



La cosecha criptográfica

Desde que la administración norteamericana optase, a finales de la década de los noventa, por un concurso público internacional para la elección de un nuevo criptosistema que sustituyese al inquebrantable DES, la creación de nuevos algoritmos se ha convertido en algo más público, popular y democrático que en periodos anteriores, más propios de la Guerra Fría. La iniciativa europea que prueba ese nuevo estilo se llamó **NESSIE¹** y su objetivo era obtener, entre los años 2000 y 2003, nuevos algoritmos criptográficos "para el siglo veintiuno".

En febrero del año 2003 se hizo pública la selección final de algoritmos que sobrevivieron de los 42 presentados tres años antes, y con autores provenientes de diez países. Durante los tres años de funcionamiento del proyecto, cierto número de investigadores se dedicó a atacar, con todas sus armas y saber hacer, a los algoritmos escrutados con la esperanza de llegar a comprometer su seguridad y, a la vez, determinar características más pragmáticas como lo son la velocidad, la eficiencia de implementación, etc.

En una primera ronda eliminatoria sólo sobrevivieron 21 algoritmos y en una segunda, y última, la lista se quedó con sólo doce candidatos. Junto a estos doce algoritmos nuevos, publicados para la ocasión, el informe **NESSIE** también recomienda otros cinco algoritmos que, aún no siendo parte de su concurso, los considera dignos de toda confianza.

Aunque esta iniciativa no pretende ser un ejemplo más de los procesos de estandarización al uso, ésta declara abiertamente su vocación de "puente" entre la comunidad científica y el mundo de los usuarios, y se quiere colocar antes de cualquier proceso de estandarización de modo que los resultados de este proyecto ya

Cuando la administración norteamericana decidió sustituir al inquebrantable DES, la creación de nuevos algoritmos dejó de ser algo secreto y pasó a convertirse en algo público y popular. En nuestro escenario europeo, la iniciativa para la obtención de nuevos algoritmos se llamó **NESSIE (New European Schemes for Signatures, Integrity and Encryption) y no hace más de un año, publicó sus conclusiones y la lista con los algoritmos elegidos por ellos; sin embargo, esto por el momento no parece haber afectado al colectivo empresarial de la seguridad informática más concernido en estos temas.**

estarían listos para su integración en el ámbito empresarial de la seguridad.

Los cuatro cifradores simétricos de bloques elegidos son **MISTY1**, **Camellia**, **SHACAL-2** y el **AES**; los dos primeros propuestos por compañías japonesas, y el tercero por una muy conocida compañía francesa. Los tres criptosistemas de clave pública propuestos son: **ACE Encrypt** de **IBM**, **PSEC-KEM** de **NTT Corp.** Japón, y **RSA-KEM** (draft **ISO/IEC 18033-2**).

embargo, es importante resaltar que, de los algoritmos elegidos, ninguno de ellos es un cifrador en flujo, lo cual pone de manifiesto una seria carencia de soluciones en el extremo de las velocidades máximas en lo que a la criptografía en general se refiere.

Prácticamente, todos los algoritmos **NESSIE** pueden utilizarse libremente (excepto **ACE Encrypt**, **ECDSA** y **GPS**) por lo que su informe final

humano que participó en el proyecto **NESSIE**, que procedía de seis instituciones europeas diferentes y un instituto israelí, y sus contactos profesionales a los que solicitó ayuda. Aunque este modo de proceder pueda todavía estar lejos de un sistema público perfecto, ya que ha sido una comunidad muy reducida la que ha llegado a las conclusiones que se han publicado, esta opción es más amplia y fiable que la seguida en el nacimiento del propio **DES**, o en el de cualesquiera de los algoritmos propietarios que están incrustados en multitud de productos en el mercado.

Por este motivo, podemos y debemos sentirnos confiados en que, entre otras cosas, no habrá escasez real de algoritmos criptográficos durante los próximos años siempre y cuando, claro está, excluyamos de nuestra afirmación a la criptografía de alta velocidad en la que sí "tenemos un problema".

Iniciativas como el proyecto **NESSIE** no deberían ser procesos aislados, materializados siempre por las mismas instituciones supranacionales y/o realizadas por los mismos investigadores ya consagrados en sus ámbitos locales. La propuesta y evaluación de primitivas criptográficas debe ser un proceso inherentemente público, con financiaciones serias provenientes de todos los sectores que, directa o indirectamente, usan y necesitan este tipo de tecnologías y, sobre todo, el proceso de propuesta, evaluación y análisis de nuevos algoritmos debe ser continuado. Sólo de aquí puede manar la confianza que es, a final de cuentas, lo que realmente estamos buscando con nuestra siembra inicial. ■

La propuesta y evaluación de primitivas criptográficas debe ser un proceso inherentemente público, con financiaciones serias provenientes de todos los sectores que usan y necesitan este tipo de tecnologías y, sobre todo, el proceso de propuesta, evaluación y análisis de nuevos algoritmos debe ser continuado.

Por su parte, los nueve autenticadores simétricos de mensajes son: **Two-Track-MAC**, **UMAC** de **Intel Corp.**, **CBC-MAC** (**ISO/IEC 9797-1**), **HMAC** (**ISO/IEC 9797-1**), **Whirlpool**, **SHA-256**, **SHA-384** y **SHA-512**.

En cuanto a los algoritmos de firma digital, los elegidos son: **ECDSA** de **Certicom**, **RSA-PSS** de **RSA Labs.**, y **SFLASH** de **Schlumberger**. Por último, ya sólo queda en la lista un único esquema de identificación, denominado **GPS**, que fue propuesto por la **École Normale Supérieure** francesa.

En el estudio de estos diecisiete algoritmos, los miembros de **NESSIE** no encontraron debilidad alguna, e incluso, consideran que algunos de ellos aportan mejoras significativas al arte de diseñar algoritmos criptográficos. Sin

puede considerarse como una buena fuente de soluciones criptográficas para aquellas empresas que piensen renovar sus actuales desarrollos de seguridad. La gran aportación de este proyecto es que pone en escena y en circulación más opciones que trascienden el mero uso del **AES** y del **RSA** como cifrador y sistema de firma digital respectivamente. El hecho de que no todos los algoritmos sean de dominio público, probablemente termine suponiendo un demérito para los algoritmos que han optado por esa vía, y la oferta real sea un poco mas reducida.

En principio, el proceso de evaluación ha sido completamente abierto, los criterios de evaluación convenientemente publicados, y los resultados pueden conseguirse de la correspondiente URL del proyecto. En este esfuerzo evaluador ha trabajado el indeterminado equipo

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

¹ **NESSIE** = New European Schemes for Signatures, Integrity and Encryption 2000-2003. Ver <http://www.cryptoneessie.org> Este proyecto es parte del Information Society Technologies (IST) Program de la Comisión Europea.