FIRMA DIGITAL

Julio M. Pérez

El Contraalmirante VGM (R) Julio Marcelo Pérez cursó estudios en el Colegio del Salvador. Egresó de la Escuela Naval en 1958 como Guardiamarina y alcanzó el grado de Contraalmirante, retirándose del Servicio activo en 1992. Realizó estudios de Ingeniería Electromecánica orientación electrónica en la Facultad de Ingeniería de UBA y posgrado en Control y Guiado en la Universidad de Roma (Italia. 1967-68). Profesor en universidades estatales y privadas argentinas nombrado por concurso. Se desempeñó como Rector del Instituto Universitario Naval y actualmente es asesor del director de Educación Naval.
Condecorado por la Armada Argentina y el Congreso Nacional por el diseño, construcción y operación de un sistema misilístico Exocet operado desde tierra con el que, durante el conflicto del Atlántico Sur, dejó fuera de combate al crucero liviano HMS Glamorgan. *Condecorado por el gobierno francés con la "Ordre National du Mèrite" en el grado de Comandante*

Vivimos en un mundo cambiante en el que la tecnología nos asombra día a día con novedades ni siquiera imaginables en los libros de ciencia-ficción. Así vivimos bombardeados por términos técnicos, muchos de los cuales los aceptamos casi con resignación sin comprender lo que significan y en medio de la confusión que nos generan terminamos asignando capacidades inexistentes a algunos procesos tecnológicos o subestimando las posibilidades de otros.

Uno de estos términos que encierra un halo de misterio es el de "firma digital". Desde una ignorancia total podríamos pensar que "no es otra cosa que firmar un documento utilizando la impronta del dígito pulgar", cosa que no es en absoluto cierto, pero, como veremos, tiene un lejano parentesco.

Entender el concepto de firma digital es simplemente entender los conceptos de la criptografía moderna, en particular la que se conoce como criptografía por clave asimétrica o también llamada criptografía por clave pública y que en definitiva no es otra cosa que una aplicación particular de la teoría de números.

El objetivo que nos proponemos es mostrar en forma simple qué es la firma digital, cuáles son los principios en que se basa, sus ventajas y debilidades.

Consideremos previamente cuáles son las características que tiene una firma hológrafa para luego entender lo que debe cumplir la firma digital.

Al firmar en forma manual un documento lo que hacemos es, sintéticamente:

a) Reconocer y acreditar el documento que firmamos y no otro cualquiera.
b) Imponer un agregado al documento (la firma), por el cual reconocemos ante quien lo desee que aceptamos públicamente lo que el documento contiene, es decir que mediante ese proceso no podemos "repudiar" o negar lo que hemos firmado.
c) Asegurar mediante nuestro trazo que dicha firma es propia de nosotros y que (en principio) ninguna otra persona puede haber estampado nuestra firma, es decir que ella representa una característica propia y única del firmante.
d) Si se entabla una disputa vinculada al reconocimiento o no de lo firmado, una tercera parte está en condiciones de verificar y asegurar quién es el firmante sin que para ello necesite (esta tercera parte) efectuar la firma por nosotros.

BOLETÍN DEL CENTRO NAVAL
Número 819
Enero / marzo de 2008
Recibido: 3.11.2006

Los puntos que hemos señalado son obvios y no necesitan mayores explicaciones. Por otra parte, si pensamos en la posibilidad de una nueva forma de firma, como la que encararemos, es evidente que se deben cumplir por lo menos los puntos anteriores.

En este artículo trataremos de mostrar, en forma sencilla, cómo es posible alcanzar dichas condiciones mínimas y aún superarlas.

Definamos previamente, en forma sintética, lo que se entiende por firma digital para luego mostrar cómo es posible su implementación.

La firma digital de un mensaje o documento no es otra cosa que un número (entero) que está vinculado en forma unívoca a un secreto sólo conocido por el firmante y adicionalmente está ligado al contenido del documento o mensaje (ver punto a anterior). Este número debe ser factible de verificar por una tercera parte en caso que se entable una disputa. Dicha verificación debe poderse efectuar sin necesidad que el firmante revele el secreto asociado con su firma.

Obsérvese, en primer lugar, que la firma digital es simplemente un número entero N_f (que en general será largo) que debe estar unívocamente relacionado con un secreto propio del firmante (otro número) y que N_f debe, de alguna manera, estar también unívocamente vinculado con el contenido del documento pues, como ya hemos dicho, lo que firmamos es ese documento y no otro.

Es claro que estamos hablando de números y al hablar de documentos pensamos en letras, números y símbolos que evidentemente no son números. Sin embargo cuando redactamos un documento en nuestra computadora lo que realmente ocurre es que la máquina va guardando números cada uno de los cuales representa a los símbolos del documento (es lo que se conoce por codificación). Un ejemplo típico es el caso del sistema Morse en el cual los símbolos están codificados por una combinación de puntos y rayas que bien podrían ser números.

La forma más común actualmente de codificación, que utilizan las computadoras, de los símbolos utilizados en nuestros documentos es el código ASCII en el cual cada letra, símbolo y número está codificado como un número entre 0 y el 127 (por ejemplo la letra A mayúscula es el 65, el número 7 es el 55, la coma es el 44 y el espacio es 32).

Concretamente, lo que la máquina guarda en su memoria o lo que se envía por las redes de información son números (en realidad no se envían los número en base decimal, sino en base binaria, es decir como un conjunto de unos y ceros que en binario corresponden a la numeración decimal. Así la A sería 1000001, el 7 sería 110111, la coma 101100 y el espacio 100000).

En consecuencia, y sin entrar en el detalle, un documento o mensaje no es otra cosa que un conjunto de números cada uno de los cuales representa un símbolo.

Por lo tanto, resulta claro que es un problema relativamente simple asociar un número representativo (por aplicar un proceso matemático, por ejemplo sumándolos, al conjunto de números que forman el documento) a un documento específico. Nótese que el número resultante depende de los números o símbolos que contiene el documento, de manera que el simple hecho de cambiar una coma por un espacio cambiará el número representativo asociado a ese documento.

Esto último es importante ya que implica que el número representativo que se asocia al documento está ligado a él y cualquier cambio que se haga dará origen a un nuevo número representativo. Esta característica es más rigurosa que en el caso de un documento manuscrito o mecanografiado ya que en este último caso se podría, operando con mucho cuidado, reemplazar, por ejemplo, una coma por un espacio. Podemos entonces afirmar que la asignación de un número representativo (vinculado al contenido) a un documento es la forma más segu-

ra de establecer la inviolabilidad del mismo (siempre, por supuesto, que no pueda cambiarse el número representativo).

En general, el establecimiento de dicho número representativo es un proceso matemático que se realiza mediante un algoritmo que es de conocimiento público. Por razones de conveniencia, dicho número tiene en general una longitud fija independientemente del largo del documento y a la función matemática que realiza el proceso se la conoce como "función de hash" (en general las funciones de hash generan un número entero relativamente corto de 16 a 64 cifras decimales). Lo concreto es que si enviamos un mensaje con la única palabra "si" o enviamos un mensaje con todo el contenido de *El Quijote*, la misma función de hash aplicada a ambos mensajes dará un número representativo de sólo 16 dígitos decimales (según la función de hash que estemos utilizando). Lo que no es posible, desde ya, es que conociendo el número representativo se pueda reconstruir el texto que lo ha generado (se dice que las funciones de hash son *funciones unidireccionales*).

Es evidente que si utilizamos un número representativo de 16 dígitos decimales como hash, puede ocurrir que dos documentos distintos tengan el mismo número representativo ya que con 16 dígitos sólo podemos representar 10^{16} números distintos, pero la probabilidad que ello ocurra es justamente $1/10^{16}$, lo que es una probabilidad sumamente baja.

A lo largo de lo expuesto debe quedar claro que el concepto de firma digital implica que se pueda firmar digitalmente documentos criptografiados así como aquellos que estén en claro (esto se verá al explicar las bases matemáticas del proceso de firma digital) y, por lo tanto, es la herramienta clave para concebir "la empresa sin papeles".

Para poder entender el proceso de firma digital veamos las bases matemáticas del mismo que, como se verá, son sumamente simples.

1- Bases matemáticas

Cuando en los primeros grados del colegio aprendimos a dividir lo hicimos utilizando números enteros como dividendo, divisor, cociente y resto. Así, por ejemplo decimos que 43 = 7 x 6 + 1 donde 43 es el dividendo, 7 el divisor, 6 el cociente y 1 el resto.

Exactamente este concepto es el que utilizaremos, pero tomando ahora no el clásico resultado de la división, sino el resto de ella.

Así, si dividimos 43 por 7 obtenemos un resto que es igual a 1. En cambio si dividimos 43 por 11 obtenemos como resto a 10. Esto es lo que básicamente se conoce por operación módulo y decimos que 43 módulo 7 es igual a 1 y que 43 módulo 11 es igual a 10. Los restos que obtenemos al dividir por un entero *n* son a su vez enteros cuyos valores están comprendidos entre 0 y *n*-1.

La operación módulo tiene la propiedad de ser distributiva respecto a la suma y respecto a la multiplicación y mediante la operación módulo podemos generar un álgebra particular.
Por ejemplo si tenemos que efectuar la operación (27 + 16) módulo 7 es lo mismo que aplicar la operación módulo en forma distributiva, es decir 27 módulo 7 + 16 módulo 7. En efecto los resultados serían:
27 (mód 7)= 6 y 16 (mód 7)= 2, es decir (27 + 16) (mód 7) = (6 + 2) (mód 7) = 8 (mód 7) = 1

Análogamente, por ejemplo (27 x 16) (mód 7) = [27 (mód 7)] x [16 (mód 7)] = 6 x 2 (mód 7) = 12 (mód 7) = 5 que es el mismo resultado haciendo 27 x 16 (mód 7) = 432 (mód 7) = 5

Podemos ilustrar las siguientes dos tablas que corresponden a la suma y a la multiplicación cuando utilizamos, por ejemplo, módulo 7 (se designa como Z_7)

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

?	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Observando la tabla de sumar vemos que, por ejemplo 3 + 4 = 0 (por supuesto módulo 7) es decir que en esta matemática módulo 7 resulta que 4 es igual a -3 (ó 3 es igual a -4) y de la tabla de multiplicar vemos que, por ejemplo 2 x 4 = 1 lo que implica que módulo 7, multiplicar por 4 es igual a dividir por 3 (ó 3 es igual a dividir por 4). En definitiva, vemos que quedan perfectamente definidas las cuatro operaciones básicas del álgebra clásica. Asimismo vemos que nuestro sistema estará formado por un número finito de números enteros del 0 hasta n-1 (en la terminología matemática es lo que se conoce como un “cuerpo finito”).

Ahora bien, las tablas que hemos generado han sido para un número particular, el 7 que es un número primo. ¿Qué ocurre si en lugar de operar con un número primo operamos con un número que no es primo?

Tomemos por ejemplo el 6. Operando como antes resultarían las siguientes tablas:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

?	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

La tabla de suma no presenta problemas como en el caso anterior, pero la tabla de multiplicar presenta la anormalidad que, por ejemplo 2 x 3 = 3 x 2 = 0 cosa que viola el principio que sólo multiplicando por 0 el resultado del producto vale cero (es una de las propiedades generales de lo que se conoce en teoría de números como que *no posee divisor cero*).

Por lo tanto, para salvar este problema aceptemos que utilizaremos sólo números primos como elementos de base para las operaciones modulares (si bien no lo analizaremos, el concepto se puede extender y se puede probar que la condición también es satisfecha por potencias de números primos, lo que se conoce como Cuerpos de Galois y que se desarrolla a través de polinomios irreducibles que son el equivalente a los números primos).

En lo que sigue, trataremos las operaciones módulo en un cuerpo numérico Z_p, donde p es un número primo.

Si vamos a trabajar con números primos, la pregunta que surge es: ¿cuántos números primos existen hasta una determinada cifra? Si bien no existe una expresión que permita determinar exactamente la cantidad de números primos que existen en un determinado

intervalo (debido a la aleatoriedad con que aparecen los números primos), se ha podido determinar que la cantidad aproximada de números primos Y(N) que existen entre 0 y un cierto número N está dada por:

$$\Psi(N) \cong \frac{N}{\ln N}$$

Así, por ejemplo, hasta 10.000 (10^4), existen aproximadamente, $\Psi(10^4) \cong \frac{10^4}{\ln 10^4} = \frac{10^4}{4 \times 1{,}38} = 1086$ es decir hay 1086 números primos menores a 10.000.

Este dato es importante ya que, como veremos, la seguridad en el uso de la firma digital está ligada al tiempo necesario para determinar los números primos que componen a un dado número, lo que se conoce por "factorear".

En el colegio primario hemos aprendido a factorear según el proceso que requiere ir probando divisiones sucesivas por la serie de números primos. Este proceso no ha podido resolverse a través de algún algoritmo eficiente a pesar que desde hace más de trescientos años los más grandes matemáticos han atacado el problema. En resumen, el proceso de factorear un dado número, aun cuando el mismo sea el producto de sólo dos números primos, es, de alguna manera, proporcional al tamaño del número considerado.

Para completar los elementos básicos que necesitamos para explicar el concepto de firma digital veamos dos puntos más. El primero es lo que se conoce como *función fi (φ) de Euler*. Esta función no es otra cosa que "la cantidad de números entre 1 y n-1 que no dividen al número n considerando al 1 como no divisor" (la definición correcta es "la cantidad de números enteros entre 1 y n-1 cuyo máximo común divisor respecto a n vale 1"). Por ejemplo, para el número tres resulta φ(3) = 2, ya que no lo divide el 2 y el 1 por definición de la función fi. Para el número 5 resulta φ(5)= 4 pues son los números 1, 2, 3 y 4. Es evidente que para todo número primo p, es φ(p) = p-1.

En cambio, si queremos conoce la función j de un número no primo (un número compuesto), necesitamos primero factorearlo y luego aplicar la función j a sus factores primos. Así resulta, por ejemplo que si tomamos 385, su factorización es 385 = 5 x 7 x 11 y por lo tanto resulta: φ(385)= φ(5) x φ(7) x φ(11) = 4 x 6 x 10 = 240

Lo último que necesitamos para comprender el proceso de firma digital (y de criptografía por clave pública, tal como se utiliza actualmente) es el que se conoce como *Teorema del módulo de Euler* (que es una extensión del denominado "pequeño teorema de Fermat") que establece:

Sean los números A y M primos entre sí (es decir que pueden ser compuestos pero no poseen ningún factor en común excepto el 1) y los números K y Q tales que K x Q =1 (mód φ(M)) entonces se cumple que: $A^{KxQ} = A$ (mód M)

Veamos con un ejemplo cómo se cumple este teorema:
Sea un número M entero del que calculamos j(M). En razón de la aplicación posterior "armemos" este número como el producto de dos números primos p y q, por ejemplo eligiendo p = 13 y q = 7, es decir que resulta M = 13 x 7 = 91. Resulta inmediato que φ(M) = φ(91) = (p-1) x (q-1)= 12 x 6 = 72.

Elegimos un K primo a j(M) y menor que j(M), por ejemplo K = 29 y determinamos el valor de Q tal que el producto K x Q sea igual a 1 módulo φ(M) resultando Q = 5.

Tomemos ahora un número A primo a M, por ejemplo A = 60 y veamos si se cumple el teorema. Si calculamos A^K módulo M será 60^{29} (mód 91) = 86 *(*)*.

Para verificar el teorema debemos calcular A^{KxQ} (mód 91)= $[A^K$ (mód (91)$]^Q$ (mód 91) = 86^5 (mód 91) y efectuando la operación resulta 86^5 (mód 91) = 60 con lo que verificamos que se cumple.

(*)
En álgebra modular el cálculo del módulo de potencias es simple a causa de la propiedad distributiva respecto a la multiplicación. Por ejemplo 6029 (mód 91) = 60´604´608´6016 (mód 91) y luego calcular el módulo de 604 = (602)2 y así sucesivamente.

Hemos completado así todo el bagaje matemático básico necesario para explicar el proceso de la firma digital.

2- Proceso de firma digital

Supongamos tener un documento al cual le aplicamos el algoritmo de hash (uno de los existentes), que es conocido por todo el mundo, y mediante el cual determinamos el número H. Vemos que si enviamos el documento junto con su H correspondiente, el receptor (o cualquiera que reciba o intercepte el documento que lleva adjunto H) puede tomar el documento, aplicarle la función de hash y obtener un número H_1. Luego de ello, quien recibió el documento verifica si $H = H_1$, y si ello se cumple está seguro que el documento corresponde con el H agregado. Nótese que no decimos que el documento es el original ya que una tercera parte podría haberlo modificado, aplicarle la función de hash y remitirlo como si fuese el documento original.

Ahora veamos cómo se salva el problema de asegurarnos quién realmente envió el mensaje. Supongamos que el que nos envía el documento ha elegido los números primos p y q y calculado el número M como mencionamos anteriormente (para no repetir cálculos vamos a suponer que el hash del documento original H resultó 60, que se eligieron p = 13 y q = 7 y por lo tanto M = 91 y además K = 29 y Q = 5) y cuando envía el documento, además del H agrega al documento el resultado de haber calculado H^K (mód M), es decir, como vimos antes el número 86 siendo el número calculado de esta manera el que se conoce por firma digital (es decir que la firma digital es un número que es distinto para cada documento). Por otra parte, el emisor anuncia públicamente que usa el sistema que hemos visto (que se denomina RSA por las iniciales de sus autores) y que los números clave que utiliza son M (en este caso 91) y Q (en este caso 5) y tiene guardado como secreto, que sólo el transmisor conoce K y j(M) que son 29 y 72. A partir de este momento puede descartar los números p y q.

¿Qué hace ahora el receptor? Como antes aplica el hash y obtiene el número H. Por otra parte al número H le aplica H^K (mód M) (tomando K y M de la información pública que dice que quien envió el documento tiene como números característicos a K y M, es decir que son los números que públicamente identifican al firmante) y si el resultado coincide con el H puede asegurar que:

a) el documento es el original y no ha sufrido modificaciones
b) reconoce al que envió el documento
c) si surgiera, a posteriori, la negativa del remitente a que él es el firmante, un juez puede fácilmente verificar que efectivamente a sido firmado por el remitente.

Según el ejemplo numérico que hemos visto previamente, el sistema no presenta ninguna seguridad pues hasta un alumno del colegio primario podría factorear a M y hallar rápidamente p y q con lo cual calcular $\varphi(M)$.

¿Cómo se asegura entonces la seguridad del sistema? La clave está en generar números primos "grandes". Por ejemplo, si elegimos números primos de 20 cifras (orden 10^{20}) resultará que M es del orden de 10^{40} y tratar de factorear un número de esta magnitud es lo que se conoce en informática como un "problema intratable". Si una persona deshonesta quiere fraguar nuestra firma debe, necesariamente, calcular $\varphi(M)$ para poder luego hallar K y para poder calcular $\varphi(M)$ debe poder factorear el número M.

Si los números primos con que forma M son de igual orden y éste es de 10^{20}, para hallar los factores primos de M debemos probar de dividir a M por todos los números primos comprendidos entre 10^{19} y 10^{20}, lo que implica generarlos y probar las divisiones de M.

La cantidad X de números primos que existen entre 10^{19} y 10^{20} es (de acuerdo a lo visto anteriormente):

$$X \cong \frac{10^{20}}{\ln 10^{20}} - \frac{10^{19}}{\ln 10^{19}} = \frac{10^{20}}{20 \times 1{,}38} - \frac{10^{19}}{19 \times 1{,}38} = \frac{19 \times 10^{20} - 20 \times 10^{19}}{1{,}38 \times 20 \times 19} \cong \frac{10^{20}}{26{,}22} \cong 4 \times 10^{18}$$

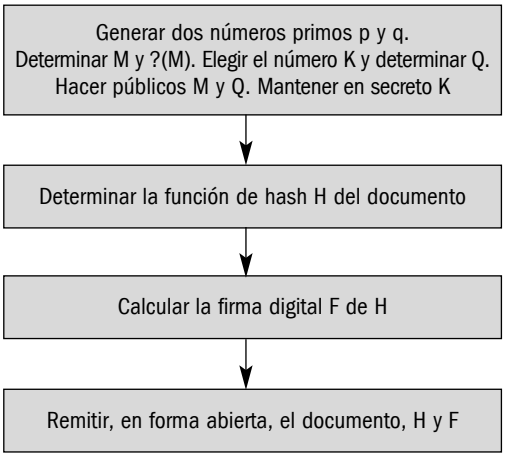
Si suponemos en forma muy optimista que podemos determinar un primo del orden de 10^{20} y verificar si divide a M cada 0,1 de microsegundo (10^{-7} segundos), para probar todos esos primos se requeriría un tiempo $4 \times 10^{18} \times 10^{-7} = 4 \times 10^{11}$ segundos y teniendo en cuenta que en un año hay $3{,}15 \times 10^{7}$ segundos, el tiempo requerido, en años, sería de aproximadamente $4 \times 10^{11} / 3{,}15 \times 10^{7}$ » ¡¡¡13.000 años !!!

En los casos prácticos se utilizan números primos del orden de 10^{20} a 10^{64} y en muchos casos de 10^{128}.

Sobre estos resultados debemos tener en cuenta que los tiempos indicados son en la suposición de tener que determinar ***todos*** los números primos del intervalo considerado. En realidad sólo tenemos que determinar uno de ellos y el resultado mostrado correspondería al caso que sea justo el último de todos los analizados el que resuelve el problema, nada impide que por simple azar, el que se busca fuese el primero de los probados. Obviamente es un problema de probabilidades y ambos casos extremos (de ser el primero o el último) corresponden a probabilidades prácticamente nulas.

Por otra parte hemos supuesto el caso de una única máquina resolviendo el problema en forma sucesiva pero podría pensarse en la operación simultánea (por ejemplo mediante técnicas de procesamiento en paralelo) de muchas máquinas con lo cual se pueden disminuir sensiblemente los tiempos. De todas maneras, actualmente se considera que si los números primos elegidos son del orden de 10^{64} aunque se pudiera procesar con todas las computadoras del mundo en un trabajo coordinado el tiempo para "romper" la seguridad del proceso sería de varios miles de años.

Analizando el ejemplo visto resulta evidente que, obtener la función de hash no es imprescindible, ya que el proceso de firma digital podría realizarse directamente sobre el documento (es lo que se conoce como "*firma digital con recuperación del documento*" ya que en ese caso la firma digital incluye en su proceso a todo el documento y en consecuencia sólo es necesario enviar la firma y no el documento pues el receptor, al efectuar el proceso, recupera el documento). En la práctica se prefiere el uso del hash (lo que se conoce como *firma digital con apéndice*) ya que permite operar con documentos de cualquier tamaño y el proceso de generar y de recuperar la firma digital es mucho más rápido. La firma digital con recuperación del documento sólo se usa en el caso de documentos muy cortos o de longitud fija.
Resumiendo, la forma de firmar digitalmente un documento se puede sintetizar en el esquema que se ilustra (si se usa firma digital con recuperación del documento se omite el paso de generar la función de hash y la firma digital se calcula sobre el documento total).



No es éste el único modo de generar la firma digital. El proceso que hemos ilustrado se conoce como RSA por Rivest, Shamir y Adleman quienes en 1978 desarrollaron este método pero para criptografiar.

El proceso de criptografiar con este método es simple de comprender. En el caso de criptografiar, el que va a recibir mensajes es el que genera los primos, M, φ(M), K y Q y publica en forma abierta que todo aquel que quiera enviarle un mensaje use el método RSA con los parámetros M y Q. El que le envía el documento (supongamos que el documento

está representado por el número D) genera el documento criptografiado D_C según $D_C = D^Q$ (mód M) y lo remite por un medio público. Finalmente, el receptor aplica D_C^K (mód M) de donde recupera el documento en claro D (ver *Revista de Publicaciones Navales*, Tomo CXXXII Nº 683 "La seguridad en las comunicaciones", del mismo autor).

Entre otros métodos de generar firmas digitales, además del más popular que es el RSA existen otros que en general se conocen por el apellido de su o sus inventores tales como El Gamal, Schnorr, Diffie Hellman, etc. pero todos tienen en común que operan en base al concepto visto de la operación módulo (en la planilla de cálculo Excel la operación módulo figura en castellano como Residuo y en inglés como Mod).

3- Conclusiones

Hemos visto así cuáles son los fundamentos de la firma digital, cómo es posible su aplicación y la seguridad que posee. Como resultado de la facilidad y seguridad de su empleo la firma digital está haciendo que las empresas eliminen el uso de papeles ya que toda la tramitación, tanto interna como externa, puede hacerse a través de la vinculación informática asegurando la responsabilidad de los firmantes. No sólo elimina papeles, sino también el personal de empleados administrativos o furrieles, ya que cada responsable puede redactar y firmar sus documentos. Esto se está aplicando desde hace más de diez años en gran número de empresas, las que han reducido del orden del 70% del gasto en papel.

Tanto el proceso de criptografía por clave pública (o asimétrica) junto con la firma digital se encuentran reconocidos y utilizados para las transacciones internacionales. Hoy, a través del empleo de las comunicaciones digitales, las redes de datos y las computadoras personales, se realizan millones de transacciones comerciales, incluso internacionales, sin que los firmantes y responsables de dichas transacciones tengan necesidad de verse.

Es de señalar que el uso de la firma digital es un proceso muy seguro, que como mencionamos es de uso internacional, por lo que debe descartarse la opinión de aquellos que, por no conocer los fundamentos del proceso, "desconfían" de su valor. Si se piensa que se considera que de cada 100.000 personas existe al menos una capaz de falsificar con mucho éxito una firma hológrafa no queda duda que la firma digital tiene, además de otras, una ventaja de seguridad notable para su empleo. ■

BIBLIOGRAFÍA RECOMENDADA PARA QUIEN DESEE PROFUNDIZAR EL TEMA

- An introduction to The Theory of Numbers. *Niven, Zuckerman & Montgomery. Editorial John Wiley*
- Advanced Number Theory. *Cohn. Editorial Dover*
- Algorithmics: Theory and Practice. *Bassard & Bratley. Editorial Prentice Hall*
- Number Theory in Science and Communication. *Schroeder. Editorial Springer*
- Cryptography: An introduction to computer security. *Sberry & Pieprzyk. Editorial Prentice Hall*
- A course in Number theory and Criptography. *Koblitz. Editorial Springer Verlag*
- Algebraic aspects of cryptography. *Koblitz. Editorial Springer Verlag*
- Introduction to Finite Fields and their Applications. *Lindl & Niederreiter. Editorial Cambridge University Press*