Tú también usas criptografía

por

Paz Morillo Bosch, Universitat Politècnica de Catalunya

El teléfono móvil, las tarjetas bancarias, el DNI electrónico,... son elementos que utilizamos de forma cotidiana. Todos ellos tienen en común un dispositivo, la tarjeta inteligente o "*smart card*", con una cierta capacidad para almacenar datos y para realizar cálculos. Ahora bien, tanto el almacenamiento como los cálculos, deben hacerse de forma segura, esto es, preservando la confidencialidad de los datos privados. En este trabajo vamos a presentar algunos de los conceptos que subyacen al funcionamiento seguro de estos tres elementos.

1. El teléfono móvil

En la comunicación mediante telefonía móvil, el teléfono contacta con una antena de una estación base. El primer paso para establecer la comunicación es la *autenticación* del teléfono para la antena. Esto significa que la antena puede verificar la identidad del teléfono que solicita la comunicación.

Este servicio de seguridad se consigue mediante lo que se denomina **Protocolo de reto-respuesta unilateral**.

Veamos cómo funciona. La tarjeta SIM (del inglés, *subscriber identity module*, en castellano módulo de identificación del suscriptor) del teléfono tiene una clave secreta que comparte con la antena, la antena envía un valor aleatorio al móvil, éste calcula un valor como resultado de una función del número aleatorio recibido y de la clave que posee. Este resultado es enviado a la antena que puede comprobarlo. Así la antena queda convencida de la identidad del teléfono ya que sólo con el uso de la clave privada se puede obtener dicho resultado.

Por otra parte, las comunicaciones entre teléfonos móviles deben ir cifradas, ya que en caso contrario cualquiera que poseyera un receptor podría capturar las conversaciones debido a que viajan en forma de ondas por el aire.

El método utilizado para cifrar las comunicaciones es un método de *cifrado simétrico*, esto es, emisor y receptor comparten una clave secreta que se usará tanto para cifrar como para descifrar los mensajes. La elección de la criptografía de clave simétrica frente a la de clave pública es debida a su mayor rapidez, tanto en la fase de cifrado como en la de descifrado.

Para el proceso de cifrado, debe tenerse en cuenta que la clave secreta del teléfono móvil está almacenada en la tarjeta SIM y, por tanto, no tiene un gran tamaño. Esto hace que no sea adecuada como clave de cifrado, ya que no resistiría ataques de fuerza bruta (prueba y error) o ataques estadísticos (análisis de frecuencias de letras). La solución que se adopta es la generación de *claves de sesión* que son claves de un solo uso. Estas claves se generan cada vez que se quiere establecer una comunicación y se obtienen como resultado de aplicar una cierta función a la clave almacenada en la SIM y a un número generado de forma aleatoria cada vez.

En la siguiente subsección estudiamos con una poco más de detalle la criptografía simétrica.

1.1. Cifrado simétrico

La necesidad de la comunicación secreta se suele situar en el contexto de la diplomacia y la guerra.

Los primeros ejemplos de mensajes cifrados los encontramos en el siglo I a.C. El emperador romano Julio Cesar utilizaba el siguiente sistema para cifrar sus mensajes. Cada letra del mensaje original era sustituida por la que ocupaba 3 posiciones después en el alfabeto, así por ejemplo **Bilbao** quedaría cifrado como **Eloedr**. Por cierto, si se nos acaba el alfabeto volvemos a empezar con la A.

Se trata de un *cifrado de sustitución*, es decir, cada letra tiene su correspondiente símbolo de cifrado. A veces pares de letras o incluso palabras muy usadas se corresponden con un único símbolo.

A continuación vemos una tabla en la que se muestra en una primera fila un alfabeto aleatorio y en la segunda fila el correspondiente alfabeto cifrado.

O	Y	D	M	L	F	V	C	R	E	H	S	I	N	U	B	A	Y
W	T	B	J	K	X	G	R	C	I	Q	Z	E	L	A	D	U	T

Con esta tabla de sustitución, el mensaje “Bilbao” quedaría cifrado como “Dekduw”.

Este tipo de cifrado por sustitución es uno de los métodos más utilizados en la criptografía clásica. El emisor y el receptor del mensaje deben compartir una clave: en el caso de Cesar el 3 (número de posiciones que desplaza la letra), en el otro la tabla de sustitución, ...

Estos métodos de sustitución fueron criptoanalizados, descifrados, con el denominado *Análisis de frecuencias*. Si observamos un texto escrito en castellano,

en seguida nos daremos cuenta de que la letra que más aparece es la *e*, podemos contar el número total de letras y mirar cuál es la proporción de cada una de las letras del alfabeto, es decir, con qué frecuencia aparece cada letra. Por ejemplo, a continuación se muestra una lista de les frecuencias con que cada letra del alfabeto aparece en castellano.

e	a	o	l	s	n	d	r	u
16.78	11.96	8.69	8.37	7.88	7.01	6.87	4.94	4.80
i	t	c	p	m	y	q	b	h
4.15	3.31	2.92	2.77	2.12	1.54	1.53	0.92	0.89
g	f	v	j	ñ	z	x	k	w
0.73	0.52	0.39	0.30	0.29	0.15	0.06	0.01	0.01

Si se intenta ocultar cada letra sustituyéndola por otra (cifrado por sustitución), aún se pueden reconocer las letras originales, ya que las características frecuenciales de las letras originales pasan directamente a las nuevas. Así, si en un texto cifrado en castellano, la letra que más aparece es la *u*, podemos pensar que la *u* está sustituyendo a la *e*.

Durante mucho tiempo, los únicos métodos de cifrado que se utilizaban eran los denominados de clave privada o simétricos. En ellos, el emisor y el receptor deben acordar a priori cuál es la clave con la que se van a cifrar y descifrar los mensajes.

Este *intercambio de claves* supone un gran problema ya que la comunicación cifrada se establece entre usuarios que no poseen un canal de comunicación segura por el que acordar la clave.

En 1976 W.Diffie y M.Hellman en su artículo "New directions in Cryptography" [1] dan un método para establecer una clave común entre dos usuarios. A continuación mostramos el **Protocolo de Diffie-Hellman de intercambio de claves**:

El conjunto $\mathbb{Z}_n$, enteros módulo n, se puede representar como $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. Así,

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}\,.$$

Las operaciones modulares (operaciones en $\mathbb{Z}_n$) se realizan como en los enteros, es decir, $3+4 = 7$ y $4*4 = 16$, sin embargo, para que el resultado de la operación siga dentro del conjunto, a veces hay que realizar una operación adicional y es restar al resultado obtenido tantas veces n como sea necesario, para obtener un valor entre 0 y $n-1$. Así por ejemplo $3+4 = 1(= 7-6)$ y $4*4 = 4(= 16-2*6)$.

Supongamos que n es un número primo p y consideremos el conjunto $\mathbb{Z}_p^*$ (el asterisco indica que quitamos el número 0) con la operación producto. Se trata

de un grupo cíclico, es decir, los números de este conjunto pueden escribirse como potencias de un número dado, llamado generador. Por ejemplo

$$\mathbb{Z}_{17}^* = \{5^0, 5^1, 5^2, 5^3, \ldots, 5^{14}, 5^{15}\} = \{1, 5, 8, 6, \ldots\},$$

esto se denota por $\mathbb{Z}_{17}^* =< 5 >$.

Dos usuarios A y B que quieran acordar un elemento del grupo Z_{17}^* como clave común, procederían de la siguiente forma. Cada uno de ellos elige de forma independiente una potencia, por ejemplo A elige el 3 y B el 7, a continuación se intercambian el resultado de elevar el generador a la potencia que han elegido y que guardan en secreto. En el ejemplo, A enviaría a B $5^3 = 6$ y B enviaría a A $5^7 = 10$. Una vez recibido este número sólo queda que cada uno eleve, a la potencia que guarda en secreto, el número recibido, en el ejemplo, A elevaría $10^3 = 14$ y B calcularía $6^7 = 14$ y el valor 14 sería la clave común.

Se debe comentar que este intercambio de claves es susceptible al ataque denominado *man-in-the-middle*. Un suplantador que intercepte los mensajes que A envía a B puede hacerse pasar por B sin que A se de cuenta.

1.2. Aplicación de la telefonía móvil al voto electrónico

Uno de los ámbitos de aplicación de la telefonía móvil que está ocupando a muchos investigadores es la *votación electrónica*.

A continuación veamos algunas de las posibilidades en este campo.

En primer lugar está el voto por teléfono en el que hay un menú por el que se navega y se hacen las selecciones apretando un botón o diciendo un número cuando toca, como en los servicios de atención al cliente en los que habla un dispositivo. Este dispositivo es un IVR (Interactive Voice Response) que detecta cuándo se le dice que entre en un menú (por ejemplo, un partido para poder seleccionar candidatos) y se encarga de toda la parte de navegación. Para recoger las selecciones y "securizarlas" se propone un sistema, que es que el IVR pase las selecciones que marca el votante a una aplicación que, al final del voto las firma y las cifra, y las envía a un servidor remoto de voto igual que si fuera nuestro ordenador.

Otras aplicaciones del móvil en voto electrónico es, por ejemplo, la utilizada en Barcelona para el referéndum sobre la Diagonal, en la que se ponía DNI, fecha de nacimiento y un número de móvil en la aplicación que se ejecutaba en un ordenador, y esto se enviaba al servidor remoto de votación. El servidor generaba una contraseña de un solo uso, *one-time-password*, que se enviaba al móvil y era la contraseña para entrar a la aplicación de voto en el ordenador.

Finalmente, los estonios, que votan mucho por internet, estrenaron el año pasado un sistema de autenticación por móvil en el que la tarjeta SIM tiene integrado un par de claves de firma. La clave privada se usa de alguna manera para autenti-

carse (también se puede hacer con el eDNI) y obtener una contraseña de un solo uso que permite acceder a la aplicación de voto que corre en el ordenador.

Finalmente, también se puede votar enviando un SMS. En el pollsterless, se tiene una tarjeta con códigos asignados a los candidatos, donde para cada votante estos códigos son diferentes, y luego también hay códigos de retorno. Para votar por un candidato, simplemente se envía un SMS con el código que toca. En el servidor del voto se tiene la clave necesaria para transformar el código del candidato en el código de retorno correspondiente, que se envía de vuelta por SMS para que el votante sepa que el voto registrado en el servidor representa al candidato que ha escogido (verificación). En el servidor de recuento está la clave necesaria para transformar este código en el identificador de candidato y poder así obtener los resultados de la elección. Estas soluciones se plantean para países en desarrollo, donde es más difícil que la gente tenga un ordenador en casa.

2. El teléfono móvil

Estas tarjetas permiten comunicación entre el banco, el cliente y el vendedor. Tres características que se piden son: que sea no falsicable, no clonable y no repudio. Analicemos cada una de ellas.

- **No falsificable**. El banco *firma digitalmente* las tarjetas que emite. Esa firma se guarda en un lugar legible del chip incorporado en la tarjeta. Cualquiera puede verificar esa firma para estar seguro de que esa tarjeta ha sido emitida por un banco. Es decir, se trata de una firma digital *públicamente verificable*.

- **No clonable**. La tarjeta debe poder demostrar al vendedor que es una tarjeta original expedida por un banco. Para ello la tarjeta posee una clave secreta inaccesible. Esta autenticación se realiza mediante un **Protocolo reto-respuesta**, como el mostrado en la autentificación de los teléfonos móviles frente a la antena, pero en este caso utilizando *criptografía de clave pública*. El protocolo funciona de la siguiente manera: El terminal del vendedor envía a la tarjeta un número aleatorio cifrado con la clave pública de la tarjeta que se corresponde con la clave privada de la misma, este cifrado es el reto al cual la tarjeta responde descifrando con su clave privada y devolviendo al terminal el número aleatorio.

  Comprobada la tarjeta (no es falsa ni ha sido clonada), se autentica el propietario de la tarjeta. Este protocolo se realiza entre la tarjeta y el terminal, el propietario de la tarjeta introduce el PIN (*Personal Identification Number*: Número de identificación personal), el terminal retorna a la tarjeta dicho número cifrado con la clave pública de la tarjeta. El chip de la tarjeta descifra y compara con el número guardado en la memoria del chip.

- **No repudio**. Hay que garantizar que la tarjeta que hace la compra no pueda engañar diciendo que no la ha hecho y que el banco no puede adjudicar compras a tarjetas que no las han realizado. Esto se consigue haciendo que la tarjeta haga una firma digital de cada transacción.

Como hemos visto en la explicación anterior aparecen conceptos de criptografía de clave pública tales como firma digital, públicamente verificable,... En la siguiente subsección daremos un esbozo de estos conceptos para comprender un poco mejor su funcionamiento.

2.1. Criptografía de clave pública

El nacimiento de la criptografía científica se suele fechar en 1948 con el artículo de Shannon sobre la Teoría de la Información y la Comunicación Secreta [3].

Hay que esperar hasta 1976 para el nacimiento de la *criptografía de clave pública* o *asimétrica*. W.Diffie y M.Hellman sentaron las bases de la criptografía moderna en [1]. En la criptografía de clave pública cada usuario tiene un par de claves, una pública y otra privada. La clave pública se deposita en una especie de listín telefónico al que todo el mundo puede acceder y la clave privada se mantiene en secreto, la pública servirá para cifrar los mensajes y la privada para descifrarlos. Se puede pensar en una caja fuerte en la que cualquiera puede dejar un mensaje que sólo puede ser leído por el poseedor de la llave.

El modelo matemático en el que se basa la criptografía de clave pública es el de las *funciones unidireccionales con trampa* (*one-way trapdoor functions*), funciones fáciles de calcular pero cuya inversa es difícil de obtener salvo que se tenga una cierta información adicional (la trampa). Pero ¿cuál es el significado de "difícil"? es decir, ¿qué tipo de problemas son "difíciles" de resolver? Una definición simple de problema difícil es aquel para el que no se conoce ningún algoritmo que en tiempo polinómico nos de la solución.

Ejemplos de *problemas computacionalmente difíciles* son:

- **Logaritmo discreto** Se trata del problema del logaritmo pero en grupos de orden finito, es decir, dados y y g, siendo y un elemento de un grupo G generado por g, encontrar x tal que $y = g^x$. Naturalmente, este problema es difícil si estamos en grupo de orden grande (con muchos elementos), ya que en otro caso podemos deducir el valor de x por prueba y error. Se considera adecuado un orden de unos 1500 bits.

- **Factorización** Dado un número natural n producto de dos números primos p y q se trata de hallar estos factores. Tamaño de los primos de 1024 bits se considera correcto para que la factorización sea difícil.

Para poder hacer una buena comparación, en la criptografía de clave simétrica,

el tamaño de las claves que dan un buen nivel de seguridad está alrededor de 128 bits.

A continuación se muestra el criptosistema de clave pública y la firma digital RSA.

2.2. Cifrado y firma RSA

El método de cifrado RSA (iniciales de sus autores Rivest, Shamir y Addleman), fue el primer criptosistema de clave pública propuesto (1976, fecha del artículo pionero de Diffie y Hellman). Se basa en la dificultad de factorizar un número entero grande. Se trabaja en $\mathbb{Z}_n$ siendo n el producto de dos primos grandes p y q que se mantendrán en secreto, la función que se utiliza para el cifrado es elevar a una potencia e que formará parte de la clave pública del usuario y cuyo único requisito es que no tenga factores en común con $(p-1)(q-1)$. Gracias a este requisito, existirá un número d satisfaciendo

$$ed = 1 \mod (p-1)(q-1)$$

y por el Teorema de Fermat, cualquier número x verificará que $x^{ed} = x \mod n$. Este valor d sólo es calculable por aquél que conozca la factorización de n.

El concepto de firma digital de mensajes se puede entender como un método electrónico que garantiza la identidad del remitente del mensaje. Es decir, el emisor ha de mostrar el resultado de alguna operación que sólo él puede haber realizado correctamente. Por ejemplo, usando el criptosistema RSA el usuario que ha hecho públicas n y e es el único que conoce d y, por tanto, el único que puede calcular x^d mód n para un x fijado. Así, este valor serviría como firma digital del mensaje x.

Veamos un ejemplo, tomemos $N = 133$ y $e = 5$, estos dos valores serán nuestra clave pública y nuestra clave privada correspondiente estará formada por los primos $p = 7$, $q = 19$ y $d = 65$. Observemos que se satisface que

$$e \cdot d = 5 \cdot 65 = 325 = 1 \mod 108$$

siendo $108 = (p-1)(q-1) = 6 \cdot 18$, ya que $325 = 1 + 108 \cdot 3$.

- **Cifrado**: Alguien que quiera enviarnos un mensaje cifrado, por ejemplo $m = 6$, usa la clave pública (n, e) para calcular $m^e \mod n$, en el ejemplo calculará $6^5 \mod 133$ cuyo resultado es 62. Cuando recibimos el mensaje $c = 62$, para descifrarlo usamos nuestra clave privada d y hacemos c^d, veamos, en el ejemplo calcularíamos $62^{65} \mod 133$ que efectivamente da como resultado 6.

- **Firma**: Alguien que quiera comprobar nuestra identidad nos pide por ejemplo que firmemos el mensaje $x = 8$, nuestra firma será $8^{65} = 50 \mod 133$.

En resumen, el mensaje 8 ha sido firmado con el valor 50. Cualquiera puede comprobar que $50^5 = 8 \mod 133$ y sólo nosotros podemos haber hecho el cálculo que conduce a ese valor. Esta idea de que cualquiera puede comprobar la firma corresponde al concepto antes mencionado de verificabilidad pública.

Observemos que las operaciones de firmar y descifrar son la misma, análogamente a las de cifrar y verificar la firma.

Esta firma RSA es la usada por PGP (pretty good privacy) sistema gratuito y el más usado en correo electrónico, diseñado y desarrollado por Phil Zimmermann en 1991. La página oficial es www.pgp.com.

3. DNI electrónico

El poseer un documento de identidad con un chip permite poder realizar gestiones como declaración de renta, trámites con la seguridad social, gestiones administrativas,... desde cualquier lugar con acceso a un ordenador. Por otra parte permite la firma de documentos con las prestaciones de la firma digital esbozada en la sección anterior, es decir, la firma va ligada al documento y es públicamente verificable.

El uso del DNI electrónico conlleva la autenticación del cliente (poseedor del DNI) frente al servicio (hacienda, seguridad social, ...) y viceversa, ya que el usuario debe estar seguro que está contactando con la entidad adecuada. Esta autenticación se realiza mediante un **protocolo de reto-respuesta**, pero en este caso **bilateral**.

Veamos su funcionamiento. El servicio reta al usuario con un número aleatorio, r_s, el usuario retorna otro aleatorio generado por él r_u, así como la firma, con su clave secreta S_u, de la pareja (r_u, r_s) y el servicio devuelve al usuario la firma, con su clave secreta S_s, de la misma pareja. Así cualquiera de las dos partes puede verificar que la otra ha firmado la pareja de aleatorios.

4. Estructura de clave pública, PKI

En los párrafos anteriores debería de haber quedado claro las ventajas de la criptografía de clave pública. Sin embargo adolece de un gran problema que es la *gestión de las claves*: de alguna manera se ha de garantizar que la clave pública pk_U efectivamente es del usuario U. Este proceso se realiza mediante certificados digitales. Así, por ejemplo, podemos suponer que la clave pública de nuestro DNI está firmada por una comisaría cuya clave pública está firmada por la central de policía cuya clave pública está firmada por ....

En 1984 Shamir [4] definió el concepto de *Identity based cryptography*, en castellano, *criptografía basada en identidades*, para solventar el problema de la gestión

de las claves públicas. La clave pública de cada usuario es su identidad y la clave privada la genera una autoridad, *master entity*, a partir de una clave maestra y la identidad del usuario.

Las propuestas realizadas hasta la fecha utilizan un objeto matemático conocido como *pairings*. Son aplicaciones bilineales, esto es, $\widehat{e} : G_1 \times G_1 \to G_2$, siendo G_1 y G_2 grupos, satisfaciendo $\widehat{e}(g_1^a, g_2^b) = \widehat{e}(g_1, g_2)^{ab}$.

4.1. Esquemas basados en identidades

En este apartado mostramos el funcionamiento de un esquema de cifrado de clave pública basado en identidades, fue propuesto por Boneh y Franklin en 2003 [5]. Se supone una aplicación bilineal como la antes mencionada $\widehat{e} : G_1 \times G_1 \to G_2$, un elemento g generador del grupo G_1, una clave maestra secreta s y un valor público $h = g^s$. El espacio de los mensajes es G_2 y las identidades son elementos del grupo G_1. Entonces, la clave secreta asociada a una identidad es generada por la autoridad como $SK_{Id} = Id^s$. El algoritmo para cifrar un mensaje m destinado a la identidad Id es el par

$$(c_1, c_2) = (g^r, m \cdot \widehat{e}(Id, h)^r)$$

siendo r un número aleatorio elegido por el emisor del mensaje. Para descifrar, el receptor debe poder calcular el factor $\widehat{e}(Id, h)^r$, para dividir por él la cantidad c_2 y recuperar el mensaje m. Este factor lo obtiene a partir de su clave secreta realizando $\widehat{e}(SK_{Id}, c_1)$. En efecto, observemos

$$\widehat{e}(SK_{Id}, c_1) = \widehat{e}(Id^s, g^r) = \widehat{e}(Id, g^s)^r = \widehat{e}(Id, h)^r \,,$$

donde las igualdades son consecuencia de la propiedad de bilinealidad.

Cabe destacar que este esquema también permite la realización de firmas digitales.

5. Conclusiones

Sin criptografía la vida sería más complicada

Bibliografía

[1] W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory, vol IT-22, 644-654, 1976.
[2] R.L.Rivest, A.Shamir, and L.Addleman, *A method for obtaining digital signatures and public-key cryptosystem*, Comm. ACM, vol 21, 120-126, 1978.
[3] C.Shanon, *A Mathematical Theory of Communication*, Bell System Technical Journal, vol 27, 379-423, 623-656, 1948.

[4] A. Shamir, *Identity-Based Cryptosystems and Signature Schemes*, Advances in Cryptology: Proc. of CRYPTO 84, LNCS, vol 7, 47-53, 1984.
[5] D.Boneh, M.K. Franklin, *Identity-Based Encryption from the Weil Pairing*, Advances in Cryptology - Proc. of CRYPTO 2001, LNCS, vol 2139, 213-229, 2001.

Paz Morillo Bosch
Matemática Aplicada IV
C. Jordi Girona, 1-3, 08034 Barcelona
e-mail: pazma4.upc.edu