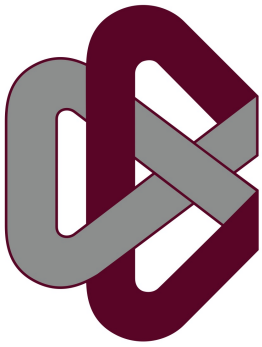

CIMAT

Centro de Investigación en Matemáticas A. C.

ALGORITMOS DE CIFRADO DE DATOS

TESIS

que para obtener el grado de

Maestría en Ciencias con Especialidad en Computación y Matemáticas Industriales

presenta

Marcos Daniel Calderón Calderón

Director de Tesis

Rogelio Hasimoto Beltrán

Capítulo 1

0.1 Introducción

Se dice que un mapa f que está definido en el intervalo $I = [\alpha, beta]$ es caótico si se cumplen las siguientes condiciones:

1. Los puntos periódicos de f son densos en I.
2. f es una función transitiva en el intervalo I, esto significa que, dados dos subintervalos cualesquiera U_1 y U_2 en I, hay un punto $x_0 \in U_1$y un $n > 0$ tal que $f^n(x_0 \in U_2)$.

Capítulo 2

0.2 Caos

Se dice que un mapa f que está definido en el intervalo $I = [\alpha, beta]$ es caótico si se cumplen las siguientes condiciones:

1. Los puntos periódicos de f son densos en I.
2. f es una función transitiva en el intervalo I, esto significa que, dados dos subintervalos cualesquiera U_1 y U_2 en I, hay un punto $x_0 \in U_1$y un $n > 0$ tal que $f^n(x_0) \in U_2$.
3. f tiene dependencia a las condiciones iniciales en I; esto significa que hay una constante de sensibilidad β tal que para cualquier $x_o \in I$ y cualquier intervalo abierto U sobre x_0, hay alguna semilla $y_o \in U$ Y $n > 0$ tal que

$$|f^n(x_0) - f^n(y_0)| > \beta. \tag{1}$$

Anexos

Prueba de la Frecuencia

La prueba consiste en medir la proporción de ceros y unos de la secuencia analizada. Se busca determinar si el número de ceros y unos en una secuencia es aproximadamente el mismo como debería ser para una secuencia verdaderamente aleatoria. La prueba evalúa que la fracción de unos se acerce a $\frac{1}{2}$. Es importante recordar que todas las pruebas subsecuentes dependen del resultado de esta prueba.

Prueba de la Frecuencia por Bloques

Esta prueba mide la proporción de unos en un bloque de M bits, se busca determinar si la frecuencia de unos en el bloque es aproximadamente de $\frac{M}{2}$, que es el resultado esperado bajo la suposición de aleatoriedad.

Prueba de las Corridas

La proueba mide el número total de corridas en la secuencia, donde una corrida es una secuencia nininterrumpida de bits idénticos. Una corrida de longitud k consiste de k bits idénticos que está reada al inicio y al final con un bit del valor opuesto. Con esta prueba se busca demostrar si el número de coridad de ceros y unos de diversas longitudes es el que se espera para una secuencia aleatoria.

Prueba de la Frecuencia

Prueba de la Frecuencia

Prueba de la Frecuencia

Prueba de la Frecuencia

Prueba de la Frecuencia