1 Introducción

La comunicación es una actividad indispensable del quehacer cotidiano del hombre. Mucha información es día a día transmitida por diversos medios, almacenada de diversas formas, y está expuesta a ser interceptada o robada por personas que no deberían obtener esa información. Si la información es trivial puede no importar que otras personas tengan acceso a ella, sin embargo en muchas ocasiones se desea tener una comunicación segura y que sólo la persona a la que la información está dirigida tenga acceso a ella.

A lo largo de la historia se han creado métodos para proteger información importante. Se sabe que los griegos, y tiempo después los romanos utilizaban métodos de sustitución de letras para proteger los mensajes que enviaban en la guerra. En la edad media se desarrollaron más métodos para ocultar mensajes, y se iniciaron a desarrollar métodos para descifrar mensajes ocultos.

La criptografía moderna nace al mismo tiempo que las computadoras. Durante la Segunda Guerra Mundial, en un lugar llamado Bletchley Park, un grupo de científicos entre los que se encontraba Alan Turing, trabajaba en el proyecto ULTRA tratando de descifrar los mensajes enviados por el ejército alemán con el más sofisticado ingenio de codificación ideado hasta entonces: la máquina ENIGMA [1]. Este grupo de científicos empleaba el que hoy se considera el primer computador aunque esta información permaneció en secreto hasta mediados de los 70.

Al terminar la Segunda Guerra Mundial, se tiene un avance significativo con el trabajo de Claude E. Shannon sobre teoría de información donde sienta las bases teóricas de las comunicaciones seguras. Desde entonces hasta hoy ha habido un crecimiento espectacular de la tecnología criptográfica, si bien la mayor parte de estos avances se mantenían y se siguen manteniendo, según algunos, en secreto [1]. Financiadas fundamentalmente por la

NSA (Agencia Nacional de Seguridad de los EE.UU.), la mayor parte de las investigaciones hasta hace relativamente poco tiempo han sido tratadas como secretos militares. Sin embargo en los últimos años, investigaciones serias llevadas a cabo en universidades de todo el mundo han logrado que la criptografía sea una ciencia al alcance de todos, y que se convierta en la piedra angular de asuntos tan importantes como el comercio en Internet, operaciones bancarias, llamadas telefónicas seguras, en los accesos a redes que manejen información personal, etc.

La mayoría de las técnicas criptográficas han sido aplicadas sobre información discreta: secuencias de bits, alfabetos, etc. Sin embargo, existen técnicas que se aplican directamente sobre señales de información, las cuales no han sido tan desarrolladas como aquellas aplicadas sobre señales discretas.

En 1990, Pecora y Caroll descubren la posibilidad de sincronizar los estados de dos osciladores caóticos distantes y en base a ese hecho crean un sistema de encripción que se basa en esconder la señal de información dentro del ruido determinístisco que representa el caos. A partir del trabajo de Pecora y Caroll se desarrolla el área de comunicaciones basadas en caos.