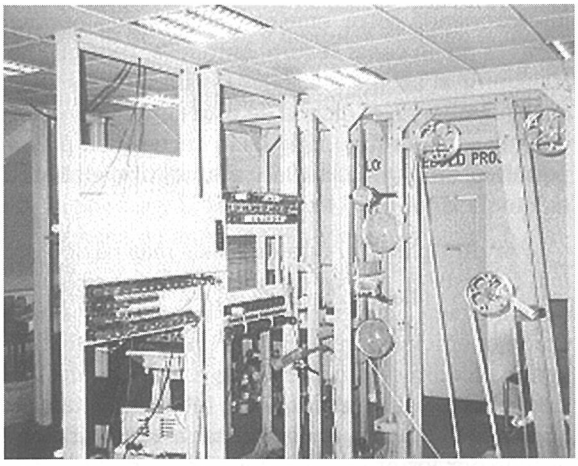
ALGUNOS HITOS DE LA CRIPTOGRAFÍA DEL SIGLO XX

Pino Caballero Gil

Historia

La criptografía, o ciencia que estudia las comunicaciones cifradas, ha ido siempre de la mano de las matemáticas. Desde el punto de vista de la matemática moderna, nos encontramos con nombres de criptógrafos en los campos de la estadística (W. F. Friedman, 1920), el álgebra combinatoria (L. S. Hill, 1929) y la teoría de la información (C. E. Shannon, 1941). Pero además de estas disciplinas matemáticas, juegan un papel fundamental en el estado actual de la criptografía, la teoría de números, la teoría de grupos, la lógica combinatoria, la teoría de la complejidad y la teoría ergódica. De hecho, esta ciencia puede verse como una subdivisión de las matemáticas aplicadas y de las ciencias de la computación.

Antes del siglo XX la criptografía se consideraba un arte que resultaba útil sólo para unos pocos políticos y militares. Durante el presente siglo se produjo un cambio radical en su concepción. En la primera mitad, aunque se realizaron las primeras aproximaciones científicas importantes, todavía su uso se restringía a ámbitos político-militares. Durante las dos guerras mundiales, se produjeron sendos hitos criptográficos que modificaron el curso de la historia. En la primera, la ruptura del cifrado del famoso telegrama *Zimmermann* hizo entrar en guerra a los EEUU al descubrir los planes alemanes. Por otra parte, desde el principio de la Segunda Guerra Mundial, los aliados eran capaces de leer los mensajes secretos alemanes ya que habían roto su máquina de cifrar, la Enigma. Para ello diseñaron una máquina de cálculo gigantesca, el Colossus, precursora de los ordenadores modernos. Uno de sus artífices fue el matemático inglés A.M. Turing (1912-1954), fundador de las ciencias de la computación y de la inteligencia artificial.



El Colossus, *precursor de los ordenadores modernos.*

La criptografía empezó a ser considerada una ciencia

en 1949, cuando C. E. Shannon, padre de la teoría de la información, utilizó ésta para establecer su base teórica. Sin embargo, en esos años todavía los cifrados eran demasiado complicados y caros para utilizarse a diario. Haría falta esperar hasta los setenta, en que los microprocesadores se hicieron rápidos y asequibles, ofreciendo con ello los medios necesarios para poder alcanzar nuevos hitos criptográficos. En 1976 las ideas de C. E. Shannon fueron utilizadas para desarrollar el cifrado conocido como DES, que durante muchos años fue estándar en EE. UU. Por otro lado, ese mismo año, dos matemáticos estadounidenses, W. Diffie y M. E. Hellman, idearon una nueva forma de cifrar, la clave pública, basada en una gran cantidad de cálculos e ingenio matemático. A partir de esa década y en apenas veinticinco años el uso de criptografía se generaliza y se diversifica, poniéndose al alcance de todos.

Conceptos

En el mundo de las comunicaciones secretas cohabitan dos tipos de personajes. Por un lado están los usuarios que quieren preservar el secreto de sus mensajes (y usan la criptografía), y por otro están los denominados *enemigos* que tratan de leer dichos mensajes (y usan el criptoanálisis). La criptología es la continua lucha entre ambos. Un éxito del enemigo conduce a la necesidad de fortalecer los sistemas criptográficos, lo que implica la búsqueda de nuevos métodos criptoanalíticos, y así continuamente. Esto implica que la criptología es una ciencia viva, ya que en el mismo momento en que se describe un nuevo método de cifrado, automáticamente surge la posibilidad de atacarlo. Así, en la práctica, aunque la certidumbre matemática sobre la seguridad de los cifrados no se pueda alcanzar, lo que sí pretende el criptógrafo es una alta probabilidad de que los ataques no fructifiquen.

A este respecto, el único sistema de cifrado matemáticamente seguro es el llamado cifrado de Vernam. Su inconveniente es que requiere una clave de cifrado igual de extensa que el propio mensaje. Como esta clave tiene que ser intercambiada entre emisor y receptor, es necesario su envío del uno al otro a través de un canal seguro. Entonces, ¿por qué no usar ese canal seguro para transmitir el propio mensaje? De ahí que el sistema resulte inútil en la práctica. Sin embargo, el diseño de este cifrado constituye la base de los denominados cifrados en flujo, que usan secuencias pseudoaleatorias como claves, y permiten una aproximación a la seguridad matemática evitando el inconveniente de la longitud de la clave.

Por otra parte, el criptoanálisis más básico denominado *búsqueda exhaustiva* consiste en probar cada una de las posibles claves hasta dar con la que ha sido utilizada. Este es el ataque más largo posible ya que el número aproximado de operaciones requerido para romper un cifrado con una clave de determinada longitud es dos elevado a esa cantidad. Este valor representa para el diseñador de cifrados una cota inferior del tamaño de las claves a usar, dado que existen muchas herramientas matemáticas y estadísticas que pueden ser usadas por los criptoanalistas para deducir la clave sin tener que probar una a una todas las posibles.

Clave pública

La introducción de la clave pública en 1976 conmocionó el mundo de la criptografía. Dos consecuencias de esta revolución fueron la consiguiente aceptación de la criptografía como una rama importante de las matemáticas, y el enorme crecimiento de la comunidad criptográfica en universidades y empresas de todo el mundo. Pero la elegancia de la clave pública proporciona algo más que un juguete para matemáticos. Es una herramienta muy práctica que puede ser utilizada con diferentes utilidades.

La clave pública se basa en un tipo especial de funciones matemáticas conocidas como funciones unidireccionales con trampa, cuya característica consiste en que se pueden aplicar de forma sencilla, pero sin embargo es muy difícil invertirlas salvo que se posea determinada información adicional (trampa). Esta herramienta permite el diseño de sistemas en los que el cifrado se realiza con una clave pública, mientras que para descifrar es necesario poseer una clave secreta. De ahí que la introducción de la clave pública fuera tan crucial. En los sistemas tradicionales se utiliza una sola clave tanto para cifrar como para descifrar, lo que conlleva la necesidad de que emisor y receptor se comuniquen previamente y mediante un canal seguro la clave a usar. La clave pública elimina el problema ya que usándola se hacen innecesarios la comunicación previa y el canal seguro. Además, el número de claves a manejar por cada usuario disminuye proporcionalmente al número de interlocutores que se tenga.

En el algoritmo propuesto por W. Diffie y M. E. Hellman, el emisor utiliza dos números, uno secreto x y otro público g, para calcular g^x, y envía el resultado al receptor. Este, por su parte usa su número secreto y, junto con el público g, para calcular g^y, y se lo remite al emisor. Así, ambos pueden fácilmente calcular g^{xy} y usar este valor como clave secreta compartida. Aunque un enemigo interceptara g^x y g^y e intentara deducir los números secretos x e y, no lo podría hacer ya que todos los cálculos anteriores se llevan a cabo en un cuerpo finito y el cálculo de logaritmos discretos es uno de los problemas considerados más difíciles. El manejo de aritmética modular se da en la mayoría de los sistemas de clave pública, entre otras razones, porque acota las dimensiones de los números manejados, lo que influye positivamente en la eficiencia computacional de los cifrados.

El cifrado de clave pública más usado y analizado hasta hoy, fue ideado por tres matemáticos: R. L. Rivest, A. Shamir y L. M. Adleman, y se conoce por sus iniciales, RSA. Se basa en un problema de análisis numérico muy sencillo consistente en que es fácil multiplicar dos grandes números primos, pero es extremadamente difícil factorizar su producto. Así, el producto puede ser publicado y usado como clave de cifrado y, como no es factible recuperar los primos a partir del producto, aquéllos pueden usarse como claves de descifrado.

Sin embargo hay que decir que también la clave pública tiene una desventaja. Conlleva una gran cantidad de cálculos matemáticos, que son el origen de su relativa lentitud comparada con la velocidad de la criptografía de clave secreta. De hecho, cuando los mensajes son muy largos, o bien cuando es

imprescindible la inmediatez en las comunicaciones, hoy en día sigue utilizándose generalmente clave secreta, o bien sistemas híbridos; aunque hay que decir a este respecto que los avances tecnológicos liman las diferencias entre velocidades de ambos tipos de criptografías.

Futuro

No hace falta una bola de cristal para predecir el crecimiento que la criptología experimentará en los próximos años. Hoy en día casi todo el mundo es consciente de la importancia de la seguridad de la información, pero podría preguntarse ¿por qué la criptografía es el mejor remedio? ¿No existen otras formas de lograr la tan ansiada seguridad? Claro que las hay. Pensemos por ejemplo en las elaboradas técnicas desarrolladas durante siglos para conseguir cheques seguros, como papel especial, intrincados dibujos, impresión de precisión, marcas especiales, alambres de plata, etc. Entonces, ¿por qué criptografía? La respuesta es simple: La criptografía es mejor porque ¡La criptografía es una disciplina matemática! Las matemáticas proporcionan la justificación teórica de la fortaleza de un algoritmo o protocolo particular. Aunque no siempre permitan demostrar que un algoritmo dado es seguro, lo que sí proporcionan es un medio para investigar sistemáticamente su seguridad.

Bibliografía

Bauer, F. L.: *Decrypted Secrets*. Springer, 1997.

Caballero, P.: *Introducción a la Criptografía*. Ra-Ma, 1996.

Patterson, W.: *Mathematical Cryptology*. Rowman & Littlefield, 1987.

Sgarro, A.: *Códigos Secretos*, Pirámide. 1990.