Criptografía

Imagine que desea realizar una compra por Internet, pagar su tarjeta de crédito o realizar transferencias entre sus cuentas a través del portal de su banco, pagar servicios o quizá acceder a la página del SAT para hacer su declaración anual. Ahora imagine que cualquier persona pudiera visualizar todas las operaciones que realice con relativa facilidad mientras se transfieren a través de la red, y obtenga sus datos confidenciales (nombre, números de cuenta, contraseña, montos, número de tarjeta de crédito, etc.). Seguramente al saber esto evitaría llevar a cabo cualquier clase de transacciones utilizando una computadora. Afortunadamente, dicha visualización no es así de simple. Gracias a la criptografía, prácticamente cualquier transacción que se haga a través de Internet, sobre todo de índole comercial, financiera o militar, se efectúa con un alto grado de seguridad y confiabilidad.

La criptografía es definida como la ciencia (anteriormente considerada como arte) encargada del estudio de la codificación (encriptamiento u ocultamiento) de la información con el fin de que ningún usuario, salvo el propietario o aquel que haya sido autorizado, pueda decodificarla (desencriptarla) mediante el uso de una clave que únicamente él conoce. La utilidad de codificar texto (hacerlo secreto) no es reciente; desde la antigüedad, los hebreos empleaban técnicas de cifrado sencillas pero muy efectivas, como el Atbash, que consistía básicamente en un método por sustitución simple; es decir, la primera letra del alfabeto hebreo era sustituida por la última, la segunda letra por la penúltima y así sucesivamente. Durante el paso de los siglos, las técnicas de codificación fueron perfeccionándose, y pasaron a formar parte de lo que actualmente conocemos como criptografía clásica; Polybios, Vigenère o Playfair son ejemplos de ella. Sin embargo, la criptografía empleada en la actualidad utiliza técnicas más sofisticadas y se auxilia de la teoría de la información, la teoría de números, el álgebra abstracta, la aritmética modular, la geometría algebraica, las curvas elípticas, entre otras.

El esquema básico de encriptamiento es relativamente sencillo. Primeramente se tiene un texto llamado *plain text* (o texto claro), el cual se somete a un proceso de cifrado (ocultamiento o encriptamiento) mediante la aplicación de un algoritmo, y deja dicho texto ininteligible y se genera además una clave que permita desencriptarlo. Una vez codificado, puede almacenarse o enviarse a algún destinatario sin que exista la posibilidad de ser visualizado y hacer mal uso de su contenido, a menos que conozca la llave correspondiente o aplique algún método de criptoanálisis (descifrar el código sin el uso del algoritmo original); esto último es un trabajo de personas altamente especializadas en seguridad y encriptamiento de datos.

La aplicación de la criptografía es variada y muy útil. La mayoría de las transacciones comerciales y financieras a través de Internet (pago de servicios, adquisición de bienes, renta de vehículos, suscripciones, operaciones bancarias, entre otras) deben cifrar la información considerada como sensible (número de cuenta, tarjetas de crédito o datos personales) antes de ser enviada por algún medio de comunicación. Una vez recibida, se desencripta haciendo uso de una llave y se obtiene el texto original. La razón por la que debe ser cifrada es que dichos medios pueden ser altamente inseguros (como las redes Wi-Fi públicas), ya que alrededor de ellos existe una infinidad de intrusos: *sniffers* (programas que verifican la información que transmiten los distintos dispositivos a través de una red) o *crackers* sedientos de obtener datos que comprometan la identidad y la seguridad del propietario. Sin embargo, encriptar datos no es exclusivo de las comunicaciones, también existen programas que cifran información sensible para el usuario o la organización (documentos, bases de datos e incluso imágenes) y que debe ser almacenada aplicando medidas de seguridad extremas para evitar que la información pueda ser leída en caso de caer en manos de usuarios indeseables.

Otra aplicación de la criptografía es en las contraseñas. Normalmente, las contraseñas de los usuarios, antes de ser almacenadas en su perfil, se encriptan utilizando algoritmos especiales, de tal forma que ni el mismo administrador del sistema operativo sea capaz de visualizarlas, logrando con ello garantizar su confidencialidad.

Así pues, la criptografía, aunque no la vemos de manera directa, es altamente útil para garantizar la seguridad de los datos mientras fluyen a través de un medio de comunicación, o bien para evitar que sean utilizados por usuarios maliciosos.

REFERENCIAS

- Anderson, Ross. (2001). Security engineering: a guide to building dependable distributed systems, 2a edición, Wiley. Tomado de http://www.cl.cam.ac.uk/~rja14/Papers/SE-05.pdf.
- Atanasov, A. (2007). A short primer on cryptography, Harvard University. Tomado de http://www.math.harvard.edu/~nasko/documents/short_primer_on_cryptography.pdf.
- Diffie, W. (1976). New directions in cryptography, Stanford University. Tomado de http://www4.ncsu.edu/~singer/437/proj38.pdf.
- Muñoz, A. (2013). Curso de privacidad y protección de comunicaciones digitales, Universidad Politécnica de Madrid. Tomado de
- http://www.criptored.upm.es/crypt4you/temas/privacidad-proteccion/leccion0/leccion0.html.