La Matemática que confiere seguridad a las transacciones bancarias

[El Criptosistema RSA]

El Criptosistema **RSA** es uno más de los diversos sistemas de encriptado que se utilizan hoy día con el propósito de asegurar el intercambio de información. El nombre del criptosistema es un acrónimo de los apellidos de sus creadores (**R**ivest, **S**hamir, **A**dleman) y fue ideado en el año de 1978[1], bajo la inspiración de los criptosistemas de llave pública que dos años atrás (1976) crearon Diffie y Hellman.

Todo criptosistema tiene por objetivo asegurar el intercambio de información entre dos sujetos a través de un canal de flujo de información que puede ser altamente vulnerable (teléfono, Internet, etc.) que –se asume- está siendo rastreado por otro sujeto cuyo objetivo es interceptar el mensaje a fin de conocer el contenido del mismo (a ello se dedica el criptoanálisis). Supóngase entonces que las personas S_1 y S_2 necesitan compartir información secreta o privada, por ejemplo, un mensaje (un texto en español, un mensaje numérico o alfanumérico, etc.). Entonces, S_1 encripta (cifra) el mensaje original utilizando una clave determinada a la que llamaremos "llave" y envía el texto cifrado resultante a través del canal. La persona S_3 puede tener acceso al mensaje cifrado a través del canal, pero ésta no puede determinar el contenido del mensaje original pues no conoce la clave de encriptado que, en cambio, S_2 sí conoce y quien, por tanto, está en capacidad de reconstruir –a partir del mensaje cifrado- el mensaje original. La figura 1 ilustra este esquema de cifrado/descifrado.

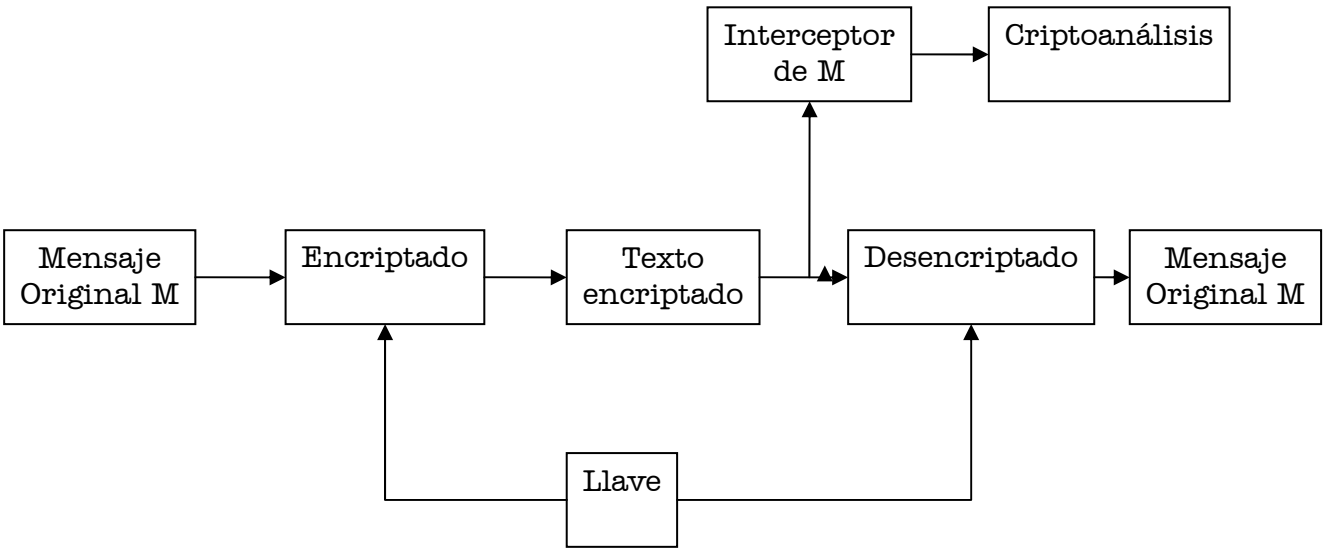

Fig. 1: Esquema de Cifrado/Descifrado

En términos formales, un criptosistema es una quíntupla $(\mathrm{P}, \mathbb{C}, \mathrm{K}, \mathrm{E}, D)$ en el que son satisfechas las siguientes condiciones:

[1] Se sabe, sin embargo, que para 1973 fue publicado un *paper* escrito por Clifford Cocks, intitulado "A note on non-secret encryption", en el cual es descrito un criptosistema de llave pública que, en esencia, opera igual que el Criptosistema RSA.

- P, un conjunto finito de posibles mensajes a enviar
- $\mathbb{C}$, un conjunto finito de posibles mensajes cifrados
- K, un conjunto finito de llaves posibles
- $\forall k \in \mathrm{K}$ existe una regla de encriptado (función) $E_k \in \mathrm{E}$ y una correspondiente regla o función de desencriptado $D_k \in D$. Cada $E_k : \mathrm{P} \to \mathbb{C}$ y $D_k : \mathbb{C} \to \mathrm{P}$ son funciones tales que $D_k\left(\mathrm{E}_k(m)\right) = m$ para todo mensaje m perteneciente a P.

Ahora bien, convencionalmente los criptosistemas de llave privada utilizan una misma clave o parámetro para asegurar el intercambio de información (encriptar/desencriptar); el inconveniente de ello reside en el hecho simple de que, como la llave debe viajar también por el canal de información aludido, entonces un sujeto no autorizado podría descubrir la llave de desencriptado en un corto período de tiempo. Sin embargo –como ya se dijo- hacia 1976 Whitfield Diffie y Martin E. Hellman de la Universidad de Stanford proponen un revolucionario sistema de encriptado de llave pública que permite prescindir de la necesidad de mantener a la misma a salvo de usuarios no autorizados. A pesar de no haber generado una implementación práctica de su propuesta, Diffie y Hellman establecieron tres características para el cifrado de llave pública:

1. Todo usuario debe tener una llave de encriptado E (que es pública) y una llave de desencriptado D (mantenida en secreto), tales que $M = E\left(D(M)\right) = D\left(E(M)\right)$ para todo mensaje M. De esta manera E y D son funciones (algoritmos) inversas.
2. Resulta computacionalmente sencillo para el usuario calcular las llaves E y D.
3. Es computacionalmente no factible para usuarios no autorizados, emplear la llave de encriptado E con el propósito de desarrollar la llave de desencriptado D. Ello garantiza la seguridad del sistema.

Criptosistema RSA

El *quid* de este criptosistema radica en el uso de una función trampa cuyo algoritmo es fácil de computar, pero cuya función inversa implica un cálculo –salvo que se conozca la llave de encriptado- prácticamente irrealizable.

A continuación se describen, sin mayor rigor, las herramientas teóricas de que hace uso este criptosistema:

El inverso módulo n en $\mathbb{Z}_n$

Se dice que $[a]_n$ es invertible en $\mathbb{Z}_n$ si existe un $[b]_n \in \mathbb{Z}_n$ tal que $[a]_n \cdot [b]_n = [1]_n$. En notación de congruencias, esto significa que $a \cdot b \equiv 1 \pmod{n}$. Todo elemento invertible en $\mathbb{Z}_n$ es una unidad de n.

Proposición. Un entero a tiene una inversa $\bmod n$ si y sólo si $mcd(a,n) = 1$.

Definición. Sea $\mathbb{Z}_n^*$ un subconjunto de $\mathbb{Z}_n$ formado por aquellos elementos que son invertibles. Entonces, $\mathbb{Z}_n^*$ está constituido por todos aquellos elementos a de $\mathbb{Z}_n$ tales que $mcd(a,n)=1$.

Sea $\varphi(n)$ la cardinalidad de $\mathbb{Z}_n^*$; si, por ejemplo, n es un número primo, entonces, $\varphi(n)=\varphi(p)=p-1$ (ya que todos los residuos en $\mathbb{Z}_n$, excepto p mismo, tienen como máximo común denominador con p, al 1). Lo anterior nos lleva a definir la siguiente función.

La función φ de Euler

Se define la función de Euler $\varphi(n)$ como el número de números enteros mayores ó iguales a 1 y menores que n, primos relativos con n. Algunas propiedades de φ son:

P1: $\varphi(n)=n-1$ para n primo.

P2: $\varphi(n^k)=n^{k-1}(n-1)$ para n primo.

P3: $\varphi(m\cdot n)=\varphi(m)\cdot\varphi(n)$ ssi $mcd(m,n)=1$

IMPORTANTE: Nos damos cuenta que $\varphi(n)$ es fácil de computar si se conoce la factorización prima de n, de otra manera, resulta difícil.

El Teorema de Euler

Si a es un elemento de $\mathbb{Z}_n^*$, entonces $\left[a^{\varphi(n)}\right]_n=[1]_n$ o sea:

$$a^{\varphi(n)}\equiv 1(\bmod n)$$

[→Ejemplo Práctico←]

Supóngase que S_1 necesita enviar a S_2 el mensaje $M=19$. S_2, entonces, pone a disposición de S_1 la llave pública constituida por los números (n,e) conformados de la siguiente manera:

S_2 selecciona dos números primos bastante grandes (digamos, 100 dígitos cada uno) y obtiene el producto $n=p\cdot q$. Para efectos prácticos, supóngase que $p=7$ y $q=17$. Después, calcula $\varphi(n)$ obteniendo: $\varphi(n)=\varphi(p\cdot q)=\varphi(p)\cdot\varphi(q)=\varphi(p-1)\cdot\varphi(q-1)=6\cdot 16=96$.

Luego S_2 escoge un número e tal que $mcd(e,\varphi(n))=1$. Por ejemplo, $e=5$. Hasta este punto, S_2 ha calculado la llave pública (n,e). Para calcular, ahora, la llave privada, hace lo siguiente:

Elige un d tal que, $e\cdot d\equiv 1(\bmod\varphi(n))$ o sea $5\cdot d\equiv 1(\bmod 96)$, es decir, d es la inversa de e $\bmod(\varphi(n))$. En la práctica y para números más grandes, se utiliza el algoritmo extendido de

Euclides para hacer este cálculo. Sin embargo, por tratarse de números "pequeños" nos damos cuenta de que $[5]_{96} \cdot [77]_{96} = [1]_{96}$, ya que $77 \cdot 5 = 385 = 4 \cdot 96 + 1$.

Ya disponemos, entonces, de la clave privada $(d, n) = (77, 119)$. Entonces, S_1 está ya en posibilidad de encriptar su mensaje y enviarlo a S_2. Para obtener el mensaje encriptado C, S_1 procede de la siguiente forma:

$C = M^e \pmod n = 19^{4+1} \pmod{119} = 66$ (Para realizar este cálculo se expresa el exponente como una suma de sus potencias de 2 a fin de hacerlo más ligero y rápido). Ahora S_2 recibe C y para desencriptarlo lo eleva a la potencia $d \bmod n$, es decir: $M = 66^{77} \pmod{119} = 19$. Lo anterior fue posible debido a que si d es el inverso de $e \mod \varphi(n)$, entonces -como ya se mencionó- $e \cdot d \equiv 1 \pmod{\varphi(n)}$ lo que significa que existe un t tal que

$$e \cdot d = t\varphi(n) + 1$$

Entonces:

$$m^{e \cdot d} = m^{t\varphi(n)+1} = m^1 \cdot m^{t\varphi(n)} = m\left(m^{\varphi(n)}\right)^t$$

Pero por el Teorema de Euler tenemos que $m^{\varphi(n)} \equiv 1 \pmod n$, entonces

$$m^{e \cdot d} = m\left(m^{\varphi(n)}\right)^t \equiv m(1 \bmod n)^t \equiv m \cdot 1^t \bmod n$$

$$\therefore m^{e \cdot d} \equiv m \pmod n$$

Entonces, nos damos cuenta de que la seguridad de este criptosistema depende de la dificultad de factorizar números grandes.

Un par de anécdotas históricas

Uno de los factores que incrementa el interés por la criptología en el siglo XIX, es la publicación del relato de *Edgar Allan Poe* "El escarabajo de oro"; cuento cuya trama emplea mensajes cifrados que logran excitar la imaginación de muchos lectores.

En 1917, en el punto más álgido de la Primera Guerra Mundial, Alemania envía un cable al gobierno mexicano, anunciándole que comenzaría una guerra submarina contra Estados Unidos, una vez que éste entrase a la guerra, prometiéndole a México la recuperación de Arizona, Nuevo México y Texas si éste se unía a los países de la triple Alianza. El cable fue interceptado, el código fue descubierto por la inteligencia británica, el mensaje llegó a manos de Woodrow Wilson y el resto es historia.

Referencias bibliográficas

[1] Camacho, Sara; ***Análisis de Algoritmos***, UNAM, FES Acatlán, México, 1998.
[2] Koshy Thomas; ***Elementary Number Theory with Applications***, Academic Press, 2007.
[3] Stillwell, John; ***Elements of Number Theory***, Springer-Verlag, 2002.
[4] Stinson, Douglas R.; ***Cryptography. Theory and Practice***, Chapman & Hall, 2002.