Criptografía

El término criptografía procede del griego (*kryptos*: oculto; *graphia*: escritura). Ha estado asociado desde el inicio de los tiempos con el arte y la técnica de ocultar información escrita a los ojos no autorizados. Esta es la razón de que la Real Academia Española la defina como el "arte de escribir con clave secreta o de un modo enigmático", lo que inevitablemente conduce a la percepción de la misma como algo antiguo y propio de otros tiempos. Nada más lejos de la realidad, la criptografía ha evolucionado a la par que las técnicas y los métodos para transmitir información. Del mismo modo en que aparece y se desarrolla la Escritura, como respuesta a la necesidad del ser humano para comunicarse entre iguales y dejar testimonio de su existencia, surge la criptografía con el fin de ocultar el contenido de los mensajes, provocado por la desconfianza del remitente, la importancia de la información o la sospecha sobre potenciales interceptaciones.

En sus inicios, las técnicas aplicadas se basaron en la sustitución de unas letras por otras, o por otros símbolos, a veces extraños, con intención de añadir más misterio que dificultad. La historia de la humanidad está llena de ejemplos, entre los que destaca el cifrado del César (s. I a.C.) utilizado por el emperador romano para comunicarse con sus generales. Consistía en la sustitución de cada letra por la que se encontraba desplazada tres lugares en el alfabeto romano de 21 símbolos. Un mecanismo diferente, conocido como Escitala, basado en la permutación de las letras del mensaje, fue utilizado por los guerreros espartanos hasta el 400 a.C. Ejemplos todos de escenarios bélicos que junto con el diplomático lideraron casi en exclusiva la utilización de la criptografía hasta bien entrado el siglo XX. Durante este largo período de la Historia aparecieron cifrados de sustitución más complejos, especialmente en el Renacimiento, que fueron más tarde relevados por máquinas, algunas tan conocidas como la Enigma alemana, durante la Segunda Guerra Mundial y el final de la Guerra Civil Española.

Actualmente, la criptografía se puede considerar una disciplina matemática que permite diseñar sistemas para garantizar, principalmente, la confidencialidad, la integridad, la autenticación y el no repudio de los mensajes, en cualquier sistema, servicio o red de telecomunicación, tanto civil como militar. Los protocolos criptográficos están presentes en los estándares internacionales que regulan todo tipo de comunicaciones. Así lo hicieron con los telegramas de finales del XIX y principios del XX, y así lo continúan haciendo en el s. XXI con las comunicaciones móviles, por satélite, en internet y en todo tipo de transacciones electrónicas, para proteger información de cualquier naturaleza: texto, imagen, audio o video.

Profesor Alberto Peinado. U.M.A.