



# Treinta años pueden no ser suficientes para los criptosistemas asimétricos

Hace ya más de treinta años, en 1976, Whitfield Diffie y Martin Hellman inventaron un protocolo para el intercambio de claves<sup>1</sup> que supuso la primera publicación, en el seno de la sociedad civil<sup>2</sup>, de la tecnología que hoy conocemos como **criptografía de clave pública**. Ese primigenio algoritmo permitía, ni más ni menos, establecer en el más absoluto secreto una clave simétrica entre dos agentes distantes que sólo pudiesen utilizar para ello un canal de comunicación abierto y no protegido.

El siguiente gran paso no se hizo esperar mucho y un año después, en 1977, unos estudiantes del MIT publicaron un algoritmo que terminó llamándose RSA en honor a sus tres inventores, y que permitía simultáneamente establecer canales confidenciales basados en el uso de claves públicas, y también el establecimiento de una muy importante primitiva criptográfica como es la Firma Digital. Sin embargo, el origen del concepto mismo de la criptografía de clave pública habría que encontrarlo en los trabajos, a finales del siglo XIX, de William S. Jevons<sup>3</sup> que describían las posibles relaciones de las funciones de sentido único con la Criptografía y que, en concreto, discutió la pareja Multiplicación-Factorización como una de esas funciones<sup>4</sup>.

Desde aquellas primeras invenciones, la historia de la criptografía de clave pública ha estado salpicada en algunos puntos por ciertas tensiones entre los Gobiernos y la Industria para limitar unos y favorecer otros el uso civil y comercial de esa tecnología. A pesar de estos anecdóticos enfrentamientos, las tecnologías criptográficas de clave pública han experimentado un crecimiento y una innovación lenta pero continua desde hace treinta años.

Desde la década de los setenta, se han desarrollado cierto número de algoritmos para el cifrado, la firma digital y la negociación de claves, entre otros. Taher ElGamal propuso su sistema de cifrado basado en la dificultad para calcular logaritmos discretos, y su algoritmo está muy relacionado con lo que más tarde sería

**Este año se celebra el 30 aniversario de la aparición de los algoritmos criptográficos asimétricos Diffie-Hellman y RSA, y es interesante preguntarse cuántos nuevos algoritmos de ese tipo les han seguido. También es interesante conocer las medidas que está tomando el NIST para seguir proporcionando un estándar de función hash que sea válido después del abandono en 2011 de la función SHA-1. Los criptosistemas asimétricos y funciones hash son los que dan esencia a la firma digital, y los problemas de ellos, son limitaciones y problemas de ésta.**

el sistema de firma digital DSS (Digital Signature Standard) que incorpora en su seno el DSA (Digital Signature Algorithm) desarrollado por la NSA y el NIST para su uso dentro de la Administración USA. A mediados de los ochenta, Neal Koblitz inventa la criptografía basada en curvas elípticas que es una nueva familia de algoritmos de clave pública.

Debido a los ataques sufridos a partir de mediados de 2005 por el SHA del NIST, éste organismo ha puesto en marcha un esfuerzo público para desarrollar uno o varios algoritmos hash nuevos mediante la convocatoria de una competición pública y planetaria. Este proceder es en

ciones hash y ha aprobado un calendario tentativo para la sustitución de éstas allá por el año 2011.

El pasado día 23 de enero el Registro Federal de los EEUU recoge una comunicación del Departamento de Comercio, en concreto del NIST, donde anuncia y solicita comentarios públicos para el desarrollo de un(os) nuevo(s) algoritmo(s) para la revisión del Secure Hash Standard. Como primer paso, el NIST publica un borrador con los requisitos mínimos aceptables que han de satisfacer los candidatos, las normas a seguir en la presentación de cada candidatura, y los criterios de evaluación que se aplicarán

**El NIST ha anunciado y solicitado comentarios públicos para el desarrollo de un(os) nuevo(s) algoritmo(s) para la revisión del Secure Hash Standard. Como primer paso, ha publicado un borrador con los requisitos mínimos aceptables que deben satisfacer los candidatos, las normas para la presentación de cada candidatura, y los criterios de evaluación. Los comentarios públicos han de recibirse antes del 27 de este mes de abril.**

todo análogo al que se culminó, en el año 2000, con la determinación del algoritmo que pasaría a ser el Advanced Encryption Standard (AES). Hasta la fecha sólo se han celebrado dos reuniones públicas de trabajo para evaluar cuál es el estado de las funciones hash ya aprobadas por el NIST, para discutir las opciones que tienen a corto, medio y largo plazo, y para discutir sobre el estado de la investigación en funciones hash para preparar el lanzamiento del concurso. Siguiendo en esta línea, el NIST ya había publicado su política para el uso de sus actuales fun-

a los algoritmos que se presenten como candidatos. Los comentarios<sup>5</sup> públicos sobre esta relación de mínimos deberán recibirse en el NIST antes del próximo día 27 de este mes de abril.

Los requisitos solicitados más interesantes son que el algoritmo deba ser público y disponible sin *royalties* para todo el mundo, que se pueda desarrollar en un amplio rango de soluciones hardware y software, que proporcione resúmenes de salida de, al menos, 224, 256, 384, y 512 bits y que acepte sin riesgo longitudes de mensaje de

entrada de hasta 2<sup>64</sup> bits. Los algoritmos candidatos serán evaluados comparativamente en cuanto a su seguridad, a su eficiencia computacional, a los requisitos de memoria que tengan, a su adecuación para ser implementados en hardware y software, a su simplicidad, su flexibilidad y a sus condiciones de uso (licencias).

A la vista de estos hechos, está claro que treinta años no han sido suficientes como para que la comunidad criptográfica internacional haya proporcionado un número suficiente de algoritmos asimétricos de clave pública como para cumplir aquella premisa básica del sentido común de "no poner todos los huevos en la misma cesta". Toda la oferta asimétrica actual se basa, de facto, en sólo tres problemas distintos: el del logaritmo discreto, el de la factorización de números compuestos grandes y especiales, y en las propiedades de curvas elípticas y semejantes. La situación en el caso de las funciones hash es un poco más relajada ya que su oferta es más numerosa y sus "ataques con éxito" suelen ser de carácter netamente formal, suelen ser inicialmente inaplicables, y sirven de advertencia para su renovación como es el caso de la iniciativa del NIST respecto a la familia de SHAs.

Si recordamos que todo sistema de firma digital, tal y como lo concebimos hoy en día, es la conjugación de un sistema criptográfico asimétrico y de una función hash, los sistemas de firma digital de los que podemos hacer uso hoy son demasiado pocos, y toda la seguridad informática actual depende de ellos. Es cierto que en el futuro a medio y largo plazo puede llegar a no pasar nada con los sistemas de firma digital, pero nuestros sistemas actuales muy bien podrían ser "gigantes con pies de barro" que un día se derrumben estrepitosamente. La falta de "diversidad" en la oferta algorítmica de la criptografía asimétrica moderna es un problema cuya solución conviene estudiar (financiar) con un poco más de interés por parte de los que construyen su valor añadido sobre esos sistemas de firma digital. ■

**JORGE DÁVILA MURO**  
Consultor independiente  
Director  
Laboratorio de Criptografía  
**LSIIS – Facultad  
de Informática – UPM**  
jdavila@fi.upm.es

<sup>1</sup> Diffie, W., Hellman, M.E.: "New Directions in Cryptography", IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, pp 644-654.

<sup>2</sup> Según parece esta invención habría que reconocérsela a James H. Ellis, Clifford Cocks y Malcom Williamson mientras trabajaban para la GCHQ británica a principios de los setenta (1973). Esta invención no se hizo pública a su tiempo y se mantuvo en secreto hasta 1997 debido a su clasificación de Top-Secret.

<sup>3</sup> Jevons, William Stanley: "The Principles of Science: A Treatise on Logic and Scientific Method", Macmillan & Co. London 1874, 2<sup>nd</sup> ed 1877, 3<sup>rd</sup> ed 1879. Reprinted by Dover Publications, NY, 1958.

<sup>4</sup> Ver Solomon W. Golomb: "On Factoring Jevons' Number", CRYPTOLOGIA 243 (July 1996).

<sup>5</sup> Los comentarios pueden mandarse por correo-e a la dirección [hash-function@nist.gov](mailto:hash-function@nist.gov) con una línea de *subject* igual a "Hash Algorithm Requirements and Evaluation Criteria". Los comentarios recibidos en esta dirección se harán públicos a través del sitio Web <http://www.nist.gov/hash-function>.