SUMA 46
Junio 2004, pp. 27-30

Criptografía

La aparición de Internet, el correo electrónico, el comercio on-line, etc, han obligado al hombre actual a desarrollar rápidamente sistemas de criptografía cada vez más sofisticados y a la vez más seguros. Este texto trata de explicar el método de clave pública, que es en el que se basan los sistemas de criptografía más difundidos en Internet. Al final se incluye un anexo con resultados matemáticos utilizados y algunas direcciones web y títulos de libros para poder ampliar información sobre el tema.

The Internet, e-mail, on-line trade and so on have made man quickly develop more and more sophisticated and safe cryptography systems. This text aims at interpreting the public key method, the one most Internet-spread cryptography systems are based on. An appendix with used mathematic results is included at the end, along with some websites and book titles that will allow for further information on the issue.

Criptografía viene de la concatenación de dos palabras griegas *kryptós*, que signica *escondido* y *graphein* que quiere decir *escribir*. Esconder la escritura, el arte de enmascarar los mensajes con signos convencionales, que sólo cobran sentido a la luz de una clave secreta. Desde hace mucho tiempo, el hombre ha utilizado su ingenio para mantener la confidencialidad de sus comunicaciones. Hay que remontarse a la época de los egipcios, donde se encuentran los primeros signos de este arte. Existen pruebas palpables en tablas cuneiformes, en papiros, en textos militares y de espías, incluso en artículos del Kamasutra (manual erótico hindú del Vatsyayama), pero desde entonces hasta ahora las cosas han evolucionado mucho, sobre todo por la aparición de los sistemas informáticos. La aparición de Internet, el correo electrónico, el comercio on-line, las transacciones bancarias a través de la red... han obligado al hombre actual a desarrollar rápidamente sistemas de criptografía cada vez más sosticados y a la vez más *seguros*.

No vamos a hacer un recorrido histórico de los distintos métodos de cifrar mensajes, sino que trataremos de explicar las bases de los métodos actuales, que aunque sean más complejos que los clásicos, tienen más importancia. Además, por suerte, no hay que conocer las ideas que nuestros antepasados tenían sobre criptografía para comprender los métodos de cifrado vigentes. Concretamente trataremos de explicar el método de clave pública, que es en el que se basan los sistemas de criptografía más difundidos en Internet.

En todos los sistemas de cifrado debe de comunicarse una clave entre el emisor y el receptor para que éste último entienda el mensaje del emisor, de tal forma que quien no tenga esa clave no lo pueda entender. El problema es encontrar un canal seguro para transmitir dicha clave. Por ejemplo, si queremos cifrar el mensaje 'HOLA' con el método de transposición utilizado por Julio Cesar que consistía en sustituir cada letra del mensaje por la situada 3 lugares más adelante resulta 'KRÑD'. Lo que tiene que hacer el receptor al ver este mensaje es la operación inversa, es decir, sustituir cada letra por la situada 3 lugares más atrás. La clave es la forma con que se cifra y el emisor debe comunicársela al receptor para que este pueda aplicar la inversa y leer el mensaje.

En el ejemplo anterior bastaría con una comunicación oral y privada para comunicar la clave, pero esto no nos vale para garantizar la seguridad en la red, porque si todos quisiéramos utilizar nuestra tarjeta de crédito por Internet tendríamos que cifrar su número para transmitirlo y sólo el banco tendría que saber cada una de nuestras claves (todas ellas diferentes y desconocidas para los demás usuarios) para descifrarlo. Surgen entonces tres problemas:

Miguel Ángel Jonquera García
IES Villa de Santiago. Santiago de la Espada (Jaén).

– Hay que comunicar al banco la clave de cifrado, sin que nadie más lo sepa.

– Cada uno de nosotros tendría que tener un método diferente de cifrado y el banco tendría que tener una clave por cada uno de nosotros, lo que es poco viable.

– El método de cifrado debe ser seguro, de manera que si alguien intercepta nuestro número de cuenta cifrado, no lo pueda descifrar. Los métodos clásicos distan mucho, en la actualidad, de ser infalibles y en la mayoría de los casos basta hacer unos sencillos cálculos para averiguar los códigos secretos que generamos.

El método de clave pública

Intentando resolver estos problemas surge el *método de clave pública*, ideado en 1975 por los matemáticos Whitefield Diffic y Martin Hellmann de Estados Unidos.

La cuestión general del método consiste en generar una clave, llamada pública y otra denominada privada, para descodificarlo, de tal manera que conociendo la primera no se pueda acceder a la segunda. Las claves públicas se difunden lo máximo posible en la red, mientras que sólo los destinatarios conocen las privadas. De esta forma, el primer problema desaparece radicalmente.

Ejemplo:
Pongamos el mismo banco antes mencionado, que distribuye entre sus clientes su clave pública con la que enmascarar el número de la tarjeta de crédito y que sólo el banco puede descifrar una vez cifrado, utilizando la clave privada. Notar que un cliente no puede averiguar el número de otro cliente pues no conoce la clave privada, aunque consiga interceptar el envío del número de cuenta cifrado. Es el banco el que nos dice la clave con la que cifrar nuestro número y además es la misma para todos.

De esta forma, con una sola clave, que además es pública y no hay que preocuparse de esconderla si no de todo lo contrario, solucionamos los problemas antes comentados. Lo único que tenemos que hacer es mantener oculta la clave privada, pero esto es fácil porque no hay que comunicársela a nadie.

Una vez llegados a este punto, parece que la idea está bastante clara, pero se ha hablado de una clave pública que cifra mensajes que sólo pueden ser descifrados con su correspondiente clave privada y que sin ella, nadie podría, aun conociendo la forma en que está cifrado el mensaje. Pero, ¿existe realmente esa clave pública?, si es cierto, ¿cómo se obtiene? y ¿cómo es posible que sin la clave privada nadie pueda descifrar un mensaje que se sabe de qué manera está cifrado?

Todas estas preguntas las resolvieron en 1977, tres matemáticos, Ron Rivest, Adi Shamir y Leonard Adlerman con el cifrario RSA, que lleva sus iniciales. Para comprender el método hay que recordar algo sobre números primos.

Números Primos
Desde los cursos de Primaria los alumnos aprenden lo que es un número primo y un método para calcular los primeros, denominado la criba de Eratóstenes, que aunque lento, su funcionamiento es muy evidente. Otro problema asociado es la descomposición de un número en factores primos, donde vamos probando con los distintos números primos obtenidos por el procedimiento anterior. Con un poco de práctica, uno se da cuenta de que descomponer un número relativamente grande resulta muy costoso y en algunos casos casi imposible. Sin embargo, el problema inverso consistente en dados los factores primos hallar el número, es muy sencillo, basta con multiplicar todos los factores. En resumen, generar números primos requiere mucho tiempo, descomponer números en factores primos aún más, pero construir un número a partir de sus factores primos es casi inmediato.

Después de más de dos mil años de esfuerzos de grandes matemáticos, la situación al respecto es la siguiente:

– Existen algoritmos muy rápidos para generar números primos grandes, utilizando una computadora.

– No se conocen algoritmos rápidos para descomponer un número en factores primos, ni utilizando las últimas tecnologías informáticas. Descomponer un número suficientemente grande con el mejor algoritmo conocido implementado en la más potente computadora podría tardar ¡billones de años! Tras muchos esfuerzos no se ha avanzado prácticamente nada en este tema, lo cual resulta muy útil a la criptografía.

Cifrado y Descifrado con el método RSA

Ya estamos preparados para comprender el método RSA, utilizando para ello la formalización del ejemplo del banco. Evidentemente el cifrado que vamos a describir no es real ya que sería con números muchísimo más grandes, pero así se comprenderá mejor, aunque los cálculos pueden resultar un tanto tediosos al hacerlos a mano.

1. El banco genera dos números primos muy grandes p y q y calcula su producto $n = p \cdot q$. También elige un número $e < n$ de manera que mcd(e, $\phi(n)$) = 1, es decir, e es primo con $\phi(n)$= = $(p - 1) \cdot (q - 1)$. La clave pública sería: (e, n). Ahora hay que encontrar otro número d que sea el inverso de e módulo $\phi(n)$, es decir, $d \cdot e \equiv 1(\phi(n))$, que es fácil utilizando el *algoritmo de Euclides* y conociendo p y q. La clave privada sería: (d, n).

Ejemplo:
$p = 43$, $q = 59$, $n = 2537$, $e = 13$ que es primo con $\phi(n) = 2436$ y $d = 937$. Siendo la clave pública (13, 2537) y la clave privada (937, 2537).

Resumiendo:
p y q primos $\rightarrow$ $n = p \cdot q$ y e tal que mcd$(e, \phi(n)) = 1 \Rightarrow (e, n)$ clave pública, que se utiliza para cifrar de la siguiente forma

$$P \rightarrow C \equiv P^e\,(n)$$

Para descifrar obtenemos d tal que $d \cdot e \equiv 1(\phi(n))$, siendo la clave privada (d, n) y se utiliza para descifrar C de la forma

$$C \rightarrow P \equiv C^d\,(n)$$

La explicación del proceso de descifrado sería:

$$C^d \equiv \left(P^e\right)^d \equiv P^{ed}\,(n)$$

y como $d \cdot e \equiv 1(\phi(n))$,

$$C^d \equiv P^{1+x\phi(n)}(n) \equiv P \bullet P^{x\phi(n)} \equiv P\,(n)$$

donde en la última equivalencia de la congruencia hemos utilizado que

$$P^{\phi(n)} \equiv 1(n)$$

Este resultado de teoría de números se encuentra demostrado en el anexo del presente artículo, donde se suponen unos conocimientos mínimos de congruencias y anillos.

Lo único que es un poco más laborioso es el cálculo de d, pero existen programas matemáticos que calculan el inverso de un número dado, módulo $\phi(n)$. El *algoritmo de Euclides* nos ayuda ya que lo único que tenemos que hacer son unas divisiones. Empezamos dividiendo $\phi(n)$ entre e, luego el divisor entre el resto resultante y así hasta que el resto sea 1.

En nuestro caso quedaría, utilizando la notación

Dividendo = divisor x cociente + resto;

$$2436 = 13 \cdot 187 + 5$$
$$13 = 5 \cdot 2 + 3$$
$$5 = 3 \cdot 1 + 2$$
$$3 = 2 \cdot 1 + 1$$

y ahora despejando el 1 y volviendo hacia atrás desde la última igualdad,

$$1 = 3 - 2 \cdot 1$$
$$1 = 3 - (5 - 3 \cdot 1) = 2 \cdot 3 - 5$$
$$1 = 2(13 - 5 \cdot 2) - 5 = 2 \cdot 13 - 5 \cdot 5$$
$$1 = 2 \cdot 13 - 5(2436 - 13 \cdot 187)$$
$$1 = -5 \cdot 2436 + 13(2 + 187 \cdot 5)$$
$$1 = -5 \cdot 2436 + 13 \cdot 937$$

Por lo que deducimos que el inverso de $e = 13$ módulo $\phi(n)$ es $d = 937$.

2. Ahora ya tenemos las claves para poder cifrar y descifrar. Supongamos que el número de nuestra tarjeta de crédito es 1520 (para simplicar).

Cifrado:
$1520 \rightarrow 1520^{13} \equiv 95(2537) \rightarrow 0095$ para completar a 4 cifras.

Descifrado:
$0095 \rightarrow 0095^{937} \equiv 1520(2537)$
El resultado del cifrado 95 se puede obtener fácilmente utilizando una calculadora con la tecla 'MOD'.

Noten que la facilidad del descrifrado es gracias a que conocemos $d = 937$ y que su cálculo ha sido posible al conocer p, q y el *algoritmo de Euclides* . Esto, como se ha razonado antes, hubiera sido imposible conociendo sólo n y no su descomposición factorial.

Noten también que en un caso real el número de cuenta tiene 20 dígitos y para cifrarlo se cifrarían de 4 en 4 sus cifras (por ejemplo) de la forma descrita.

En el caso de que quisiéramos cifrar el texto de un correo electrónico, convertiríamos los caracteres en sus equivalentes numéricos según un código elegido (por ejemplo código ASCILL o (A = 00, B = 01...)).

Fuera de engaños
Para terminar intentaremos resolver la siguiente pregunta. ¿Está seguro el receptor de que el mensaje codificado haya sido enviado efectívamente por el cliente X y no por alguien que se hace pasar por él?

La respuesta a estas preguntas es la siguiente:

El cliente X cifra su firma, utilizando su clave privada y, después codifica el mensaje con la clave pública del destinatario. El receptor descifra el mensaje con su clave privada y después con la pública de X. De esta manera el receptor se asegura que la firma es la de X.

Recomendaciones

Actualmente existen muchos programas en Internet que cifran mensajes, aunque recomiendo el PGP, que se puede descargar junto con mucha información en

http://glub.ehu.es/seguridad/pgpintro.html

Otras direcciones de interés son:

http://www.kirptopolis.com

http://www.pgp.com

http://www.gvsu.edu/mathstat/enigma/enigma.htm

aunque si se busca en cualquier buscador la palabra criptografía o RSA saldrán muchas direcciones relacionadas con el tema y además hay bastantes en español.

Como libros, destacaría *Códigos Secretos* de Andrea Sgarro, Editorial Pirámide, que describe cronológicamente la criptografía sin entrar en muchos tecnicismos.

También podría ser interesante *Introducción a la criptografía* de Caballero Pino, editorial Ra-ma.

Por último, puede ser que alguno de los lectores se pregunte si éste método es infalible o incluso tengan la tentación de intentar romperlo. Muchas de las técnicas que se han considerado infalibles a lo largo de la Historia han sido derrotadas por la habilidad de criptoanalistas. Les dejo con las palabras de Edgar Allan Poe,

> *es dudoso que el género humano logre crear un enigma que el mismo ingenio humano no resuelva.*

Anexo

Notación:

$$\overline{a},\overline{b}\in\mathbb{Z}/n\mathbb{Z}\wedge\overline{a}=\overline{b}\Leftrightarrow a-b\in n\mathbb{Z}$$

es decir, a y b dan el mismo resto al dividir por n.

Se escribe $a \equiv b(n)$ y se lee *a congruente con b módulo n*.

Proposición 1:
Son equivalentes:

b) $\overline{a}$ es generador de $\mathbb{Z}/n\mathbb{Z}$

b) mcd(a, n) = 1

c) $\overline{a}\in\left(\mathbb{Z}/n\mathbb{Z}\right)^*$, es decir, a es una unidad (tiene inverso en el anillo)

Demostración:
1) $\rightarrow$ 2)

$\overline{1}=t\overline{a}$ para cierto $t'\in\mathbb{Z}^+$

$\overline{1}=t\Leftrightarrow 1-ta=nt'$ para cierto $t'\in\mathbb{Z}^+$

$1=nt'+ta\Rightarrow$ mcd(n, a) =1 por la Identidad de Bezout.

2) $\rightarrow$ 3)

$mcd(a,n)=1\Rightarrow\exists\alpha,\beta\in\mathbb{Z}/\alpha a+\beta b=1$

$\alpha a+\beta n=\overline{\alpha}\,\overline{a}+\overline{\beta}\,\overline{b}=1\Rightarrow\overline{\alpha}\,\overline{a}=\overline{1}$ ya que $\overline{n}=\overline{0}$,
por tanto $\overline{a}$ es unidad

3) $\rightarrow$ 1)

$\overline{a}\in\left(\mathbb{Z}/n\mathbb{Z}\right)^*\Rightarrow\exists\,\overline{b}\,/\,\overline{a}\cdot\overline{b}=\overline{1}$

$\forall\overline{t}\in\mathbb{Z}/n\mathbb{Z}/\overline{t}=\overline{t}\cdot\overline{b}\cdot\overline{a}=(t\cdot b)\cdot\overline{a}$ por lo que $\overline{a}$
es un generador de $\mathbb{Z}/n\mathbb{Z}$

Con lo que queda demostrado.

Podemos entonces decir que las unidades del anillo $\mathbb{Z}/n\mathbb{Z}$ son:

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^*=\left\{\overline{a}/\overline{a}\text{ es invertible}\right\}=$$
$$=\left\{\overline{a}/1\le a\le n-1\wedge mcd(a,n)=1\right\}$$

Se define $\phi(n)$ como el número de elementos de este grupo de unidades. En el caso de que $n = p \cdot q$ con p y q números primos, resulta que $\phi(n) = (p - 1) \cdot (q - 1)$

Conguencia de Euler:

Sea $n\in\mathbb{Z}^+$ y sea $a\in\mathbb{Z}/mcd(a,n)=1\Rightarrow a^{\phi(n)}\equiv 1(n)$

Demostración:

$$\overline{a}\in\left(\mathbb{Z}/n\mathbb{Z}\right)^*\Rightarrow(\overline{a})^{\phi(n)}=\overline{1}\Rightarrow a^{\phi(n)}\equiv 1(n)$$

ya que cualquier elemento de un grupo $g \in (G, \cdot)$ elevado al orden (número de elementos) del grupo cumple que $g^n = 1$. Este útimo resultado utilizado ya no lo demostraremos. El lector podrá encontrarlo en cualquier libro básico de teoría de grupos. ■