



32 años de criptografía asimétrica y de clave pública

A principios del pasado diciembre pasó por España para dar un par de conferencias el **Dr. Martin Hellman**. La primera de ellas fue para hablar de su participación en el invento de la criptografía de clave pública y del protocolo que lleva su nombre, y la segunda como parte de su activismo contra la guerra.

Hellman, de pura cepa neoyorquina, se licenció en 1966 en la Universidad de Nueva York, para luego cambiar de costa e irse a la Universidad de Stanford donde adquirió primero el grado de máster en 1967, y luego el de doctor en 1969; todo ello en ingeniería eléctrica. Durante los años 1968-1969 trabajó en el Watson Research Center de IBM donde coincidió con **Horst Feistel**. Entre 1969 y 1971 fue profesor titular del MIT, para terminar regresando a Stanford en 1971 donde desarrolló sus actividades hasta 1996, fecha en la que pasó a ser Profesor Emérito de dicha institución.

En la citada conferencia –auspiciada por la **Cátedra UPM Applus+ de Seguridad y Desarrollo de la Sociedad de la Información**– rememoró el nacimiento del concepto de criptografía de clave pública hace ya treinta y un años. Todo empezó a principios de la década de los setenta, tiempos en los que **Hellman, Diffie y Merkle**, meditaban sobre cuál era el componente elemental y más sencillo sobre el que construir

Hace más de treinta años que se inventó el concepto de criptografía de clave pública y uno de sus inventores, Martin Hellman, tuvo ocasión de recordarlo recientemente en Madrid. Con la perspectiva que da el tiempo, y con pocas alternativas en este sector, empieza a ser el momento en el que plantearse si se puede seguir confiando en el RSA, si hay que pasar a las curvas elípticas o si, por el contrario, todavía queda mucho que hacer en la criptografía asimétrica.

toda la criptografía.

Ellos identificaron a las funciones de sentido único como una pieza clave para poder construir la criptografía moderna. Dentro de esas cavilaciones, se plantearon la posibilidad de que hubiese funciones que fuesen de sentido único para todos y no para unos pocos. Con esa segunda asimetría esencial, acuñaron el concepto de funciones

todo este último, percibieron la utilidad que tendrían ese tipo de sistemas para resolver el problema esencial de la criptografía simétrica convencional, que no es otro que el de la distribución de claves simétricas.

En su conferencia, Hellman contó, con la tranquilidad de quien puede hacerlo de primera mano, lo fácil que fue pergeñar el protocolo de negociación de

esencialmente secreta. A ese protocolo, según el Dr. Hellman, debería llamarse de “*Diffie-Hellman-Merkle*”², y esos tres autores solicitaron su patente en EEUU al año siguiente de su publicación³ (USA Patent 4.200.770).

Revisiones

Desde su publicación, son varias las revisiones que se han hecho de aquel artículo seminal. La primera fue por parte de los mismos autores a los diez años de la publicación del original. La segunda se produjo en 2003, donde se recurrió a volver a publicar el artículo original incluyendo algunos nuevos ma-



Con un sencillo juego conceptual, Diffie, Hellman y Merkle –sobre todo este último–, percibieron la utilidad que tendrían ese tipo de sistemas para resolver el problema esencial de la criptografía simétrica convencional, que no es otro que el de la distribución de claves simétricas.

de sentido único con trampa, y con ello la Criptografía de clave pública.

De hecho, la clave pública es esa función de sentido único que todos pueden calcular con cierta eficiencia, pero nadie puede invertir, y la clave privada es esa información que se mantiene en secreto y que desbarata la característica de sentido único de la función anterior. Con este sencillo juego conceptual, Diffie, Hellman y Merkle, sobre

claves que lleva su nombre. Buscando una función asimétrica, preguntó a un amiguete matemático, que era **John Gill** –un gran desconocido en todo este tinglado–, y a él le atribuye el mérito de haber elegido el logaritmo discreto en aritmética modular como función difícil, como función de sentido único¹. Así pues, en ese punto ya tenían establecido un protocolo que permite a dos agentes negociar en absoluto público una clave

teriales⁴. En la primera de ellas, la del año 1978, ya se incluye el descubrimiento del algoritmo RSA, y con ello parecen fraguar todas las posibilidades disponibles. Sin embargo, en 1984 Taher ElGamal publica⁵ un nuevo sistema de cifrado basado en el problema del logaritmo discreto, que luego, en 1993, inspiró el estándar DSA de firma digital (FIPS 186)⁶ del NIST.

Criptografía de Curvas Elípticas

Contemporánea con la propuesta de ElGamal, llegó la **Criptografía de Curvas Elípticas** que es otra aproximación al concepto de clave pública. Este nuevo planteamiento se construye sobre la estructura algebraica de las curvas elípticas sobre cuerpos finitos, y el uso de estas curvas con fines criptográficos se lo debemos a **Neal Koblitz**⁷ y **Víctor S. Miller**⁸

¹ La operación cortaría al cálculo de logaritmos discretos en una aritmética modular, es la operación de exponenciación que, aun siendo pesada, es fácil de calcular. El cálculo de logaritmos discretos no es tarea fácil, y en algunos casos es realmente difícil. Ver http://en.wikipedia.org/wiki/Discrete_logarithm

² Ver <http://en.wikipedia.org/wiki/Diffie-Hellman> o <http://tools.ietf.org/html/rfc2631>

³ W. Diffie, M. E. Hellman, *New Directions in Cryptography*, IEEE Trans. on Information Theory, Vol. IT-22, Nov. 1976, pp. 644-654. Ver en <http://www-ee.stanford.edu/%7Ehellman/publications/24.pdf>

⁴ M. E. Hellman, *An Overview of Public Key Cryptography*, IEEE Communications Magazine 50th Anniversary Issue: Landmark 10 Papers, May 2002, pp. 42-49 (Invited Paper). disponible en <http://www-ee.stanford.edu/%7Ehellman/publications/73.pdf>

⁵ Taher ElGamal, *A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*, IEEE Transactions on Information Theory, v. IT-31, n. 4, 1985, pp 469-472, o bien en las actas de la conferencia CRYPTO 84, pp10-18, Springer-Verlag.

⁶ En 1996 se publicó una revisión del algoritmo en la publicación FIPS 186-1, y su validez se amplió en el año 2000 como la publicación del documento FIPS 186-2.

⁷ N. Koblitz, *Elliptic curve cryptosystems*, en Mathematics of Computation 48, pp. 203-209 1987.

⁸ V. Miller, *Use of elliptic curves in cryptography*, CRYPTO 85 Proceedings, 1985.

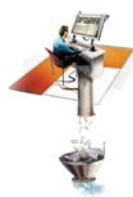
que, independientemente, lo propusieron en 1985. Con esto se cierra la oferta de distintos sistemas de clave pública. Es cierto que se han publicado algunas variantes de cifrado y, sobre todo muchas de firma digital, pero realmente no hay nada esencialmente nuevo en el panorama de la criptografía asimétrica.

De todos los sistemas mencionados, el más popular y conocido es el RSA, pero con el paso de los años, está viendo cómo necesita aumentar rápidamente las longitudes de clave si quiere mantener el mismo nivel de seguridad. En 2002 se consideraba que la longitud mínima de una clave RSA debía ser de 1.024 bits y se estimaba que su seguridad real era equivalente a 80 bits en una clave simétrica. Esos mismos cálculos decían que 2.048 bits RSA equivalen a 112 bits y que 3.072 bits RSA serían la contraparte asimétrica de una clave simétrica de 128 bits. La misma compañía recomienda que las claves RSA de **1.024 bits** se utilicen **hasta el año 2010**, que las de **2.048 bits** puedan aguantar **hasta el año 2030** y, por último, que se utilicen las claves RSA de **3.072 bits** si se persigue tener **seguridad más allá del umbral del año 2030**. Un borrador de una guía sobre la gestión de claves que está desarrollando el NIST va más allá y sugiere que las claves RSA de 15.360 bits tienen una resistencia equivalente a 256 bits de clave simétrica.

Previsiones del NIST

En su documento del pasado mes de agosto⁹, titulado "*SP800-78: Cryptographic Algorithms and Key Sizes for Personal Identity Verification*", el NIST considera que, para el

primer día del año 2011, los cifrados con seguridades equivalentes a 80 bits de cifrado simétrico ya estarán fuera de juego, al menos para la identificación personal, y los sistemas deberán haber migrado a una seguridad equivalente a 112 bits o hacia cotas más elevadas. Para los sistemas asimétricos basados en criptografía de curvas elípticas se especifica un mínimo de 112 bits de resistencia, lo que supone utilizar claves de 224 bits de longitud.



El NIST considera que, para el primer día del año 2011, los cifrados con seguridades equivalentes a 80 bits de cifrado simétrico ya estarán fuera de juego, al menos para la identificación personal, y los sistemas deberán haber migrado a una seguridad equivalente a 112 bits o hacia cotas más elevadas.

Así pues, dado que el crecimiento de la clave en ECC es menor y que las capacidades computacionales en la factorización de números enteros semiprimos, como lo son los del RSA, va creciendo a buen ritmo, quizás sea el momento de pensar en abandonar la criptografía de clave pública de primera generación, y pasar a jugar con curvas elípticas.

El que esto no se haya hecho antes quizás se deba a que la Criptografía de Curvas Elípticas está fuertemente "patentada" y sus propietarios no parecen estar por entregarla al libre uso y disfrute público.

La criptografía de curvas elípticas ha generado un gran número de patentes por parte de sus promotores. Certicom es la empresa canadiense que posee más de 150 patentes que cubren todos los aspectos de la criptografía de curvas elípticas: optimizaciones software, implementaciones hardware, métodos de

uso, protocolos criptográficos, etc. La NSA norteamericana obtuvo en 2003 la licencia de explotación por quince años, de 26 de las patentes esenciales de Certicom, por lo cual pagó 25 millones de dólares, y así poder desarrollar los algoritmos de la denominada *Suite B* de la NSA. La razón de este gasto, no es otro que el de dejar expedito el camino a todas aquellas empresas que desarrollen productos para la NSA, y que vayan a incluir en ellos algo relativo a la ECC.

Certicom está muy dispuesta a presentar batalla ante los tribunales, y muestra de ello es que el 30 de mayo de 2007, denunció¹⁰ a Sony, alegando que el uso que esta compañía hace de la ECC en su Sistema avanzado de Acceso a Contenidos (AACs¹¹), de año 2005, y su otro sistema de Protección Digital de Contenidos en Transmisión (DTCP¹²), de 1998, violarían sus patentes sobre el tema.¹³

Candidatos

Como candidatos a funciones de sentido único, en estos treinta años, se han propuesto **1)** la factorización de números enteros, **2)** la llamada *función de Rabin*, que consiste en calcular cuadrados en aritmética módulo un número compuesto, y que es equivalente a la anterior, **3)** los logaritmos discretos, **4)** el problema de saber si un valor es la suma de algún subconjunto, **5)** la decodificación de códigos

lineales creados al azar, **6)** el problema del viajante, y otros *problemas NP-completos*. Aunque de estos últimos hay muchos ejemplos, sólo los cinco primeros anteriores se han asomado, y algunos anidado, en los pagos de la criptografía.

Está claro que no es fácil diseñar funciones matemáticas de sentido único, pero nuestra experiencia natural está llena de ellas. Quizás un buen ejemplo de ello sea la ecuación de propagación del calor que, ma-

temáticamente hablando, es fácil calcular su evolución si se hace en la dirección normal del tiempo, hacia el futuro, y ello se puede hacer con extremada precisión, incluso numéricamente. Sin embargo, en dirección contraria, hacia el pasado, el objetivo perseguido se convierte en un problema muy mal condicionado, y todos los algoritmos para resolverlo resultan inestables. Desde el punto de vista físico, esta imposibilidad de revertir la *flecha del tiempo*¹⁴ es consecuencia del **Segundo Principio de la Termodinámica**. Por ello, quizás el flujo de calor bien podría ser una prometedora candidata a función de sentido único.¹⁵

Independientemente de esto, cada día está más claro que es preciso innovar en la oferta de sistemas netamente diferentes en Criptografía de Clave Pública porque, de no ser así, el mundo se entregaría a una oferta demasiado cautiva, y un avance imprevisto en las capacidades de factorización, por ejemplo, daría al traste con todas las infraestructuras montadas. ■

JORGE DÁVILA MUÑOZ

Consultor independiente

Director

Laboratorio de Criptografía

LSIIS – Facultad

de Informática – UPM

jdavila@fi.upm.es

⁹ Ver http://csrc.nist.gov/publications/nistpubs/800-78-1/SP-800-78-1_final2.pdf

¹⁰ Ver <http://www.darkbuzz.com/certicom-v-sony-complaint.pdf>

¹¹ El sistema AACs es propiedad de un consorcio administrador de licencias que incluye a las compañías: Disney, Intel, Microsoft, Matsushita (Panasonic), Warner Bros., IBM, Toshiba y Sony.

¹² Las compañías que han desarrollado el DTCP son: Hitachi, Intel, Matsushita, Sony, y Toshiba. Ver <http://www.dtcp.com/>

¹³ En concreto, Certicom alega que se están infringiendo sus patentes 6,563,928 y 6,704,970.

¹⁴ Expresión aparecida en el libro de 1928 *The Nature of the Physical World*, en el que su autor, Arthur S. Eddington (1882-1944) afirma: "*This follows at once if our fundamental contention is admitted that the introduction of randomness is the only thing which cannot be undone. I shall use the phrase "time's arrow" to express this one-way property of time which has no analogue in space.*"

¹⁵ Norbert Hungerbühler, Michael Struwe: *A one-way function from thermodynamics and applications to cryptography*. Elemente der Mathematik. Birkhäuser Basel Ed., Vol 58, Num 2, mayo de 2003 pp. 49-64