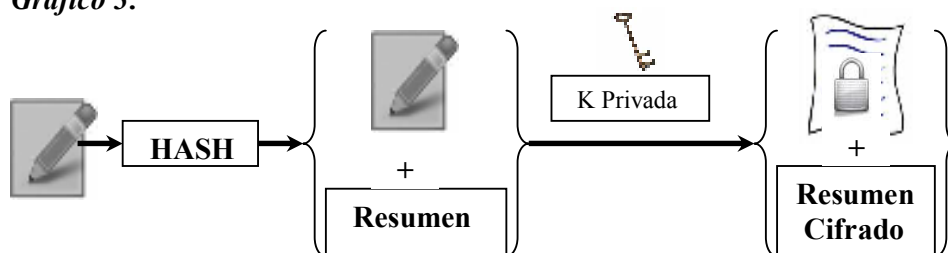
- *Longitud fija*; sin importar la extensión del documento al que se aplique, el resumen que se obtiene no será mayor a 16 bits.
- *Irreversible*; Una vez que se utiliza la función hash sobre un texto, se vuelve imposible adquirir el texto original partiendo del digesto. Es por esto que se diferencia de los

²¹ HOCSMAN Heriberto Simón; *Negocios en Internet*; Ed. Astrea 2005; p. 365

sistemas de compresión comunes, como ZIP, RAR, CAB, etc... los cuales cumplen con el objetivo de reducir el tamaño del texto para posteriormente devolverlo a su estado original.

- *Único*; el resumen hash siempre será unívoco del texto que se aplica, utilizada la función sobre un mensaje de datos, cualquier variación ulterior que se realice sobre el mismo, por insignificante que esta sea, arrojará un hash completamente distinto, garantizando la siguiente característica.
- *Medio de comprobación*; cuando el emisor envía el documento firmado digitalmente, lo hace conjuntamente con el hash respectivo, debiendo el receptor aplicar la función hash sobre el documento que ha recibido para verificar que ambos digestos, el que él efectuó y el que recibió, son exactamente iguales. Se determina de tal manera que no ha existido alteración alguna respecto del mensaje recibido con el documento original, ya que si habría existido interceptación los hash hubieran sido distintos.
- *Celeridad en el cifrado*; como se mencionó, los algoritmos de encriptación asimétrica son lentos y al aplicarlos en documentos extensos podría tomar tiempo, es por esta razón que el emisor se encuentra facultado de firmar el resumen hash, agilizando tiempo de encriptación sin alterar la seguridad ya que a pesar de envíe el mensaje original por la red, el digesto el cual garantiza que no se altera el documento, va encriptado. Por lo tanto, el receptor del mensaje usará la función hash sobre el documento que ha recibido para compararlo con el digesto anexado posterior a la descencriptación del mismo, verificando de tal manera si se ha modificado o no el documento original.

- **Gráfico 3:**



Destacando las ventajas de esta función, Froomkin realiza una enumeración tripartita: “en primer lugar, las funciones hash son públicas, por lo que cualquier personal puede repetir el cálculo para determinar si el documento original fue modificado. En segundo término, es una función de sentido único que permite confirmar que el hash del documento ha variado,

pero no permite recrearlo. En tercer lugar, es prácticamente imposible que dos documentos diferentes produzcan la misma función hash.”²²

3. FUNCIONAMIENTO

Dentro del proceso de firma digital, como es claro, existen dos sujetos involucrados, por una parte el signatario quien es una persona natural o jurídica, la cual firma el documento; y por otra, el receptor que al igual podrá ser una persona natural o jurídica que recibe el mensaje de datos firmado.

Cada uno de estos sujetos posee dos elementos fundamentales para firma y recibir el documento:

El signatario firmará el documento a través de:

- *Datos de creación de firma*; los cuales consisten en códigos o claves criptográficas privadas que el signatario utiliza para crear la firma electrónica.
- *Dispositivo de creación de firma*; es un programa informático o software que aplica los datos de creación de firma (consiste en una clave privada utilizada para encriptar el mensaje.)

El receptor a su vez recibe el documento por medio de:

- *Datos de verificación de firma*; son los datos (códigos o claves criptográficas públicas) que se utilizan para verificar la firma electrónica. Consiste en una clave pública utilizada para desencriptar el mensaje.
- *Dispositivo de verificación de firma*; Al igual que el dispositivo de creación de firma, el de verificación es una aplicación informática o software que utiliza los datos de verificación de firma o clave pública y se encarga de detectar cualquier alteración o modificación de los datos firmados.

Con esta explicación y habiendo ya analizado cada uno de los componentes que se encuentran inmersos en la aplicación de la firma electrónica, a continuación se establece paso a paso el funcionamiento de ésta, ejemplificando el supuesto de que **A** envía a **B** un mensaje de datos:

1. El emisor (**A**) una vez que ha realizado el mensaje de datos que desea enviar, utiliza sobre éste la función hash obteniendo un resumen de longitud fija e incomprensible.

²² FROMKIN; *The Essential role of trusted third parties in Electronic commerce*; www.law.miami.edu/~froomkin/articles/trusted1.htm

2. **A** se valdrá de su clave privada para encriptar el mensaje original y el digesto (o únicamente el digesto si así él lo desea), transformándolos en textos ilegibles, asegurando la confidencialidad del envío. La firma electrónica quedará representada por el mensaje cifrado.
3. **A** envía cifrados tanto el mensaje como el digesto (o solo cifrado el digesto) a **B**.
4. Acaecida la recepción, **B** utilizará la clave pública de **A** (la cual es de conocimiento general) a fin de descifrar los datos encriptados; también conocida como *dispositivo de verificación de firma*.
5. **B** utilizará la función hash sobre el mensaje de datos que ha recibido obteniendo su propio digesto o resumen, para realizar la comparación respectiva entre su hash y el que le fue enviado.
6. De no existir diferencia entre ambos digestos, el proceso habría concluido exitosamente entre **A** y **B** ya que de haber existido una alteración mínima en el mensaje original, habría dado como resultado un digesto diferente entre emisor y receptor.

De esta manera se ha conservando las características de *confidencialidad* por medio del cifrado, *autenticidad* ya que la procedencia quedó determinada a través de la firma, *integridad* en razón de que los dos resúmenes fueron exactos y el *no repudio* por cuanto la clave privada es de uso y responsabilidad exclusiva del emisor; cumpliendo así con los elementos necesarios para la autenticación de un mensaje de datos enviado por medios informáticos.

Es necesario establecer que al efectuar este procedimiento mediante claves creadas por el propio firmante, no existiría el reconocimiento legal necesario ni la seguridad absoluta requerida, es por esto que las firmas electrónicas deben ser certificadas por entidades habilitadas para prestar servicios de certificación de información y demás servicios relacionados, con las cuales existirá un nexo contractual entre la entidad y el usuario atribuyendo los efectos jurídicos a las relaciones posteriores que realicen los usuarios, teniendo derechos y obligaciones los cuales se encuentran debidamente sancionados en nuestra legislación.

Como lo menciona Devoto “La función básica de estos sujetos es la de emitir certificados de clave pública, certificados que vincularán a una persona con una clave pública.”²³

²³ DEVOTO Mauricio; *Comercio Electrónico y Firma Digital*; Ed. La Ley, 2001; p. 209