Mayo 18, 2010

Sistemas criptográficos RSA: seguros mientras no se demuestre lo contrario

Categoría: Sin categoría — dccuchile - 6:03 pm

Por Pablo Barceló, profesor del Depto. de Ciencias de la Computación, FCFM, de la Universidad de Chile

En mi penúltima columna hablé sobre Michael Rabin y su contribución a los algoritmos probabilistas. Aquellos que nos aseguran lo correcto de su resultado sólo con una probabilidad. Pero resulta que esa probabilidad es tan alta que la posibilidad de error es prácticamente inexistente (o en palabras de Rabin: "La probabilidad de error es menor que la probabilidad de que ninguno de nosotros esté despierto y estemos todos soñando lo que está sucediendo"). Sorprendentemente **estos algoritmos no sólo son confiables, sino que también utilizados a diario en todo el mundo en aplicaciones tan críticas como de intercambio de información confidencial.** Un tema que se ha vuelto clave en la última década, principalmente por el aumento acelerado de los traspasos electrónicos de datos, en especial de aquellos comerciales o financieros que requieren absoluta privacidad.

El área que estudia el intercambio seguro de información se llama Criptografía, que en su estudio realiza el cruce de técnicas matemáticas, computacionales e ingenieriles. Obviamente las aplicaciones bélicas son consumidoras habituales de técnicas criptográficas (mal que mal, en toda guerra es necesario diseminar la información entre batallones sin que el adversario conozca el contenido del mensaje). Sin embargo, hoy en día la Criptografía tiene innumerables otras aplicaciones en áreas como financiera, telecomunicaciones, etc. Por cierto, el advenimiento de la computación ha tenido mucho que ver con esto, permitiendo que haya aplicaciones criptográficas más complejas y robustas.

La Criptografía se define como el proceso de ocultar información. Pero no tomemos esta definición en su connotación negativa. Pensémosla en términos de aquellos procesos donde ocultar la información es necesario para mantener la privacidad o la seguridad de ésta. Por ejemplo, que un administrador de cuentas de correo electrónico mantenga los *passwords* de los usuarios en secreto. Conceptualmente el problema que la Criptografía desea resolver es el siguiente: Alicia (A) desea enviar un mensaje secreto a Bernardo (B), ¿Cómo hacer para que el copuchento de Carlos (C) no se entere del contenido del mensaje?

La Criptografía se divide en dos procesos: la "encriptación" del mensaje, que se refiere a convertir un mensaje ordinario en uno "secreto", ininteligible para aquellos a los que se les desea ocultar la información. Y la 'decriptación' que es el proceso inverso, es decir, convertir el mensaje cifrado en uno ordinario. Para lograr 'encriptar' y 'decriptar' mensajes es necesario tener una clave (o llave). Dependiendo del tipo de llave utilizada es posible dividir los sistemas criptográficos en dos tipos: los de llave privada y los de llave pública.

Los sistemas de llave privada (o simétricos) son aquellos en los que sólo el emisor (A) y el receptor (B) del mensaje conocen la llave. El problema que presentan estos sistemas es que la llave misma también debe intercambiarse entre (A) y (B). Y si el atacante (C) logra hacerse de la llave en ese intercambio, entonces podrá descifrar todos los mensajes de ahí en adelante. La solución a este problema fue propuesta por Difie y Hellman en 1976. Ellos diseñaron el primer sistema conocido del tipo llave pública. Tales sistemas manejan dos llaves, una para 'encriptar' el mensaje, que es pública, y otra para 'decriptarlo', que es privada. El sistema funciona así: si (A) quiere enviar un mensaje a (B), entonces (B) genera dos llaves, la pública y la privada y le envía la llave pública a (A). (A) codifica su mensaje con esta llave y se lo envía codificado a (B). Para decodificar el mensaje es necesario tener la llave privada. Y (B) es el dueño de esa llave ¡la que además nunca ha intercambiado! Concluimos entonces que (B) puede decodificar el mensaje y que nadie más podrá hacerlo. La mejor analogía de un sistema de llave pública es la de un buzón de correos: cualquiera puede dejar una carta en él, pero sólo el cartero tiene la llave para abrirlo y sacar las cartas.

El sistema criptográfico por lejos más utilizado en la actualidad es uno de llave pública. Su nombre, RSA, proviene de los apellidos de sus creadores R. Rivest, A. Shamir, y L. Adleman, quienes por entonces estudiaban en MIT. (Como dato curioso, los autores no aparecen en orden alfabético en el nombre del sistema porque las contribuciones de Adleman fueron consideradas menos relevantes que las de Rivest y Shamir. Paradojalmente Adleman más tarde se convirtió en el más famoso de los tres por sus contribuciones en un área diferente: el estudio de la diseminación de los virus, en particular, del VIH).

Archivos

Otros Blogueros

En términos técnicos, lo que hace el sistema RSA es generar como llave pública cierto número *e* que se obtiene de multiplicar dos números *p* y *q* primos enormemente grandes generados al azar (recuerde que un número es primo sólo si puede ser dividido por 1 o por el mismo; por ejemplo, 3,5,7,11 son números primos). Para esto el algoritmo debe ser capaz de reconocer rápidamente si un número es primo o no (ya que si no lo es el código podría ser quebrado). Es aquí precisamente donde se ocupan los algoritmos probabilistas: Rabin construyó un algoritmo probabilista que determina con inmensa eficiencia si un número es primo. (Existen algoritmos no probabilistas que también resuelven este problema, pero todos son considerados más difíciles de implementar que el de Rabin). Por otro lado, la llave privada "d" puede ser fácilmente obtenida desde los primos *p* y *q*.

Algo muy notable del código RSA es que es matemáticamente posible deducir la llave privada *d* desde la pública *e*. Es decir, es "teóricamente" factible para un atacante decodificar el mensaje. Sin embargo, eso implicaría tal cantidad de recursos computacionales (¡miles o millones de años de uso de los computadores más poderosos!) que el problema se vuelve "prácticamente" imposible. Esto puede verse así: ya dijimos que la llave pública *e* puede obtenerse desde *p* y *q*. Pero note que *p* y *q* mismos han sido mantenidos en secreto. Sin embargo, para conseguir *d* bastaría obtener desde *e* los primos *p* y *q* por medio de algún tipo de "factorización prima". Este problema puede ser solucionado mediante una búsqueda exhaustiva de todos los factores primos de un número. Pero como los números involucrados son muy grandes, tal búsqueda exhaustiva se vuelve imposible; en otras palabras, no se conoce un algoritmo eficiente que resuelva este problema. Y note bien lo que decimos: no se "conoce" algoritmo eficiente, ¡porque nadie ha podido demostrar que no exista! Si es que llegara a existir, todos nuestros sistemas criptográficos se verían (al menos) en aprietos.

En resumen, en los sistemas criptográficos RSA para 'encriptar' utilizamos un algoritmo probabilista (que sólo entrega resultados correctos con una probabilidad). Y para asegurarnos que nuestros atacantes no puedan 'decriptar' nuestros mensajes usamos una suposición matemática que nadie ha podido demostrar (que no es posible encontrar eficientemente la factorización prima de un número). ¡El reino de la incertidumbre matemáticamente controlada!

Para terminar, es interesante comentar que un sistema muy parecido al RSA ya había sido creado en secreto por un agente del gobierno británico, Clifford Cocks, en 1973. Sin embargo, la agencia de seguridad en la que trabajaba lo consideró no factible de ser implementado y quedó en el olvido. Tal sistema sólo pudo ser revelado al público, por razones de seguridad de estado, en 1998, cuando ya el sistema RSA era ampliamente utilizado en aplicaciones criptográficas en todo el mundo.

permalink trackback
Comentarios (0)
« Older Posts