NÚMEROS
Revista de didáctica de las matemáticas
N° 30, junio de 1997, págs. 15-30

Sistemas criptográficos de sustitución

Carlos Bruno Castañeda y Pino Caballero Gil

Se denomina **Criptografía** al *arte de escribir mensajes en clave secreta o enigmáticamente* [1]. El desarrollo de la criptografía, que en occidente está documentado desde la Grecia clásica, viene asociado a la comunicación en los entornos de poder, políticos o militares. Se denomina Criptografía clásica a todas aquellas técnicas criptográficas anteriores a la mitad de este siglo [4]. Entonces, la criptografía empezó a ser considerada como una ciencia aplicada, debido a su relación con ciencias como la estadística, la teoría de números o la teoría de la información. En la actualidad, su uso, debido a lo generalización de medios informáticos y telemáticos, adquiere nuevos aspectos que sobrepasan la pura confidencialidad de mensajes intercambiados entre dos comunicantes. Este salto tecnológico ha llevado a desarrollar nuevos, ingeniosos y sofisticados sistemas que permiten mantener al ojo no autorizado, lejos de la lectura de la información que únicamente desean compartir los ojos sí autorizados. Tanto los métodos clásicos como los actuales, mantienen una estrecha relación con las matemáticas. De hecho, tanto el diseño de un sistema como la medida de su efectividad se pueden realizar en términos matemáticos.

En este trabajo nos ocuparemos de describir el sustrato matemático que poseen algunos sistemas criptográficos clásicos. En estos sistemas, además de contar con material manipulativo de fácil construcción, se manejan conceptos que creemos pueden servir como situación problemática adecuada para desarrollar conceptos matemáticos que están incluidos en nuestros currículos de las distintas etapas de secundaria.

Comunicación y criptografía

La comunicación es una actividad que implica a dos partes y un medio. Si dos comunicantes desconfían de la confidencialidad de su medio de comunicación pueden recurrir al uso de sistemas criptográficos. Un sistema criptográfico es elegido de mutuo acuerdo por ambos. Cualquier mensaje se verá transformado por dicho sistema, de manera