“Fundamentos de Criptografía”

Seguridad Informática

IDGS 03

Cruz Suarez Osvaldo

¿Qué es la criptografía?

La criptografía es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet. Su utilización es tan antigua como la escritura. Los romanos usaban códigos para ocultar sus proyectos de guerra de aquellos que no debían conocerlos, con el fin de que sólo las personas que conocían el significado de estos códigos descifren el mensaje oculto.

Historia de la criptografía

Eventos mundiales relacionados con la criptografía

La escítala espartana (siglo V a. C.)

Los primeros mensajes cifrados que conocemos datan del siglo V antes de Cristo, de procedencia espartana, que ponían en práctica un método simple y rudimentario que consistía en tomar una vara (llamada escítala), se le enroscaba una cinta de cuero o papiro y posteriormente se escribía de forma longitudinal (como en la imagen).

El cifrador de Polybios (siglo II a. C.)

Este sistema es el primer cifrado por sustitución de caracteres. Se atribuye la invención al historiador griego Polybios y el sistema de cifrado consiste en sustituir un carácter por el número o letra de una columna o fila.

El cifrador del César (siglo I a. C.)

Los romanos hace 2100 años idearon su propio sistema de encriptación que consistía en sustituir cada letra por otro que es el resultado de desplazar tres posiciones hacia la derecha desde el carácter origen en el abecedario.

La cifra Vigenere: Según las memorias de la criptografía, a mediados del siglo XVI, Blaise de Vigenére innovó el cifrado del César. Su método se caracteriza porque posee una clave que a su vez tiene varios valores y utiliza veintiséis cifrados diferentes para traducir cada comunicación.

El enigma nazi

Siguiendo las ruedas de Alberti, a principios del siglo XX se crearon los teletipos con una secuencia de rotores móviles, que giraban con cada tecla que se pulsaba. Parecido a una máquina de escribir, pero, en lugar de la letra ‘golpeada’, aparecía escrita otra escogida por la máquina según diferentes reglas.

El aparato más importante con este sistema es Enigma, creado por el ingeniero alemán Arthur Scherbius.

Turing y el primer ordenador

Los nazis creyeron que Enigma era inviolable y lo fue… hasta que apareció Alan Turing. Durante la Segunda Guerra Mundial, los servicios secretos británicos contrataron a Turing, el matemático que descifró las claves de Enigma y contribuyó a acelerar el fin de la guerra.