15

INTRODUCCIÓN A LA CRIPTOGRAFÍA

Profesor coordinador: Miguel Trejo Malfaz

Francisco Calvo Camacho, Adrián Costales Almarza,

Nicole Herrero del Río, Oscar López Llorente.

IES Alfonso VI

Plaza San Andrés, s/n. 47410 Olmedo (Valladolid)

miguelaguassevilla@yahoo.es

En todo proceso de comunicación intervienen siempre tres elementos principales que son: emisor, receptor y mensaje, este último enviado a través de un canal. Es posible que a veces el mensaje sea interceptado por una tercera persona pudiendo conocer así el contenido del mensaje, situación poco recomendable cuando el mensaje es de carácter comprometido. Para evitar este tipo de amenazas nace la milenaria ciencia de la criptografía, por la cual pueden comunicarse emisor y receptor utilizando como medio un canal que en caso de ser atacado dificulte la lectura del mensaje al estar escrito en un texto cifrado. La criptografía permite realizar un estudio de criptosistemas, definiendo estos matemáticamente como una upla (M , C, K , c , d) donde M denota los mensajes de tamaño n, C el conjunto de los mensajes cifrados, K el conjunto de claves o llaves, c llave de cifrado, d llave de descifrado. El trabajo desarrollado consiste en identificar diversos sistemas de codificación de clave privada, denominados también como sistemas simétricos y de clave pública, denominados también como sistemas asimétricos; e intentar realizar un criptoanálisis para garantizar la seguridad del encriptado buscando los posibles ataques que se puedan hacer a este.

Palabras clave: *criptología, criptografía, criptosistemas, clave.*