Alrededores

Criptografía 30 años después

Jorge Ramió Aguirre

Grado de dificultad

¿Cree Vd. que aumentando de vez en cuando la longitud de las claves usadas, y por ende haciendo más difícil su ataque por fuerza bruta, los sistemas criptográficos que usamos por ejemplo en algunas comunicaciones en Internet son más seguros? ¿La protección de la información mediante el cifrado va por la senda correcta en esta carrera contra los criptoanalistas, al parecer huyendo solamente con esta medida, por lo demás bastante obvia?

El 6 de noviembre de 2006 se cumplen 30 años de la publicación de un invento espectacular: la criptografía de clave pública con el intercambio de clave diseñado por Diffie y Hellman. Lo que llama la atención es que desde entonces no haya sucedido nada que pueda considerarse de igual o similar trascendencia en el mundo de la criptografía; ningún nuevo invento ha removido tanto los cimientos de la criptografía... o al menos eso parece. Tal vez sea la computación y criptografía cuántica las que dentro de algunos años provoquen una revolución análoga a aquella en los cimientos algo estancados de las actuales técnicas criptográficas.

Lo cierto es que desde la revolución que significó para los sistemas de cifra de aquel entonces (año 1976) la propuesta de Whitfield Diffie y Martin Hellman sobre un nuevo sistema bautizado como criptografía de clave pública, a grandes rasgos la fortaleza de los algoritmos en nuestros días sigue basada en gran medida en la longitud de la clave y, por tanto, en la dificultad computacional a la que debe enfrentarse un atacante para obtener una clave secreta mediante un ataque por fuerza bruta, incluso mediante complejos ataques distribuidos en red.

Es decir, el problema de romper la clave o el secreto tiene solución, pero para ello y en términos de media estadística hace falta una capacidad de cálculo impresionante. O lo que

En este artículo aprenderás...

- que la seguridad de los algoritmos que usamos en la actualidad en comunicaciones seguras podría verse seriamente comprometida por el auge de la computación cuántica.
- que, por otra parte, la criptografía cuántica podría entregarnos un sistema de cifra perfecta, con una fortaleza toda prueba.
- que en esta ciencia de la criptografía hay muchos desarrollos e investigaciones que se han mantenido en el más estricto de los secretos durante décadas.

Lo que deberías saber...

- conceptos y principios de criptografía simétrica y asimétrica.
- conceptos básicos sobre fortaleza de los algoritmos, problemas matemáticos tipo P y NP.

es lo mismo, cientos de millones de computadores trabajando simultáneamente en dicha tarea podrían tardar cientos de miles de billones de años en dar con la solución.

Pero no nos engañemos, se trata sólo de una seguridad probabilística y en criptografía aceptamos de buena gana ese desafío probabilístico o bien ni siquiera pensamos en ello. Para romper una clave de cifra simétrica actual, *sólo* hay que adivinar los 128 bits de la clave... es tremendamente difícil como se ha comentado, pero no matemáticamente imposible. Algo similar ocurre con los denominados sistemas de clave pública; por ejemplo, en RSA *sólo* deberíamos factorizar un número compuesto de 1.204 bits en sus dos primos de 512 bits cada uno.

Volviendo al tema que nos preocupa, si hay sospechas de que la longitud de clave es pequeña y por tanto ésta podría ser vulnerable, simplemente aumentamos su tamaño en bits y nos sentimos otra vez seguros. Una huída hacia delante como la citada anteriormente, aumentando cada cuatro o cinco años la longitud de estas claves y aceptando así que otra vez son seguras durante un cierto espacio de tiempo, no es la solución idónea. Es más, podríamos incluso aventurarnos a decir que esta medida tiene escaso valor algorítmico.

Seguir insistiendo en algoritmos mejor elaborados -qué duda cabe- y con excelentes propiedades matemáticas como podría ser el nuevo estándar AES, pero que al final sólo dependen de que el o los atacantes sean capaces de encontrar una clave de n bits, parece ser que no es una solución definitiva y a largo plazo. Hace falta una idea revolucionaria similar a la del intercambio de clave, presentada por Diffie y Hellman hace ahora 30 años, que remueva estos paradigmas de la seguridad informática. Quizás este cambio de filosofía en los métodos de cifra venga de la mano de la computación y la criptografía cuánticas.

Está claro que es muy fácil y cómodo decir que hace años no aparece nada realmente novedoso en criptografía, aunque en estos momentos haya cientos de excelentes criptólogos estudiando y presentando nuevos enfoques y esquemas, sin proponer solución alguna. Alguien lo podrá estar pensando en estos momentos y yo en su caso como lector haría lo mismo, pero evidentemente no soy yo quien deba presentar este tipo de soluciones o nuevas propuestas, sino ese grupo relativamente reducido pero importantísimo de verdaderos gurús de la seguridad informática y en particular de la criptografía, por lo demás conocidos mundialmente.

Lo expuesto en este artículo de alguna manera viene planteándose desde hace muchos años, por lo que no soy ni mucho menos de los primeros en presentar un debate en este sentido. El lector encontrará centenas de miles páginas en Internet sobre vulnerabilidades en los sistemas de cifra, así como computación y criptografía cuánticas. Es más, el libro Los Códigos Secretos de Simon Singh cuya lectura recomiendo, le entregará una amena y completa visión sobre el desarrollo del mundo de la criptografía bajo la perspectiva de un experto, con decenas de anécdotas y citas históricas.

He aprovechado, eso sí, esta fecha del 30 aniversario de la maravillosa e ingeniosa propuesta de Diffie y Hellman, para plantear diversas cuestiones que comienzan a preocupar cada vez más a la Sociedad de la Información. Así, el artículo tiene como objetivo poner esta cuestión de la fortaleza criptográfica sobre la mesa mediante un conjunto de preguntas relacionadas entre sí, e intenta propiciar un análisis razonado sobre esta realidad que se nos avecina.

Cuestiones sobre claves usadas en criptografía simétrica

Si hablamos de criptografía simétrica o de clave secreta, lo que en la década de los 70 y 80 era una longitud de clave muy robusta, del orden de 60 bits, hoy en día sería ridículo pensar utilizar un sistema que trabajase en ese rango de magnitudes. De los 40 bits de clave secreta o simétrica (e.g. DES) que forzaban los navegadores -los comentarios sobre esta reducción del tamaño de la clave me los reservo, son de sobra conocidos- hace tan sólo unos diez años, se ha pasado rápidamente a los 128 bits. Y más, con la llegada del AES no es extraño ver en las propiedades de algunas conexiones seguras mediante plataformas SSL que la clave usada por este algoritmo está ya en los 256 bits.

¿Por qué existía un interés tan manifiesto en reducir el tamaño de las claves de uso público en Internet hasta casi finales de la década de los 90 y, de pronto, esos 40 bits pasan -sin más- a 128? Ese aumento es sencillamente espectacular (recuerde que significa multiplicar 88 veces por 2, es decir, 309.485.009.821.345.068.724.781.056) y resulta difícil creer que simplemente por la ley de Moore u otro parámetro similar de análisis de los avances en tiempos de cómputo se acepte, de buenas ganas y en un tiempo récord, que lo que antes se reducía (recordar aquellos navegadores) de 56 bits a 40 bits para bajar el nivel de seguridad y fortaleza de la cifra en prácticamente todos los países del mundo, ahora pueden ser 128, 196 ó 256. Opino que no hay lógica que resista este análisis.

¿Por qué en los Estados Unidos la criptografía era considerada en aquellos años como material bélico, con todas las limitaciones que ello suponía para su exportación y que por tanto sufrían cientos de países, España incluida, y de un día para otro deja de serlo? Algo más, ¿cómo es posible que algoritmos tan poderosos y robustos como el AES tengan su código abierto en una amplia diversidad de lenguajes disponible en Internet -lo que obviamente no critico; apoyo el

código abierto, es tan sólo un comentario- y hoy cualquier informático o programador pueda incluso modificar ligeramente su estructura, compilarlo y convertirlo en un nuevo ejecutable supuestamente imposible de descifrar, ...y que esto no cree alarma mundial?

El delito informático ha superado en 2006 los ingresos por tráfico de drogas según expertos de los Estados Unidos. Ante esta perspectiva, ¿qué sucedería ahora si la modificación al código comentada en el párrafo anterior la están realizando bandas y organizaciones criminales, en las que se sabe están reclutando expertos en criptografía y redes, dando paso a un nuevo prototipo de hacker que nada tiene que ver con aquel Robin Hood de las redes (la conciencia de la red) sino un verdadero delincuente cuyos logros no puede hacer públicos -he ahí otro gran problema añadido- por el entorno mafioso y delictivo que le rodea?

Ni qué decir lo que esto significa dentro de la lucha contra el terrorismo internacional. ¿Estamos preparados para esto? Para nuestra tranquilidad, supuestamente sí habrían sistemas trabajando para contrarrestar esta amenaza, pero casi nadie sabe cómo son, dónde están, qué hacen ni cómo lo hacen.

Son muchas preguntas. Para cada una de ellas seguro existen varias interpretaciones, con más o menos matices, unas personales, otras incluso rozando la ciencia-ficción, pero no creo sea éste el foro para presentarlas ni discutirlas.

Cuestiones sobre claves usadas en criptografía asimétrica

Si, por el contrario, estamos hablando de claves de cifra asimétrica o los llamados sistemas de clave pública, no es difícil recordar que en las mismas fechas de aquellos gloriosos 40 bits de clave simétrica, se usaban claves asimétricas tipo RSA de 512 bits. Hoy en día, un valor estándar en los certificados digitales X.509 está en los 1.024 bits, también con RSA, pero... ¿cuánto tiempo más usaremos esa longitud de clave y ese sistema de cifra?

Muchas aplicaciones modernas (e.g. PGP) crean por defecto claves de 2.048 bits, precisamente con algoritmos distintos a RSA, basados en la propuesta inicial de Diffie y Hellman, es decir cimentando su fortaleza en el denominado problema del logaritmo discreto, en vez de la dificultad de factorizar un número grande compuesto por los dos primos que usa RSA.

En este caso el atacante que desea romper el secreto del mensaje o la clave privada se enfrenta a uno de los dos problemas matemáticos antes comentados, cuya dificultad computacional es similar.

No obstante, existen otros tipos de ataques. En contraposición a los sistemas de cifra simétricos, al parecer aquí no resulta tan efectivo un ataque distribuido a la clave privada haciendo uso del principio *divide y vencerás* y que hizo sucumbir definitivamente al algoritmo DES -debido eso sí a los 56 bits de su clave, el DES no ha sido criptoanalizado- a finales del año 1979 tras un ataque en red conocido como DES Challenge III, propuesto e impulsado por RSA.

En el caso de RSA, decimos que resulta computacionalmente imposible encontrar la clave privada a partir de los valores públicos de dicha clave: el producto n de los dos primos p y q -conocido como cuerpo de cifra- y la clave pública e propiamente tal, inversa de la clave privada y secreta d, que además es el valor típico 65.537 o número 4 de Fermat. Hay que reconocer que RSA ha resistido todo tipo de ataques en sus casi 30 años de vida, pero sus claves de hace menos de 10 años de 512 bits hoy en día serían fácilmente atacadas mediante la simple factorización de ese cuerpo de cifra.

¿Qué sucedería si en los próximos años alguien encuentra un método más eficaz de factorización distribuida o bien una versión mejorada del ataque a la clave privada basado en la conocida paradoja del cumpleaños, que ha servido por ejemplo para dejar las funciones hash MD5, SHA-1 y sus familias heridas de muerte desde septiembre de 2004, y que sin embargo eran y siguen siendo ampliamente utilizadas entre otros en los certificados digitales X.509?

Peor aún, ¿y si quienes estuviesen detrás de este intento no son científicos con un interés loable y noble como nos consta por sus artículos y ponencias en congresos,

Librería

- New directions in cryptography. Whitfield Diffie, Martin Hellman, Noviembre 1976.
  http://www.cs.purdue.edu/homes/ninghui/courses/Fall04/lectures/diffie-hellman.pdf
- Algunos criptólogos importantes
  http://en.wikipedia.org/wiki/Cryptographer
- Los códigos secretos. Simon Singh, Editorial Debate S.A., 2000
  http://www.simonsingh.net/Code_Book_Download.html
- Libro electrónico de Seguridad Informática y Criptografía v4.1. Jorge Ramió
  http://www.criptored.upm.es/guiateoria/gt_m001a.htm
- DES Challenge III - RSA Laboratories
  http://www.rsasecurity.com/rsalabs/node.asp?id=2108
- La verdadera historia de RSA
  http://livinginternet.com/i/is_crypt_pkc_inv.htm
- Computación y criptografía cuánticas
  http://en.wikipedia.org/wiki/Quantum_computer
  http://en.wikipedia.org/wiki/Quantum_cryptography
  http://www.criptored.upm.es/guiateoria/gt_m471a.htm

sino delincuentes, organizaciones criminales? ¿No sería esto un motivo de real preocupación para los negocios en red y la banca por Internet? ¿Se imagina lo que sucedería si las claves privadas de bancos, organismo de gobierno, agencias de investigación, etc. quedasen en manos de criminales?

Como seguramente sabrá, tras el éxito del libro *El Código da Vinci* existen decenas de libros que se ocupan de esta temática, ahora que está tan de moda unir la intriga con la criptografía y los códigos secretos. Lo inquietante es que todo esto ya no es sólo la imaginación novelesca de un conjunto de autores; es muy posible que se convierta en una de las preocupaciones más importantes de organismos y naciones en los próximos años o bien, y en el peor de los casos, que ya esté ocurriendo.

Cuando la investigación se convierte en alto secreto

El sistema RSA se ha convertido en un estándar de facto en las comunicaciones seguras en Internet, pero poca gente conoce la verdadera historia de este algoritmo. Es verdad que Rivest, Shamir y Adleman dan con la piedra angular de la criptografía de clave pública en febrero de 1978 (15 meses después del invento revolucionario de Diffie y Hellman) patentando así RSA que lleva sus iniciales, pero este nuevo sistema para cifrar información fue descubierto muchos años antes.

En 1969 el GCHQ Government Communications Headquartes en Gran Bretaña, preocupado por la gran dificultad que entrañaba intercambiar claves de cifra simétrica, comienza a trabajar en esa misma idea y en 1973 (cinco años antes) el matemático Clifford Cocks llegará a idéntica conclusión que los creadores de RSA.

Desgraciadamente para él y su grupo de investigadores, este trabajo fue considerado como alto secreto por el gobierno británico y no pudo hacerse público ni menos patentarlo. En 1977, casi 25 años después, el GCHQ años decide desclasificar esta información y hacerla de dominio público. Aunque de poco sirva, este hecho al menos permite que hoy se les pueda reconocer a estos investigadores el trabajo realizado.

Algo similar sucedió con los avances en el criptoanálisis a la máquina Enigma durante la Segunda Guerra Mundial, especialmente gracias a científicos polacos (entre ellos Marian Rejewski) y británicos (por ejemplo Alan Turing) que vieron como, acabada la guerra, no pudieron recibir el reconocimiento mundial por sus extraordinarias proezas en el descifrado de ese monstruo de las cifras del ejército nazi y que permitió, no obstante, salvar miles de vidas humanas, por la sencilla razón de que todo ese maravilloso trabajo se mantuvo por decenas de años como un secreto de estado.

Durante muchos años la NSA, National Security Agency, es el organismo que contrata a más matemáticos a nivel mundial. Tras los atentados del 11-S ha crecido de forma espectacular la contratación de expertos en criptografía en los Estados Unidos. ¿Cuántos desarrollos similares se estarán realizando actualmente de forma totalmente secreta?

Computación y criptografía cuánticas

Retomando la idea del inicio de este artículo, tal vez la próxima revolución en los sistemas de cifra venga con la criptografía cuántica y, más aún, con la creación de computadores y sistemas cuánticos prácticos. No entraré en especificaciones técnicas; el lector encontrará miles de páginas en Internet que tratan la computación y criptografía cuánticas en profundidad, tanto en inglés como en español.

Un computador cuántico puede resolver esos problemas que antes decíamos eran intratables (la factorización de un número compuesto y el problema del logaritmo discreto) en un tiempo mínimo. De hecho ya existen ejemplos usando tecnologías como la resonancia magnética nuclear, dispositivos superconductores de interferencia cuántica conocidos como SQUIDs, iones suspendidos en vacío, imanes moleculares, etc.

En 1994 Peter Schor propone un algoritmo que sería capaz de factorizar el cuerpo de cifra RSA y de esta forma deducir la clave privada, en un tiempo muy pequeño conocido matemáticamente como polinómico, lo que fue prácticamente confirmado por un grupo de investigación de IBM en el año 2001 para un número de 4 bits y hoy se habla de algoritmos más eficientes con excelentes resultados con números por encima de 10 bits.

¿Qué nos espera en los próximos años en esta carrera? Si esto llegara a ser medianamente factible en los próximos 10 ó 20 años para ciertos organismos o estados, todos los sistemas de cifra actuales quedarían obsoletos. ¿Sería el fin de la privacidad? ¿Seguiremos confiando en las nuevas tecnologías? ¿Qué sucedería con los negocios y la banca en Internet?

Por su parte, la criptografía cuántica parte en el año 1984 cuando Charles Bennet y Gilles Brassard proponen un esquema de cifrado cuántico. Según los estudios realizados, la cifra mediante criptografía cuántica permitiría que lo que hasta ahora aceptamos como fortaleza de los algoritmos, esto es una seguridad computacionalmente intratable, se vuelva en seguridad matemática de forma que cualquier interceptación del mensaje o clave intercambiada podría detectarse.

La forma condicional en la afirmación anterior estriba en que ciertas propiedades de la mecánica cuántica como la imposibilidad de clonación del haz láser podría estar en entredicho, aunque éste es un tema que escapa del objetivo del artículo. Son simples obstáculos en el camino de algo que estamos comenzando a aprender cómo funciona.

En sus poco más de 20 años de historia, la criptografía cuántica ha tenido un avance teórico muy lento, aunque sí se han dado pasos importantes en las implementaciones prácticas, y es así como los primeros productos comerciales de intercambio de clave hacen su aparición en el año 2002.

Si la computación y criptografía cuánticas, tal y como se sospecha, llegan a convertirse en una alternativa viable a los actuales sistemas informáticos y de cifra, tendríamos por un lado una potencial amenaza en su altísimo poder de cómputo pero, por otro lado, la posibilidad de diseñar un sistema criptográfico con una seguridad perfecta y no tendría sentido entonces seguir especulando con nuevos algoritmos para la protección de datos. La seguridad sería total.

Nuevamente nos encontramos ante la disyuntiva de que este sistema, ahora sí infalible, también estaría al alcance de criminales. Y para la seguridad mundial esto sería gravísimo. ¿Permitirán los estados que todo el mundo pueda utilizar esta nueva tecnología si llega a ser factible?

Conclusiones

Para las personas puede que 30 ó 50 años signifiquen mucho, pero reflexionemos sobre estos logros y avances tecnológicos e intentemos contestar a las siguientes preguntas. ¿Pueden los países, instituciones, organismos y empresas vivir con esta incertidumbre en las herramientas y sistemas que controlarán la seguridad de sus datos e información? ¿Podemos sospechar qué novedades criptográficas nos esperan en el año 2036, por poner un horizonte de sólo 30 años, lo mismo que ha durado la criptografía de clave pública desde Diffie y Hellman?

¿Habrá en estos momentos, en algún lugar del mundo, estudios secretos con computadores y esquemas cuánticos que al ser estratégicos y vitales para algunos países y organismos, su conocimiento esté vedado para el resto la comunidad científica y, más aún, para la sociedad en general?

Aunque nos cueste reconocerlo, es meridianamente claro que esto debería estar sucediendo ahora mismo, incluso tal vez desde hace algunos años. La criptografía por su naturaleza siempre ha tenido una vertiente de investigación secreta. Recuerde el caso del invento de la criptografía de clave pública de Clifford Cocks antes comentado y que luego sí patentan Rivest, Shamir y Adleman, convirtiéndolo en un estándar mundial y en un espectacular negocio, o bien el trabajo anónimo de Rejewski y luego de los criptoanalistas de Bletchley Park con Turing a la cabeza rompiendo la máquina Enigma, y quizás tantos otros logros que no se han hecho públicos.

¿Por qué en este siglo XXI el ser humano se iba a comportar de forma distinta? Si algo ha cambiado es que cada día somos más desconfiados y paranoicos porque están sucediendo cosas hasta ahora inimaginables: los atentados en Nueva York, Londres y Madrid, el reciente intento en el aeropuerto de Londres de explotar varios aviones en pleno vuelo, el robo y fraude en Internet, la pornografía infantil, redes de pedófilos, el proyecto Echelon y sus redes de escucha, etc., son sólo algunos tristes botones de muestra de nuestra sociedad.

Porque en este tema tan delicado de la privacidad de los datos persolanes de los ciudadanos y de sus comunicaciones, no sólo hay que mirar con preocupación al ambiente delictivo. En aras de una mayor seguridad, también podríamos aceptar sin darnos cuenta un mundo Orwelliano.

En fin, demasiadas preguntas que tal vez sólo algunos de los grandes expertos, aquellos gurús a los que he hecho mención en la introducción y que puede ver en el enlace de la sección *Librería* de este artículo, podrían tener una respuesta... y si la tienen quizás nunca lleguemos a conocerla. ●

Acerca del Autor

Jorge Ramió es Dr. Ingeniero de Telecomunicación Diplomado por la Universidad Politécnica de Madrid, España 1982. Profesor titular del Departamento de Lenguajes, Proyectos y Sistemas Informáticos de la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid, desde 1994 es coordinador de la asignatura Seguridad Informática en dicha Escuela.

Autor del libro electrónico de Seguridad Informática y Criptografía de libre distribución, con decenas de miles de descargas en Internet. La quinta edición con 1.029 diapositivas de fecha 1 de marzo de 2005 ha sido traducida recientemente al inglés. La sexta y última edición del libro, versión 4.1 de 1 de marzo de 2006, contiene 1.106 diapositivas.

Participa en comités de organización y de programa en diversos congresos relacionados con la seguridad informática y enseñanza universitaria, entre ellos el congreso internacional bienal CIBSI del que es su creador y del que se han celebrado tres ediciones.

Es miembro del Comité de Revisores de la Revista IEEE América Latina, IEEE Región 9 y del Subcomité de Seguridad de T.I. (SC 27) del Comité Técnico de Normalización de Tecnología de la Información (CTN 71) de AENOR.

Participa como profesor invitado en Doctorado, Máster y Diplomado en España, Argentina y Chile.

Ha impartido diversos cursos y conferencias sobre criptografía y seguridad informática en Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, España, México, Panamá, Perú, República Dominicana, Uruguay y Venezuela.

Creador y coordinador de la Red Temática Iberoamericana de Criptografía y Seguridad de la Información CriptoRed y director de la Cátedra UPM Applus+ de Seguridad y Desarrollo de la Sociedad de la Información.

Página Web personal: *http://www.lpsi.eui.upm.es/~jramio/*