SEGURIDAD EN LA TRANSMISION DE LA INFORMACION: LA CRIPTOGRAFIA

Freddy Abarca R.*

RESUMEN

En este trabajo se discute el envío de información que se supone es secreta mediante el uso del algoritmo de Hellman-Diffie-Merkle. La presentación de ese algoritmo permite plantear el tema de la criptografía e introducir una clase de problemas denominados NP.

INTRODUCCION

Plantear el tema "seguridad en la transmisión de información" es sinónimo de colocar en el tapete de la discusión un asunto de mucha actualidad: la criptografía. Por su parte, plantear el tema de la criptografía es asociar dos áreas de estudio que día a día se unen más y más: la informática y la matemática.

Se afirma que la criptografía roza el quehacer de la seguridad de los sistemas de transmisión de la información porque dada la proliferación de microcomputadoras y la facilidad con que se adquiere la tecnología, es más vulnerable la transmisión secreta de información. En este sentido, debe tenerse en perspectiva el hecho de que, para 1992, se estima que solo en los Estados Unidios existirán cerca de veinticinco millones de microcomputadoras a lo largo y ancho del país.

Por otra parte, se dice que la criptografía roza el área de la matemática porque toca el sentimiento de muchos matemáticos al replantearse problemas que datan desde tiempos de Martin Mersenne allá por el Siglo XVII. Este sentimiento matemático se explica muy sencillamente: últimamente a la criptografía se le asocia con los problemas de "factorización primaria" de grandes números que constituyen el fundamento de los más probados algoritmos en transmisión secreta de información.

CRIPTOGRAFIA E INFORMACION

Cuando se habla de transmisión de información se hace en un amplio sentido: información privada referente a transacciones comerciales, historiales médicos, cuentas bancarias y demás, de forma tal que cada uno de nosotros, directa o indirectamente, se ha ligado a la criptografía: desde el envío de una nota confidencial en donde, con solo imaginarse a una tercera persona leyendo el mensaje se siente desvelo (peor aún si la información es vulnerable a la modificación), hasta aquellas escenas de la Segunda Guerra Mundial donde los Aliados descodificaban las rutas de los pertrechos de guerra.

Por su parte, se entenderá por criptografía aquel **arte** de codificar y descodificar "trozos" de información, de forma tal que, una vez enviado el mensaje mediante algún canal de dominio público, se tiene la seguridad de que para terceras personas, esos trozos de información carecen de valor.

Para empezar la discusión se debe establecer que, por lo menos hasta el día de hoy y hasta donde el autor tiene conocimiento, aún no se tienen las herramientas necesarias para garantizar con certeza la imposibilidad de la descodificación de información: basta con leer la historia para percatarse de ello, o estar pendiente de las "fisuras no controladas"

* Centro de Investigaciones en Computación. Instituto Tecnológico de Costa Rica

(*leaks*) de organizaciones supuestamente seguras en el manejo de la información.

Es frecuente comparar la criptografía con una "caja" con un candado en donde se deposita el mensaje pero con una importante variante: quien envía y quien recibe el mensaje "se ponen de acuerdo" en la secuencia de "caracteres" que se transmitirán por medio del canal de comunicación (en otras palabras definen la "llave"). Colocando el mensaje en la caja, cerrada y enviada, se evitaría la posible modificación del mensaje... siempre y cuando las claves para descodificar sean seguras.

La analogía anterior induce a pensar en la existencia de muchos sistemas de criptografía. Comúnmente se habla de dos: los sistemas que solo requieren una llave secreta, también llamados **sistemas de llave privada,** y los sistemas de dos llaves, también llamados **sistemas de llave pública;** mientras que en el primer sistema una sola cllave codifica y descodifica, en el segundo se requieren dos llaves: una para codificar y otra para descodificar. En cualesquiera de los dos sistemas señalados, el proceso se inicia cuando se cifra un texto –por lo general en una serie de dígitos– produciéndose un texto codificado, al que debe aplicársele la "inversa" de la codificación –esto es la descodificación–, para descifrar el mensaje enviado.

Se nota entonces que en la técnica criptográfica de llave pública, como en la sustitución y transposición que se estudiará en este trabajo, se tienen los siguientes tres elementos: **un mensaje fuente** que se desea enviar utilizando algún "canal inseguro" –como ondas de radio, por ejemplo–, **un algoritmo** que codifica o transforma la información de una manera muy especial, y, **un par de llaves** una de las cuales supuestamente muy segura, de forma tal que cuando se aplica el algoritmo al mensaje fuente, codifica y descodifica ordenadamente el mensaje deseado utilizando la llave pública y la llave privada respectivamente.

A pesar de que hubiese sido deseable que los tres elementos anteriores fuesen totalmente secretos, la experiencia demostró que el algoritmo propiamente no pudo permanecerlo (es decir tener el estatus de "clasificado") como hubieran deseado muchos usuarios urgidos de seguridad, de ahí que el problema de criptografía se reduce al "diseño" de llaves seguras y "cómodas" de operar por lo menos en aquellos sistemas denominados de "llave pública".

Por otra parte, el "diseño" de llaves *per se* no es tarea nada fácil dado que ellas deben de reunir una serie de características y propiedades. La generación y distribución de las llaves, la autenticidad de una llave dada, la modificación de llaves existentes, son algunas características que tiene que resolver el diseño completo de llaves.

Para discutir sobre criptografía se describirá una técnica criptográfica desarrollada por Hellman-Diffie-Merkle, sin que ello signifique que sea la única que existe, naturalmente. La razón de por qué se estudiará este algoritmo es porque trae consigo uno de los problemas clásicos de la Ingeniería Industrial: el problema de la mochila.

Como se dijo, existen muchas otras técnicas criptográficas, por ejemplo el sistema de una llave DES, *Data Encryption Standard*, desarrollado por la IBM para la Agencia de Seguridad de los E.E.U.U.; los sistemas utilizan lo que se denomina "super-criptografía", que en el fondo consiste en repetir un sistema estándar varias veces; el sistema Rivest-Shamir-Adleman, más comúnmente conocido como RSA, quizás el sistema líder en el campo, cuya seguridad descansa en el problema de la factorización; y, desde luego, es natural esperar la existencia de muchas otras técnicas muy confiables que por razones fáciles de entender no se publican.

El Algoritmo de HELLMAN-DIFFIE-MERKLE[1]

Este algoritmo, publicado en la Universidad de Stanford en 1976 por Martin Hellman, Whitfield Diffie y Ralph Merkle[2] se basa en el clásico problema de "la mochila" y en aquella idea que todos tenemos de "puertas secretas", es decir, cuando dada una pared que una persona "debe traspasar", se necesita saber cuál es el preciso ladrillo que debe presionarse para permitir el paso "a través de la pared". El "problema de la mochila", por otro lado, es aquel que busca resolver el siguiente planteamiento: dada una capacidad máxima de peso "p" capaz de soportar un espacio, y dados "n" artículos, cada uno de ellos con peso "p (i)" que perfectamente pueden incluirse en ese espacio si la capacidad total fuese ilimitada, se desea saber cuál artículo debe incorporarse en "p" de forma tal que una medida de efectividad dada se optimice. Dada esta particularidad del método, no por obra de la casualidad, Hellman, Diffie y Merkle llaman a su

sistema criptográfico con el nombre de *Trapdoor Knapsack System.*

Si se deseara enviar un mensaje confidencial utilizando este algoritmo, la persona mira su propia llave pública en una guía y codifica su mensaje. El mecanismo propio de codificación se describirá posteriormente. Una vez codificado el mensaje y enviado, sería descifrado por la persona receptora utilizando la segunda llave, la llave secreta diseñada para descifrar. Con esta particularidad del método, una vez enviado el mensaje ni la misma persona que envía el mensaje está en capacidad de descodificarlo por carecer de la llave de descodificación.

El método

La metodología de Hellman-Diffie-Merkle se inicia con la conversión del texto del mensaje al sistema binario. Por ejemplo, si se convirtieran las letras del alfabeto al sistema binario, un texto común tal como "ITCR" se leería así: "01000100110001010001", esto es, y si se reserva a la letra A el valor "00000", la letra "I" sería la octava, "01000" en forma binaria y así sucesivamente para las letras "T", "C", y "R": "10011", "00010", "10001", respectivamente.
Luego interviene el concepto de "llave pública". Una llave pública es un número público –más bien un conjunto de números– que se publica y distribuye en guías como si fuesen las populares guías telefónicas.

Las llaves, antes que un número absoluto, son en realidad lo que matemáticamente se conoce como un vector: un conjunto de números o de elementos como se les llama en el álgebra matricial, que vectorialmente unidos forman un conjunto; por ejemplo, si la llave pública se denominara con la letra "A", en realidad implícitamente se habla de un valor "A" de tamaño "n" definido así:

$$An = [a_1, a_2, a_3, a_4, ..., a_n]$$

donde cada "a_i" es un número y "n" la longitud del vector.

Para codificar el mensaje se hace uso de la multiplicación vectorial denominada "punto" siendo esta operación matemática el fundamento del método[3].

La información que se va a enviar es transformada en un vector "X_n",

$$Xn = [X_1, X_2, X_3, X_4, ..., X_n],$$

el que prácticamente contiene elementos con valor de cero y la unidad. Este vector se multiplica puntualmente con el vector llave pública, "A_n" produciendo el número "C" que eventualmente representaría el mensaje cifrado. El número "C" se envía mediante cualquier canal con la certeza de que nadie descifraría su contenido. Para entender mejor este paso, tómese el siguiente ejemplo.

Conocida la llave "A_n", si se deseara enviar el mensaje "ITCR", "01000100110001010001", en sistema binario, el número "C" resultaría con un valor de 77, así

X_n = [0,1,0,0,0,1, 0, 0, 1, 1, 0, 0, 0, 1,0,1,0,0,0,1]
A_n = [12,5,7,2,1,3,4,20,31,15,0,50,3,4,9,9,8,2,4,10]
C = [0+5+0+0+0+3+0+0+0+31+15+0+0+0+4+0+9+0+0+0+10]
C= 77

Principio del método

La tarea para una tercera persona interesada en descifrar el mensaje sin estar autorizado para ello, es decir, la tarea de revertir el proceso y conocidos "C" y "A_n" deducir "X_n" es en realidad la resolución del "problema de la mochila" donde cada elemento que se "desea incluir en la mochila" tiene igual prioridad. Razónese de esta manera: si el artículo está "marcado" con un "1" se incluiría en la mochila mientras que si estuviese "marcado" con un "0", no se incluye.

La tarea para esta persona es sumamente ingrata si opta por la búsqueda exhaustiva: tendría que probar 1 048 576 posibilidades, esto es 2^{20} pues el mensaje tiene longitud de tamaño veinte. Es en este preciso momento en que se inicia el aporte de Martin Hellman, Whitfield Diffie y Ralph Merkle a la criptografía. Con el afán de generar un "problema de la mochila" muy especial y fácil de solucionar a la vez cuando se manipulan algunas características –recuérdese la analogía de la pared secreta en la que se fundamenta el sistema– se refina el vector "A'_n" de forma tal que tenga un atributo clave:

Se define un nuevo vector "A'_n" con la siguiente particularidad: cada elemento de "A'_n" tiene que ser mayor que la suma de todos elementos que le preceden. En otras palabras,

$$a'_i > a'_1 + a'_2 + a'_3 + ..., a'_{i-1}$$

de tal forma que cada elemento "a_i" se obtiene de la siguiente manera:

$a_i = (a'_i * w)$ módulo m donde "w" y "m" son dos números aleatorios enteros, grandes... y preferiblemente primos relativos. Si estos números no fuesen primos pudiera ser que no exista una inversa para "w" o "m", condición necesaria en el algoritmo.

De esta forma, si para un tamaño 10 el vector "A'_n" fuese [4]:

$A'_n = [3, 5, 11, 20, 41, 83, 169, 340, 679, 1358]$

y dados los valores para "w" de 764 y de 2731 para "m", los valores de "A_n" estarán determinados por:

$A_n = [2292, 1089, 211, 1625, 1283, 599, 759, 315, 2597, 2463]$

de forma tal que, por ejemplo para el cuarto elemento del anterior vector, un resultado sería:

$a_4 = (20 * 764)$ módulo 2731

$a_4 = 1625$

Con esta nueva llave pública tan *sui generis*, el envío de únicamente las dos primeras letras del mensaje "ITCR", y valga decir "IT", se haría mediante el número 6784, calculado de esta forma:

$X_n = [0, 1, 0, 0, 0, 1, 0, 0, 1, 1]$
$A_n = [2292, 1089, 211, 1625, 1283, 599, 759, 315, 2597, 2463]$
$C = [0+ 1089+ 0+ 0+ 0 + 599+ 0 + 0 + 2597+ 2463]$
$C = 6748$

Un valor "C´" asociado a "C"

Dado es de esperar que el escalar "C" disponga de un valor asociado "C´", esto es cuando en vez de "A_n" se utiliza "A'_n", el valor de "C´" sería:

$X_n = [0, 1, 0, 0, 0, 1, 0, 0, 1, 1]$
$A'_n = [3, 5, 11, 20, 41, 83, 169, 340, 679, 1358]$
$C' = [0+ 5+ 0+ 0+ 0+ 83+ 0+ 0+ 679+ 1358]$
$C' = 2125$

Como se describió anteriormente, enviado y recibido el mensaje codificado, la tarea de descodificación es perfectamente equivalente a resolver el problema de mochila, pero merced a la forma tan particular de generar el vector "A'_n", el problema se simplifica: la reconstrucción del vector "X_n" –y por ende la lectura del mensaje– se regeneraría notando si cada elemento de "A'_n" está o no contenido dentro de la magnitud del valor de "C´" o, eventualmente, el remanente de "C´".

Por ejemplo, si el valor de "C´" es igual a 2125, definitivamente "X_{10}" "existe", esto es, "X_{10}" vale la unidad dado que el valor de "C´" es mayor que el valor de "a'_{10}", en otras palabras 2125 es mayor o igual a 1358. Una vez "colocado" "X_{10}", el remanente de "C´" será 2125-1358 = 767. Siendo "X_9" menor que esa cantidad, se selecciona de igual manera. El restante valor de "C´", 88, no "alcanzaría" los elementos 7 y 8 del vector "X_n" por ser números mayores que 88. Al seleccionar el elemento "X_6" habrá un remanente de 5, con lo que continuaría el proceso hasta reproducir todo el vector "X_n". Conocido el vector X_n el paso a la espanolización del mensaje" es elemental.

La descodificación

En el párrafo anterior se explicó cómo descodificar si el escalar enviado fuese 2125. No obstante, el secreto del método está en enviar el valor de "C" en vez de "C´". Ello se hizo en aras de explicar la facilidad de descodificación.

Para discutir lo necesario por hacer si se envía el número 6784 en vez de 2125, es pertinente recurrir nuevamente a la aritmética modular y muy especialmente con el concepto inversa en aritmética modular. Dos números pertenecientes a un módulo común se dice que son inversos entre sí si multiplicados dan por resultado la unidad, es decir si para el número "Y" se tiene por inversa al número "Y^{-1}", entonces.

$Y * Y^{-1} = 1$ módulo m

en forma más general, si dado

$X * Y = Z$ módulo m

y teniendo a "Y^{-1}" como la inversa de "Y", entonces,

$X = Z * Y^{-1}$ módulo m

Con ayuda del operador módulo se reconstruye el escalar "C´".

Multiplicando el escalar "C" por la inversa de "w", "w^{-1}",

$C = x_1 * a_1 + x_2 * a_2 + ... + x_n * a_n$
$C * w^{-1} = (x_1 * a_1 + x_2 * a_2 + ... + x_n * a_n > * w^{-1}$
$C * w^{-1} = x_1 * a_1 * w^{-1} + x_2 * a_2 * w^{-1} + ... + x_n * a_n * w^{-1}$

y recordando que cada elemento del vector "A_n" se calcula mediante la congruencia,

$a_i = a'_i * w$ módulo m
se tiene que,
$a_i * w^{-1} = a'_i$ Módulo m

Sustituyendo en la útima expresión de "$C*w^{-1}$", se obtiene:

$Cw^{-1} = x_1 * a'_1 \bmod m + x_2 * a'_2 \bmod m + ... + x_n * a'_n) \bmod m$
$Cw^{-1} = (x_1 * a'_1 + x_2 * a'_2 + ... + x_n * a'_n)$ módulo m

la cual, recordando la propiedad conmutativa del operador módulo,

Cw^{-1} módulo $m = x_1 * a'_1 + x_2 * a'_2 + ... + x_n * a'_n$

que evidentemente produce el "C" tal como anteriormente se describió, es decir,

$C' = x_1 * a'_1 + x_2 * a'_2 + ... + x_n * a'_n$
$C' = C * w^{-1}$ módulo m

Regresando al ejemplo numérico con C=6748, m=2731, y, w^{-1} = 1605, un resultado de la expresión anterior es:

C´= 6748 * 1605 módulo 2731
C´= 2125

En otras opalabras, el cálculo de "C´" es "lo único" necesario para descodificar el mensaje porque es precisamente en este detalle donde descansa la confiabilidad del método. Conocido "C´", la persona que recibe "C" utiliza su vector "A'_n" para resolver el problema "de la mochila" con "C´" y así recuperar el vector "X_n", el mensaje, como se analizó anteriormente.

La Inversa modular

No obstante, y hasta este punto, permanece un problema aún sin resolver: el cálculo de la inversa de "w". Hellman sugiere determinar la inversa basándose en el algoritmo de Euclides para encontrar el máximo común divisor[6].

Para dos enteros "a" y "b", el algoritmo de Euclides para encontrar el máximo común divisor y para cada "r_i" mayor o igual a cero pero estrictamente menor a "r_{i-1}", se procede de la siguiente manera:

$a = t_0 b + r_1$
$b = t_1 r_1 + r_2$
$r_1 = t_2 r_2 + r_3$
.
.
.
$r_{k-3} = t_{k-2} r_{k-2} + r_{k-1}$
$r_{k-2} = t_{k-1} r_{k-1} + r_k$

de forma tal que cuando "r_k" sea igual a cero, "r_{k-1}" es el m.c.d. de "a" y "b". Justamente cuando "r_k" sea igual a la unidad –no a cero–, y trabajando "hacia atrás", es cuando fácilmente se pueden ubicar las inversas buscadas.

Para el caso particular de los números 2731 y 764, se tiene que:

2731 = 3 * 764 + 439
764 = 1 * 439 + 325
439 = 1 * 325 + 114
.
.
.
17 = 1 *12 + 5
12 = 2 * 5 + 2
5 = 2 * 2 + 1

luego,

1 = 5 –2 * 2

1 = 5 –2*(12 - 2 * 5)
1 = 5 * (1 + 2 * 2) –2 * 12
1 = 5 * 5 –2 * 12

1 = 5 * (17 - 1 * 12) -2 * 12

y así sucesivamente hasta configurar la inversa.

Resumen del método

Dado un mensaje "X_n" que se va a enviar, codifíquesele mediante el cálculo de "C". Para descodificar el mensaje, calcúlese "C´"; con "C´" el vector "X_n" fácilmente se deduce.

Nótese cómo "A_n" es de conocimiento público, pero los valores de "w", "w^{-1}", "m" y el vector "A'_n" deben ser absolutamente secretos.

Los problemas NP

Se denominan "problemas NP" a aquellos problemas que se están planteando, mejor dicho replanteando a la luz de las herramientas de que dispone el hombre contemporáneo, cuyas soluciones descansan en algoritmos o metodologías que, conforme el problema en estudio crece en tamaño, el algoritmo de solución requiere cantidades de tiempo "exponenciales" para obtenerla. Este grupo de algoritmos donde el tiempo requerido para encontrar la solución es función no polinomial, generalmente exponencial, son conocidos como algoritmos NP. Del mismo modo, se llaman algoritmos polinomiales, algoritmos P, a aquellos en que la variable tamaño no es precisamente exponencial en el sentido amplio de la palabra, dentro de la función estimadora del tiempo real para encontrar la solución o conjunto de soluciones.

Es mi entender que el "encanto" por los problemas NP se remonta a unos sesenta años atrás, cuando se conjeturaba si las demostraciones a teoremas matemáticos podrían hacerse "automáticamente" "mediante algún proceso mecánico". Resultado de este ambiente de trabajo es "la máquina imaginaria" de A. M. Turing, quien postulara que **cualquier algoritmo** podría ser ejecutado por una máquina que dispusiera de dos elementos: un dispositivo similar a una impresora actual y un sensor, donde la "impresora", alimentada con infinita cantidad de papel cuadriculado, sería capaz de imprimir y borrar marcas en los cuadros mientras que el sensor, por otro lado, avisaría al usuario cuando un determinado cuadro estuviese o no marcado.

La particularidad de esta máquina –hipotética desde luego– es que es perfectamente programable y, vía programas, capaz de encontrar soluciones a un problema dado, después de ejecutar una cantidad **finita** de operaciones, esto es, de discriminar los "cuadros marcados"[7].

Resultado concreto de esta lógica es el hecho de que si un problema cualquiera puede ser resuelto por la Máquina de Turing es perfectamente aceptado como una condición necesaria y suficiente para la solución de ese problema **vía** algoritmo. Este hecho es trascendental.

A partir de los años posteriores a 1930, por tanto, el universo de los problemas –y hablando muy generalmente desde luego, ya que el tema de problemas NP es muy amplio– se plantearon en dos grandes áreas; aquellos problemas que carecen totalmente de algoritmos que conduzcan al investigador a la solución, problemas denominados "insolubles", y por otro lado, aquellos problemas "difíciles" que disponen de procedimientos bien definidos para obtener la solución, independientemente si la solución es o no encontrada en forma eficiente. De este segundo grupo de problemas, y con fundamento en la efectividad del algoritmo planteado para ubicar la solución al problema, el subconjunto de problemas se subdividen en problemas polinomiales no determinísticos[8] y problemas polinomiales; más abreviadamente, "Problemas NP" y "Problemas P".

Se desea insistir en dos de las características más sobresalientes de los problemas NP (los problemas clase P pueden interpretarse como un subconjunto de los problemas NP). El hecho de que la búsqueda de su solución puede requerir muchos años de trabajo, pero, la verificación de ella se hace en segundos, y, como dijera Conway en 1967, los problemas NP "son muy fáciles de enunciar... pero difíciles de solucionar"[9] de forma que, a una subclase de estos problemas, los denominados problemas NP completos se les ha demostrado que son computacionalmente "imposibles". Peor aún, cuando un problema se clasifica como NP completo para muchos investigadores es suficiente motivo para utilizar métodos enumerativos o heurísticos que eventualmente generarían soluciones aproximadas a la solución óptima[10].

El problema de la mochila es por excelencia un problema NP completo, algunos autores son del criterio de que la seguridad de un sistema criptográfico es en el fondo equivalente en dificultad a un problema NP completo.

Factorización de los números primos

Desde los tiempos de Euclides los números primos han acaparado la atención de científicos muy en especial cuando han de enfrentarse a la factorización de grandes números, problema actual de la criptografía como previamente se explicó. Un número primo es aquel número entero que es divisible únicamente por él mismo y por la unidad.

El problema de la factorización, que no es un problema NP, se reduce a determinar cuándo un número grande es primo o no, o bien, dado un número grande, determinar cuál sería la mejor estrategia para ubicar sus factores y así catalogarlo o no como número primo. Inclusive es perfectamente aceptado que es mucho más fácil la labor de probar que un número es primo, a la labor de encontrar los dos números primos cuyo producto es conocido.

A inicios de 1984 se corroboró que un número de 69 dígitos, el número $(2^{251}-1)$, no era primo; esta verificación se realizó en el Laboratorio Nacional de Sandia, Nuevo México, después de 32 horas 12 minutos de trabajo continuo en una supercomputadora Cray, solución muy celebrada pues el problema lo planteó Martin Mersenne desde del Siglo XVII[11]. A los números (2^q-1), donde "q" es primo, se les denominan números de Mersenne, ya que él conjeturó desde esos tiempos que para valores de "q" menores o iguales a 257 solamente los siguientes valores de "q" dan lugar a números primos: 2, 3, 5, 7,13, 17, 19, 31, 67,127, 257, aseveración que posteriormente se corroboró tiene dos conjuntos de errores: las potencias de 67 y 257 no conforman números primos y, por otro lado, no se considera que las potencias de 61, 89 y 107 constituyan números primos[12]. Para el lector interesado, es oportuno apuntar que Pomerance recoge las épocas históricas en que se demostró que ciertos números de Mersenne son primos[13].

Más recientemente, el pasado mes de Octubre de 1988, Mark M. Manasse y Arjen K. Lenstra fraccionaron un número de 100 dígitos con una estrategia muy particular: utilizando una metodología ya conocida y que no se discutirá, distribuyeron "el trabajo" entre días de trabajo continuo[14].

LA CRIPTOGRAFIA EN PERSPECTIVA

No hay duda de que la criptografía es una de las áreas de la informática que ha sido fuertemente impactada por el avance tecnológico de las nuevas herramientas. Escasamente hace 12 años, en 1977, el Rivest, uno de los autores del Sistema RSA, era del criterio que un número de 125 dígitos "era imposible" de factorizar hasta tal punto que calculaba un período de tiempo de cuarenta cuatrillones de años para factorizar un número de tal dimensión. No obstante, hasta fines del año 1988 –y hasta donde el autor tiene conocimiento–, con el sistema de Manasse y Lenstra la actividad antes descrita se estima que requeriría "únicamente" un año[15].

NOTAS

1. Hellman, M. E. *The Mathematics of Public-Key Cryptography,* **Scientific american**, Vol. 241, Número 2, Agosto 1979, página 130. Dada la vigencia de este artículo, la revista **Trends in computing** lo reproduce en su Vol. 1, Número Especial, Octubre de 1988, página 78, una vez actualizado por el autor.

2. En esos tiempos, tanto Diffie como Merkle eran alumnos del Dr. Hellman en Stanford.

3. Dados dos vectores de igual tamaño, la multiplicación vectorial "punto" se define de la siguiente forma: dados dos vectores,

   $R_n = [r_1, r_2, r_3, r_4, ..., r_n]$
   $S_n = [s_1, s_2, s_3, s_4, ..., s_n]$

   el producto punto de "$R_n \cdot S_n$" produce el escalar "T" equivalente a la suma de las multiplicaciones de cada elemento de "R_n" y "S_n" de esta forma:

   $T = r_1 * s_1 + r_2 * s_2 + r_3 * s_3 + ...+ r_n * s_n$
   donde "*" indica la multiplicación algebraica.

4. Buena parte de los cálculos numéricos están tomados directamente de la referencia de Hellman antes citada.

5. Por limitaciones tipográficas, se utilizará el símbolo de la igualdad "=" para especificar la congruencia,a pesar que la convención es la de tres pequeñas líneas paralelas.

6. Se desea agradecer en este punto la colaboración de Sr. Mario Marín, Profesor del Departamento de Matemática del Instituto Tecnológico de Costa Rica.

7. Stockmeyer, L. J.; Chandra, A. K. *Intrinsically difficult problems,* **Trends in computing,** Vol. 1, Número 1, Octubre de 1988.

8. *Non-deterministic polynomial problems,* en la literatura inglesa.

9. Conway, R. W.; Maxwell, W. L.; Miller, L. W. **Theory of scheduling.** Addison-Wesley Publishing, Reading Massachussets, 1967.

10. Lewis, H. R.; Papadimitriou, C. H., *The efficiency of algorithms,* **Scientific american,** Enero de 1978, página 96.

11. *Craking a record number,* **Time,** 13 de Febrero de 1984, página 47.

12. Jones, B. W. **Teoría de los números.** Editorial Trillas. 1a. traducción al español, 1969, página 68-69.

13. Pomerance, C., *The search for prime numbers,* **Scientific american.** Diciembre de 1982, página 136.

14. *Technology.* **TIME.** 24 de Octubre de 1988, página 40.

15. Russell, R. *Factoring Googols,* **Scientific american,** Vol. 259, Número 12, Diciembre de 1988, página 12-13.