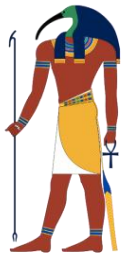

Píldora nº 27: ¿Qué es mejor, la criptografía simétrica o la asimétrica?

Escena 1: Comparativa entre cifra simétrica y cifra asimétrica

Para determinar cuándo es conveniente utilizar una cifra simétrica y cuándo una asimétrica, es menester primero comparar ambos sistemas en los siguientes entornos propios de la seguridad: la gestión de claves, el espacio de claves, la vida de las claves, la autenticación de origen y de destino, el intercambio de clave y la velocidad de la cifra. El análisis de estas características nos permitirá resolver esta cuestión.

Escena 2: La gestión de claves

En un sistema de cifra simétrica con n usuarios, cada usuario deberá memorizar n-1 claves y el sistema tendrá n(n-1)/2 claves. En cambio, la cifra asimétrica requerirá que cada usuario memorice solamente su clave privada y el sistema constará tan sólo de n claves. En este aspecto, resulta claramente más eficiente la cifra asimétrica.

Escena 3: El espacio de claves

Para que un sistema cifra simétrica se considere seguro en 2015, el espacio de claves deberá ser como mínimo de 2^{128}, por ejemplo la clave mínima de 128 bits del AES. No obstante, para una seguridad similar en cifra asimétrica RSA, será necesario utilizar claves de al menos 1.024 bits porque ahora no todos los valores de la clave serán válidos como sí ocurría en una clave simétrica. En este sentido, no son comparables estos dos sistemas de cifra.

Escena 4: La vida de las claves

La duración o vida típica de una clave de sesión en Internet en un sistema de cifra simétrica va desde algunos segundos hasta varios minutos; sin embargo una clave pública y privada de cifra

asimétrica debido a sus características de certificación por autoridades, tiene una duración típica que oscila entre uno y dos años. Nuevamente no son comparables en este aspecto estos sistemas de cifra.

Escena 5: La autenticación de origen y de destino

La cifra simétrica permite la comprobación de la integridad de los mensajes, por ejemplo mediante el uso de funciones MAC, pero no así la autenticación de los interlocutores. En cambio, la cifra asimétrica permite ambas cosas, integridad y autenticación, puesto que realizando en emisión una cifra con la clave privada, en destino sólo se descifrará el criptograma con la clave pública correspondiente. En este escenario, la cifra asimétrica es también más eficiente.

Escena 6: El intercambio de clave

Con los sistemas de cifra simétrica no es posible realizar un intercambio de clave de sesión, a diferencia de la cifra asimétrica. Ello se debe a que en esta última existe una clave pública de un receptor que permite el envío confidencial de esa clave de sesión y que sólo podrá descifrarse con la clave privada del destino. Nuevamente es la cifra asimétrica la que presenta ventajas sobre la simétrica.

Escena 7: La velocidad de cifra y conclusión

Según lo visto hasta ahora, parece que los sistemas de cifra simétrica se encuentran en desventaja pero no es así. La cifra simétrica presenta tasas de cientos de Megabytes por segundo, frente a los cientos de Kilobytes por segundo de la cifra asimétrica, es mil veces más rápida. Con esa velocidad tan baja, no es posible usar sistemas asimétricos para cifrar grandes volúmenes de información.

Resumiendo: es recomendable usar criptografía asimétrica para cifrar números de sólo algunas centenas de bits, como sería el intercambio de una clave simétrica de sesión o bien la firma digital sobre un hash de un documento, y utilizar la criptografía simétrica para cifrar grandes volúmenes de información. Esto es lo que se conoce como cifrado hibrido, que usamos habitualmente y sin darnos cuenta en conexiones seguras de Internet como SSL/TLS.

Madrid, febrero de 2015

Autor del guion: *Jorge Ramió Aguirre*

Dirección Proyecto Thoth: *Jorge Ramió Aguirre, Alfonso Muñoz Muñoz*