LA LLAVE HACIA EL MUNDO MODERNO

Si queremos ocultar el significado de los mensajes, hablamos de criptografía. La criptografía, comenzó a expandirse en España al final del siglo XV, durante el reinado de los Reyes Católicos, los cuales mantenían una correspondencia con términos, sílabas y letras representadas por un número romano. También, una de las máquinas militares más destacada de la era moderna, fue el Modelo G, al servicio de la Alemania Nazi, y que basaba su funcionamiento en estos mensajes ocultos a través de códigos secretos a ojos de los enemigos. Pero sin duda, el gran desarrollo de la criptografía fue con la llegada de los ordenadores. Este hecho se debe a que en el ordenador se necesita una seguridad superior a la de los cifrados clásicos. Sin embargo, los fundamentos de los nuevos criptosistemas siguen siendo números, números binarios principalmente.

Un número binario es una secuencia de bits y cualquier información que se procese en el ordenador, debe transformarse antes en una sucesión de número binarios mediante la asignación de un número a cada dato básico de información, empleando para ello un código. Además, también era necesario que todo tráfico de datos a través de Internet gozase de una mayor seguridad, para así proteger la integridad y autenticidad de la información. El correo electrónico, por ejemplo, llega al destinatario rápidamente pero, para reservarlo de segundas personas, estos mensajes deben ser cifrados, siendo la mejor manera ocultar la información hasta llegar a ser inteligible para todos, excepto para ese destinatario.

En los criptosistemas anteriormente mencionados, se usaba una única clave, tanto para la encriptación, como para la descodificación. La clave pública permite la transmisión del mensaje sin necesidad de enviar las claves. Estos sistemas se denominan asimétricos, ya que las claves son diferentes, pero complementarias. Cada clave descifra el mensaje que la otra cifra, pero no viceversa. Por lo tanto, estamos hablando más exactamente de un clave (clave pública), la cual no tiene un correspondiente concreto, pero la otra es una clave privada, que solo está en manos del destinatario.

Actualmente, los principales algoritmos que se emplean de clave pública son el Diffie-Hellman y el método RSA. Se basan en el hecho de que existen operaciones matemáticas que pueden realizarse en cualquier ordenador, pero, la demanda de tiempo que requiere el procesamiento, lo hace prácticamente imposible sin la autorización debida para poder desencriptarlo. Como vemos, la aplicación de la matemática de los criptogramas, resultará definitiva en un mundo hacia el que avanzamos, en el cual todas las operaciones se realizarán en un medio no físico, sin tener por ello que renunciar a la seguridad y la integridad.

Paula González González.
Estudios: Biología Sanitaria 1º