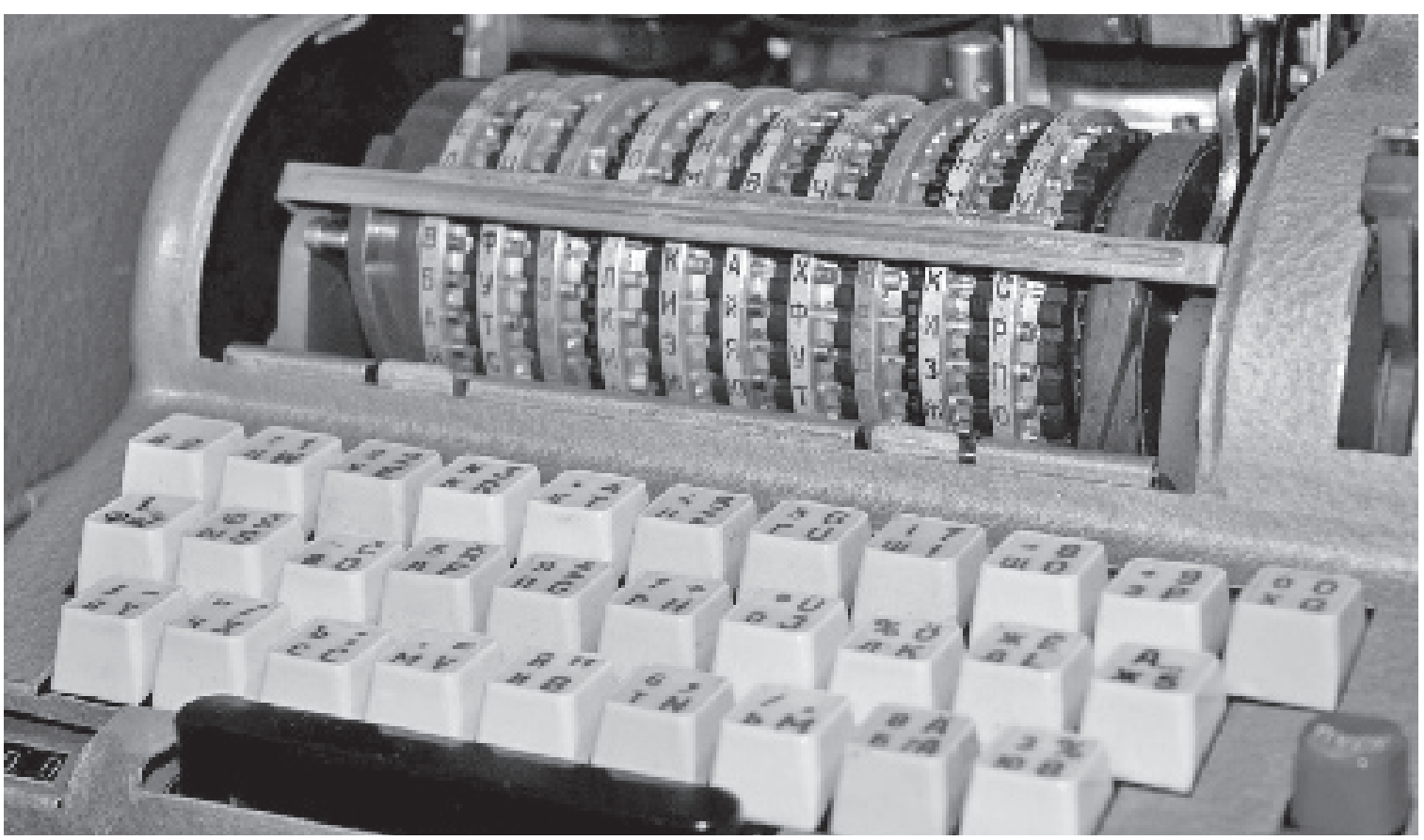
Opinión

En la ciencia de lo secreto

Jorge Franganillo
Profesor de Información y Documentación de la Universidad de Barcelona
Especial para Diario UNO



Máquina Fialka. Un dispositivo similar a este fue utilizado por el servicio secreto ruso durante la Guerra Fría (fotografía: Marco Santoro)

Bien antiguas son las artes de ocultar el texto real de un mensaje para evitar que caiga en manos indiscretas. Lejos de ser una práctica exclusiva de sectas secretas, el arte de codificar un mensaje para ocultar su verdadero significado es toda una ciencia que desde hace mucho tiempo vive entre nosotros. Es la criptografía, ciencia y arte de codificar un mensaje para que viaje oculto, o bien para descifrar aquello que su autor ha querido dejar escondido. Pero todo lo codificado, o casi todo, acaba viendo la luz, y el último ejemplo vio la luz el pasado mes de octubre: después de años de trabajos, un grupo de especialistas logró descifrar un manuscrito de 1866, el llamado Copiale Cipher, que pretendía mantener ocultos ciertos rituales relacionados con operaciones en los ojos que al parecer practicaba una secta alemana de aquel entonces.

En la Segunda Guerra Mundial, el ejército alemán usó un aparato llamado Enigma

María Estuardo, coronada como reina de Escocia a los 9 meses de edad, estando en prisión, acusada de conspiración, usó el cifrado por sustitución de caracteres para explicar en varias cartas sus planes para escapar de la cárcel, asesinar a la reina Isabel I de Inglaterra y así recuperar el trono. María y sus cómplices creyeron que nadie podría descifrarlas, pero las cartas fueron interceptadas, descifradas y utilizadas como prueba judicial. Fue decapitada, a los 45 años, el 8 de febrero de 1587.

Durante la Segunda Guerra Mundial, el ejército alemán usó un dispositivo llamado Enigma para cifrar comunicaciones militares. La máquina era tan intrincada que los alemanes la creyeron un sistema impenetrable, pero las fuerzas aliadas consiguieron vulnerar el código criptográfico y descifraron los mensajes.

El deseo (o la necesidad) de mantener el secreto del mensaje escrito, incluso cuando no se trata de asuntos importantes, está arraigado en nuestra cultura. Usar un sobre cerrado para enviar una carta no es una mera costumbre ni una simple formalidad: cerramos el sobre para evitar que el contenido quede a la vista de cualquiera que no sea su destinatario. Como alternativa, el correo electrónico es un buen medio de comunicación; aquí no hay un sobre que encierre el mensaje sino un clave privada que actúa como la llave que abre el acceso al contenido del mensaje. No es casualidad que las palabras clave y llave tengan un mismo origen: ambas vienen del latín clavis. En efecto, una clave es para la criptografía una llave, un código que protege un mensaje.

La criptografía ha tenido una importancia decisiva durante más de dos milenios, y continúa teniéndola. Es una ciencia antigua que ya utilizaban los romanos para mantener sus comunicaciones militares a salvo de los enemigos. Hasta la década de 1970 fue una especie de magia negra que sólo practicaban algunos gobiernos y ejércitos, pero hoy es una materia que se enseña en la universidad, está al alcance de empresas y particulares. Este proceso de cambio, la popularización de la criptografía, se debe sobre todo a Internet como canal de comunicación y negocio porque tanto las comunicaciones como los negocios necesitan que ciertos datos se mantengan secretos y protegidos.

Los temores sobre la seguridad de Internet son uno de los principales obstáculos para la plena aceptación del comercio electrónico. Es lógico que quien hace una transacción o se comunica a través de la red quiera asegurarse de que el interlocutor es quien dice ser y que el mensaje que recibe es auténtico. Este es un entorno donde las personas no se ven las caras, y entonces se hace necesario verificar la identidad del otro.

El DNI electrónico promete resolver este problema. Con él, la firma electrónica es, según los expertos, el medio de identificación más seguro que podemos tener como ciudadanos, y tiene validez legal. Un algoritmo matemático y una combinación de claves garantizan la integridad de un mensaje y la identidad de quien lo firma.

El cifrado de datos también está presente en otros ámbitos de la vida cotidiana: la televisión de pago, la telefonía móvil, el voto electrónico. Y protege casi todos los procesos de Internet: la conexión a una red Wi-Fi, las compras y transacciones, las pujas en una subasta, ciertas comunicaciones y muchos otros procesos. Tras estos movimientos que reclaman seguridad se esconde un complejo mecanismo de cifrado y descifrado en el que interviene una clave.

Aún no existe un sistema totalmente seguro, ni existirá, porque hay muchas maneras de romper códigos. Aunque la criptografía oculta mensajes mediante la distorsión y así impide que un atacante pueda conocer la información original, no logra que el secreto pase inadvertido porque el propio cifrado ya indica que hay información oculta. Para que no se vea que hay gato encerrado, se ha llegado a usar una técnica llamada esteganografía, que camufla el secreto en un medio aparentemente banal, de tal modo que el cifrado pasa desapercibido para quien no lo espera.

La técnica esteganográfica más común consiste en ocultar un mensaje dentro de contenido multimedia, mezclando los bits del mensaje original entre los bits del fichero gráfico o sonoro, que se mantendrá totalmente funcional y a simple vista nada hará sospechar. Así, mientras la criptografía intenta evitar el descifrado de un mensaje, la esteganografía intenta que el mensaje, además, pase inadvertido. Grupos terroristas y servicios de inteligencia han utilizado esta técnica para transmitir mensajes secretos sin levantar la menor sospecha.

El cifrado y descifrado de mensajes en clave ha inspirado novelas, películas y series de televisión, y por ellas muchas personas han sabido de la importancia del cifrado y han reflexionado sobre las consecuencias del descifrado de una clave. En el filme Al rojo vivo (1995), por ejemplo, un niño autista muestra una prodigiosa capacidad para interpretar códigos del gobierno que se consideraban indescifrables. Y ello ilustra que las claves no son inviolables. Por lo tanto, creer en la posibilidad de un algoritmo inquebrantable es una ingenuidad que puede tener malas consecuencias.

Los temores sobre la seguridad de Internet son uno de los principales obstáculos

La continua batalla entre creadores y descifradores de códigos también ha inspirado numerosos avances científicos. Los creadores se han esforzado por construir códigos cada vez más eficaces mientras los descifradores no han parado de inventar métodos más potentes para detectarlos y atacarlos.

En sus respectivos esfuerzos para preservar y destruir el secreto, ambas partes se han basado en una miríada de disciplinas y tecnologías, de las matemáticas a la lingüística, de la teoría de la información a la física cuántica.

La criptografía es, pues, un árbol de hoja caduca, y ahora se enfrenta a una amenaza: la computación cuántica. En un futuro los potentes computadores cuánticos podrán vulnerar con suma facilidad un código que hoy parece seguro. Muchos afirman que la informática cuántica provocará el derrumbe de las técnicas criptográficas conocidas hasta ahora. Efectivamente, descifrar los códigos que usamos ahora será pan comido. Habrá que encontrar entonces otros métodos en los que confiar.