Mapa Caótico Renyi y su aplicación a algoritmos de cifrado de datos.

Marcos Daniel C. Calderón
Seminario de Avance de Tesis - CIMAT
Asesor: Dr. Rogelio Hasimoto Beltrán

31 de enero de 2014

Objetivo.

La finalidad de este trabajo es encontrar nuevos métodos de cifrado de datos por medio de mapas caóticos acoplados. Se buscan nuevas alternativas que ofrezcan una mayor resistencia a ataques y donde se aprovechen los beneficios de los sistemas caóticos. Los resultados obtenidos se aplicarán al cifrado de imágenes.

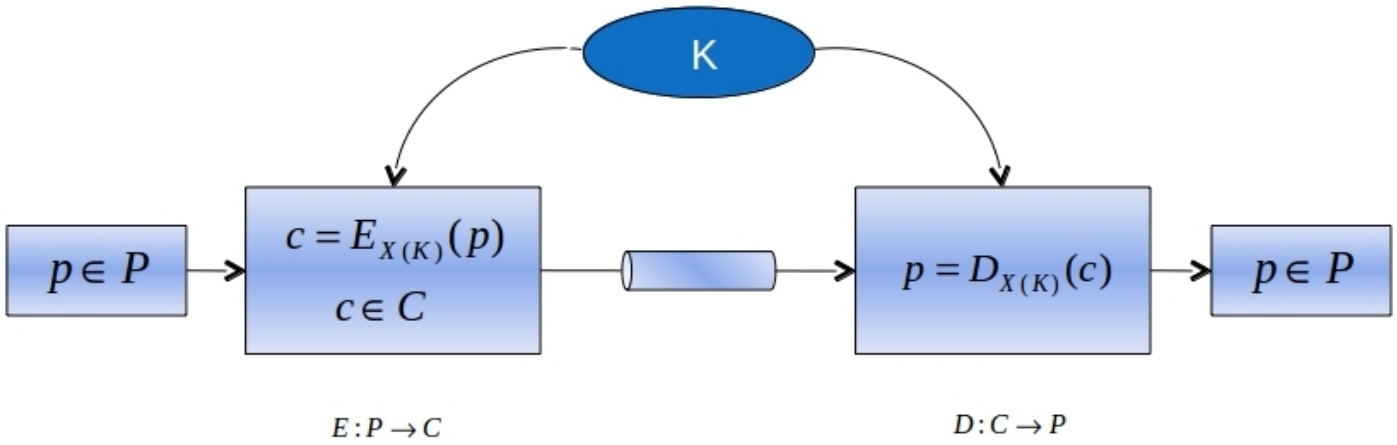
Sistema de cifrado.

Definición.

Un sistema criptográfico es una quíntupla $(\mathbf{P}, \mathbf{C}, \mathbf{K}, \mathbf{E}, \mathbf{D})$, donde se satisfacen las siguientes condiciones:

- $\mathbf{P}$ es un conjunto finito de símbolos que forman un texto "original".
- $\mathbf{C}$ es un conjunto finito de símbolos que forman un texto cifrado.
- $\mathbf{K}$ es un conjunto finito de posibles claves.
- Por cada $k \in \mathbf{K}$ existen funciones $e_k \in \mathbf{E}$ y $d_k \in \mathbf{D}$, donde cada $e_k : \mathbf{P} \to \mathbf{C}$ y $d_K : \mathbf{C} \to \mathbf{P}$ son funciones que cumplen $d_K(e_K(x)) = x$ para cada elemento del texto original $x \in \mathbf{P}$.

Esquema de cifrado.



Números aleatorios y pseudoaleatorios.

Definición.

Un ***generador aleatorio de bits*** es un dispositivo o algoritmo que produce una secuencia de dígitos binarios estadísticamente independientes y uniformemente distribuidos.

Definición.

Un ***generador pseudoaleatorio de bits*** es un algoritmo determinístico que, dada una secuencia binaria verdaderamente aleatoria; normalmente conocida como "semilla", genera múltiples bits pseudoaletorios que "parecen" ser al azar. Estos algoritmos se utilizan en la generación de claves.

Sistema dinámico caótico.

Definición.

Un ***sistema dinámico caótico*** se caracteriza por tener un comportamiento en el tiempo complejo e impredecible. Normalmente, estos sistemas están representados por un grupo de ecuaciones diferenciales o discretas.

Sistema dinámico caótico.
Características.

Propiedad caótica	Propiedad Criptográfica
Ergodicidad.	Confusión.
Sensibilidad a las condiciones iniciales.	Hay difusión con un pequeño cambio en el texto plano o llave secreta.
Propiedad de mezclado.	Hay difusión con un pequeño cambio en un bloque del texto plano, o un cambio en la totalidad del mismo.
Dinámica determinística.	Pseudoaleatoriedad determinística.
Estructura compleja.	Complejidad para atacar un algoritmo.

Generador Caótico de Números Pseudoaleatorios Renyi...

Consideremos el mapa caótico Renyi $\phi_\beta(x) : [0,1) \longrightarrow [0,1)$ definido como:

$$\phi_\beta(x) = (\beta \cdot x) \quad \text{mód } 1 \tag{1}$$

Además, la siguiente expresión nos devolverá números en el intervalo $[0,1)$:

$$\hat{x} \in \mathbf{Q} : \hat{x} = \frac{k}{2^n}, \quad k \in \mathbf{N}, \quad k < 2^n \tag{2}$$

Generador Caótico de Números Pseudoaleatorios Renyi...

Una aproximaxión de truncamiento es considerada para la evaluación de $\hat{x}$ en $\phi_\beta(x)$:

$$\hat{\phi}_\beta(\hat{x}) = (\beta \cdot \hat{x})_{tr} \quad \text{mód } 1 = \lfloor (2^n \cdot \beta \cdot \hat{x}) \quad \text{mód } 2^n \rfloor \cdot 2^{-n} \tag{3}$$

Por medio del isomorfismo $k = \hat{x} \cdot 2^n$, el espacio definido en la ecuación (2) puede ser relacionado con un conjunto de números naturales:

$$\Lambda_n = k \in \mathbf{N}, \quad 0 \leq k < 2^n \tag{4}$$

Generador Caótico de Números Pseudoaleatorios Renyi...

Podemos definir una función $f : \Lambda_n \longrightarrow \Lambda_n$ así:

$$f(k) = 2^n \hat{\phi}_\beta(2^{-n}k) = \lfloor \beta \cdot k \mod 2^n \rfloor = \lfloor \beta \cdot k \rfloor \mod 2^n \quad (5)$$

El parámetro β puede ser escrito como la suma de una parte entera b y una fracción γ, por lo tanto, (5) puede ser escrito así:

$$f(k) = (bk + \lfloor \gamma \cdot k \rfloor) \mod 2^n \quad (6)$$

Generador Caótico de Números Pseudoaleatorios Renyi.

La parte fraccional de la ecuación (6) puede ser escrita como: $\gamma = 2^{-j}$ para algún entero $j > 0$. Por lo tanto, obtenemos la expresión final del mapa caótico Renyi:

$$f(k) = \left(q2^{n-i}k + \lfloor \frac{k}{2^j} \rfloor \right) \quad \text{mód } 2^n. \tag{7}$$

Sistemas caóticos acoplados.

Acoplamiento.

Este fenómeno ocurre cuando dos sistemas dinámicos interactúan entre sí. Por ejemplo:

$$C' = \alpha C - \beta C Z \tag{8}$$

$$Z' = -\gamma Z + \delta C Z \tag{9}$$

Se dice que el sistema es acoplado porque las razones de cambio de C y Z dependen tanto de C como de Z.

Ejemplo: Redes de Mapas.

$$X_{i,j} = (1-\epsilon) f(X_{i,j-1}) + \epsilon H(X_{1,j-1}, ..., X_{N,j-1}) \qquad (10)$$

- La interacción entre diferentes mapas provoca en un sistema caótico, ciclos de mayor tamaño: H representa una transformación de acoplamiento.
- Aparece el fenómeno de sincronización, que consiste en un régimen en el cual los sistemas caóticos acoplados, después de un tiempo de transición, exhiben oscilaciones caóticas idénticas.

Pruebas de aleatoriedad.

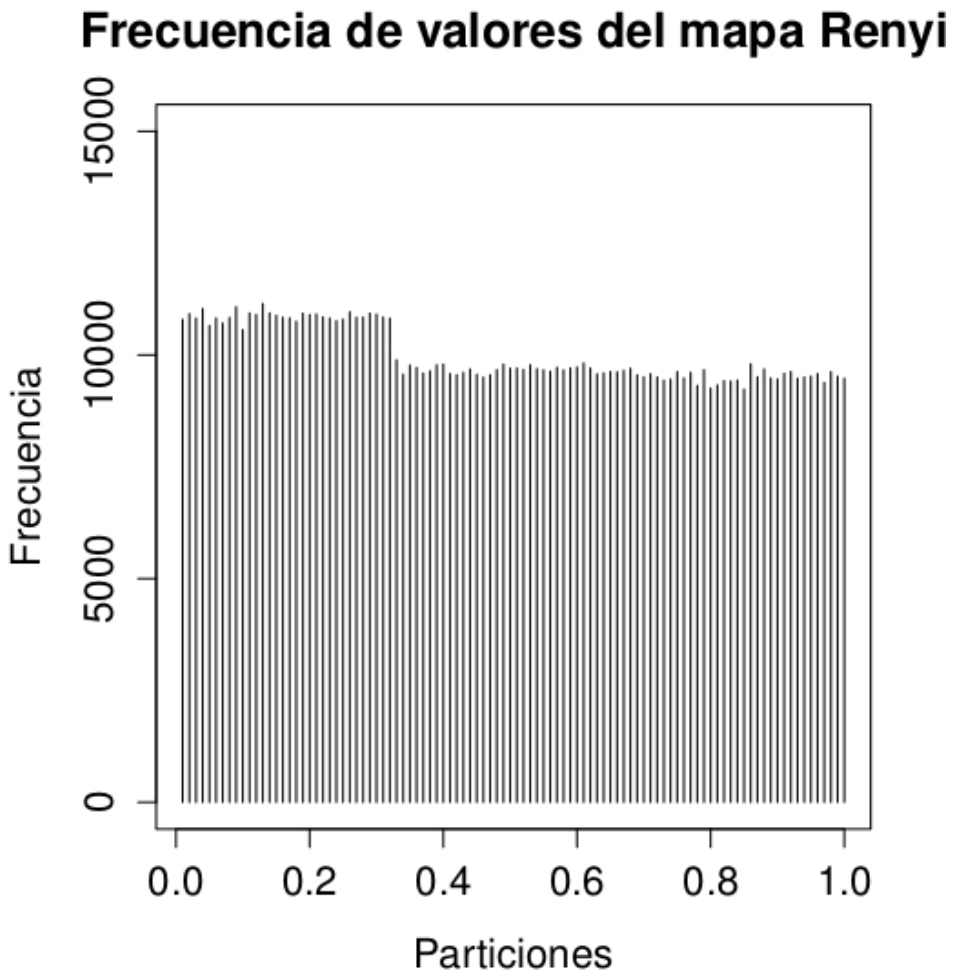
- En una prueba de aleatoriedad, se establece como falsa a priori, una Hipótesis nula: "Los símbolos analizados son independientes entre sí y uniformemente distribuídos". Lo que se busca es evaluar el grado de aleatoriedad de la secuencia para validar la Hipótesis nula.
- **NIST** es un paquete de 16 exámenes estadísticos, se han desarrollado para probar la aleatoriedad de una secuencia de bits producida por un generador de números pseudoaleatorio o aleatorio.

Pruebas NIST mapa Renyi.

Resultados obtenidos.

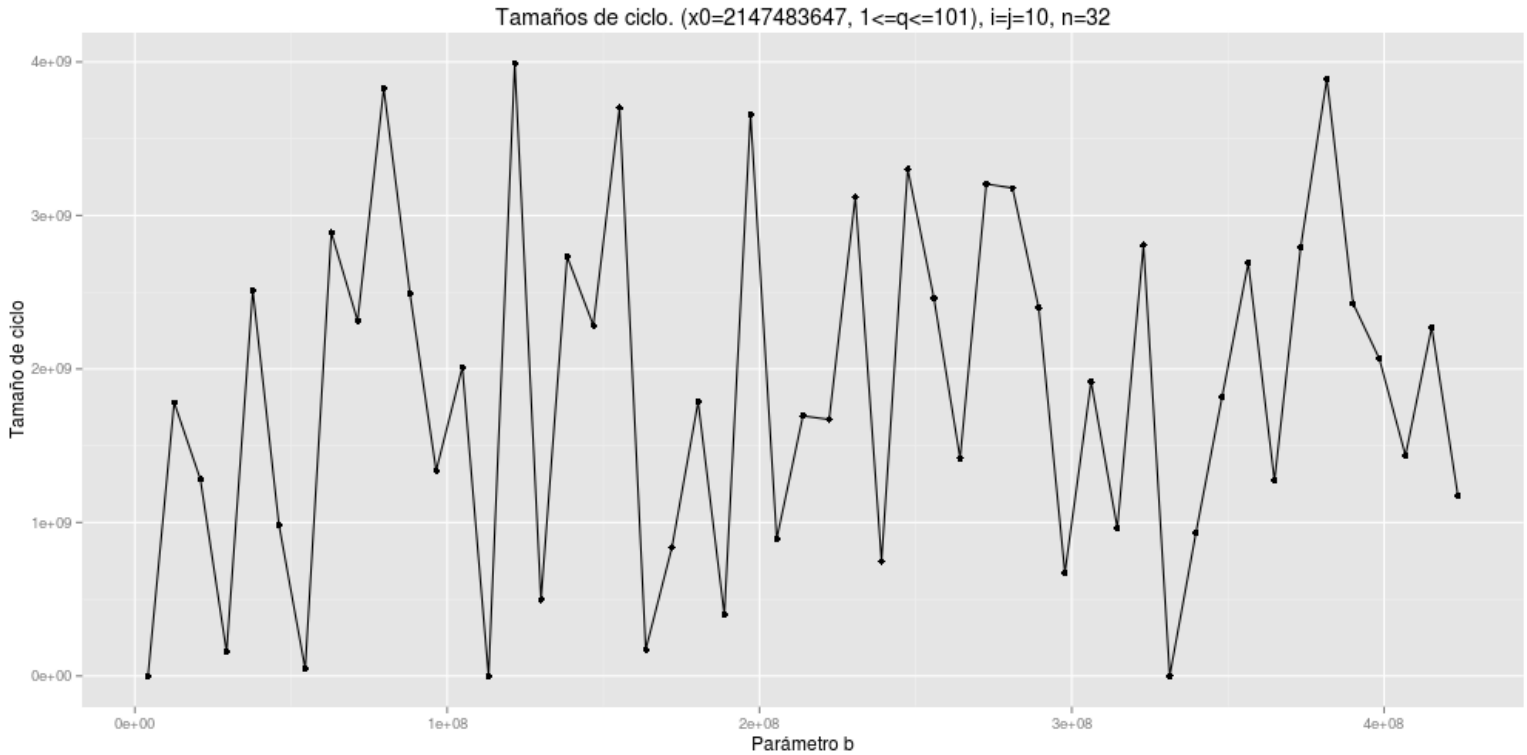
Prueba Aplicada	P-Valor	Exito?
Aproximate Entropy	0.303647	√
Block Frecuency	0.450408	√
Cumulative Sums	Forward test: 0.777054, Reverse test: 0.671857	√
FFT	0.617327	√
Frecuency	0.820988	√
Linear Complexity	0.784292	√
Longest Run	0.795471	√
Non Overlapping Template	P-valores aceptados: 148 de 148	√
Overlapping Template	0.642080	√
Random Excursions	P-valores aceptados: 8 de 8	√
Random Excursions Variant	P-valores aceptados: 18 de 18	√
Rank	0.707380	√
Runs	0.265730	√
Serial	P-valores aceptados: 2 de 2	√
Universal	0.696176	√

Comportamiento.



Tamaños de ciclo.

También es importante obtener secuencias de números pseudoaleatorios donde el tamaño de un ciclo sea muy grande.



Conclusiones.

1. Los sistemas dinámicos caóticos presentan características que se pueden aplicar en algoritmos de cifrado de datos.
2. Con las pruebas de aleatoriedad realizadas a las secuencias de bits obtenidas con el mapa caótico Renyi, se puede concluir que éste se comporta de manera adecuada para su uso en cifrado de datos.
3. Todavía se buscan métodos de cifrado que utilicen mapas caóticos acoplados con una sincronización adecuada.

Calendario de Actividades.

	Planeación							
	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto
Lectura de artículos y libros	■	■	■	■	■			
Codificación y pruebas		■	■	■	■	■		
Escritura			■	■	■	■	■	
Revisiones y presentación							■	■

Gracias.