Criptografia robusta basada en Caos.

Marcos Daniel Calderón Calderón
Maestría en Ciencias de la Computación
Centro de Investigación en Matemáticas (CIMAT)
Guanajuato , Gto.
marcos.calderon@cimat.mx

***Resumen*—Resumen de la tesis "Criptografía robusta basada en caos"**

I. INTRODUCCIÓN

A través de la historia, el ser humano se ha visto en la necesidad de sistemas que le permiten el uso de mensajes secretos con fines comerciales, religiosos, militares e incluso en algunas ocaciones, a nivel persona. Desde tiempos arcaicos el hombre ha usado su perspicacia para proteger sus comunicaciones. Se dice que la Criptografía (del griego *krypto*, "oculto", y *graphos* "escritura", literalmente "escritura oculta"), nació de la mano de la escritura. Sus primeros vestigios pueden encontrarse en las tablas cunciformes, y los papiros demuestran que egipcios, hebreos, babilonios y aisirios poseían técnicas criptográficas.

En el caso de los antiguos egipcios, el pueblo empleaba la escritura demótica (del griego *demotika* "popular", que hacía referencia a los asuntos cotidianos), mientras que los sacerdotes usaban la escritura herática (del griego *hieratica* "sacerdotal"), la primera era sólo una forma abreviada de la lengua hierática. Técnicas criptográficas, también estuvieron presentes en la escritura cuneiforme de los babilonios.

Los hebreos no se quedan atrás en el desarrollo de métodos de cifrado. Atbash, Albam y Atbah son tres sistemas de cifrado hebraicos que datan de 600 a 500 a. C., y eran usadas principalmente en textos religiosos. Escribas hebreos usaron el sistema Atbash para escribir el libro de Jeremias. Estas tres técnicas tratan de una forma de crifrado por sustitución simple (o mono-alfabética, haciendo referencia al uso de un alfabeto), también suele denominárseles por sistemas reversibles ya que en la primer operación se obtiene el texto cifrado y al aplicar nuevamente la operación sobre el texto cifrado, se obtiene el texto original. EL funcionamiento de estos métodos de cifrado es el siguiente:

1. ATBASH. Si una palabra está escrita en alfabeto hebreo, entonces, se puede encriptar intercambiando las letras de la siguiente manera: La primera letra del alfabeto es intercambiada por la última letra, la segunda letra del alfabeto es intercambiada por la penúltima, la tercera con la antepenúltima y así sucesivamente.
2. ALBAM. En este método, cada letra del alfabeto hebreo es desplazada trece posiciones.

II. CIFRADO MULTIMEDIA BASADO EN CAOS

Antedecentes del cifrado multimedia.

En las últimas décadas, se ha propuesto algoritmos de cifrado basados en caos, esto ha ocurrido así porque estos algoritmos ofrecen velocidad y seguridad.

Además, los algoritmos de cifrado como IDEA, AES, DES, RSA no son adecuados para el cifrado de algunos datos multimedia en tiempo real, tales como imágenes y video, entre otros, ya que estos cifraqdos requieren gran tiempo de cómputo y alta potencia computacional. Para el cifrado de datos digitales en tiempo real sólo son preferibles los esquemas de cifrado que demandan menor cantidad de tiempo sin comprometer la seguridad. Un esquema de cirfrado que funciona lentamente, que incluso puede tener mayor grado de seguridad sería de poca utilidad práctica para los procesos en tiempo real. Hoy en día se requiere el procesamiento de grandes cantidades de información que viajan a una gran velocidad. Las características de los mapas caóticos han atraído la atención de los criptógrafos para desarrollar nuevos algoritmos de cifrado. Dado que estos mapas caóticos tienen abundantes propiedades fundamenteales tales como ergodicidad, propiedad de mezcla y sensibilidad a las condiciones iniciales y parámetros del sistema y que pueden considerarse análogtas a algunas de las propiedades criptográficas ideales como confusión, difusión, balance y propiedad de avalancha.

Esquemas de cifrado basado en caos.

Desde la demostración de la posibilidad de autosincronización de oscilaciones caóticas, una gran cantidad de trabajo en la aplicación de caos a la criptografía se ha desarrollado en la última década. Los primeros trabajos en caos para criptografía fueron conectados con el cifrado de mensajes a través de la modulación de órbitas caóticos de sistemas dinámicoscontinuos en el tiempo. Muchos esquemas han sido propuestos, en maneras distintas, para lograr la sincronización de sistemas caóticos mediante la transmisión de información en una señal caótica portadora. A pesar de la idea y el hecho de que se pueden obtener muchos esquemas de comunicación seguros basdados en el uso del principio de sincronización de caos, todos ellos sufren de alguna debilidad común. Las principales dificultades son:

- Es difícil determinar el tiempo de sincronización; por lo que, los mensajes durante el periodo de transición pueden perderse, y el problema es que el tiempo de transición puede ser muy largo en ocasiones.

- EL ruido a través del canal de comunicación puede afectar significativamente el intento de sincronización. Esto significa que el nivel de intensidad del ruido debe ser inferior al nivel de la señal, o la sincornización deseada no podrá alcanzarse.
- Técnicamente, son difíciles de implementar dos sistemas caóticos bien sincronizados, y si esto no es requerido, entonces el oponente puede fácilmente obtener la misma sincronización para atacar.

En constraste a las técnicas basadas en sincronización, una aplicación directa de una transformación caótica a texto planto, o la aplicación de señales caóticas en el diseño de un algoritmo de cifrado, parece ser un desarrollo más prometedor. La sensibilidad a condiciones y parámetros iniciales así como las características de aleatoriedad del caos, son muy deseables en criptosistemas. Una diferencia importante a notar es que los criptosistemas oepran en un conjunto finito de enteros, mientras que los mapas caóticos están definidos en un conjunto infinito de números reales. Entonces, cómo combinar estas dos clases de sistemas, de modo que se pueda tomer ventaja de las buenas propiedades del caos, es un tema de exploración futura.

Un sistema de cifrado basado en caos discreto consiste en un generador digital de caos (mapa dinámico no lineal), que toma un mensaje de entrada conocido como texto plano y produce un mensaje de salida oculto (enmascarado) independiente llamado texto cifrado. Los sistemas dinámicos caóticos digitales fueron propuestos a finales de los años 80's como una alternativa viable en la comunicación de datos seguros. Aunque una gran cantidad de investigadores han hecho publicaciones basadas en ello algunos esquemas han resultado débiles y recientemente ha sido rotos.

Aspectos básicos del caos.

Recordemos que un sistema dinámicos es determinista en el sentido de que la evolución del sistema es descrita por un mapa específico, de forma que el presente determina completamente el futuro. Un sistema caótico presenta tanto el comportamiento de un sistema estable como el de un sistema inestable. Se dice que un sistema estable tiende a lo largo del tiempo hacia un punto u órbita, según su dimensión (atractor o sumidero), y que un sistema inestable se escapa de los atractores.

Caos y el mapa logístico.

El mapa logístico ilustra la complejidad del comportamiento caótico que puede surgir en ecuaciones dinámicas no lineales muy sencillas. Un modelo sencillo de mapa caótico que representa a grupos de población es el siguiente:

$$x_{n+1} = \lambda x_n(1 - x_n)$$

donde x_n es un número entre 0 y 1, y representa la población del año n (X_0 representa la población inicial), λ es el período biótico, un número positivbo que representa la tasa combinada para reproducción e inanición