Análisis del Generador Renyi Map.

Marcos Daniel Calderón Calderón

Abstract

Se explican algunas generalidades del método de Renyi Map. Y se dan algunos resultados de su rendimiento.

1. Introducción.

Un paso importante en cualquier sistema de encriptacion caótica es la selección del mapa. Los mapas caóticos tienen diferentes comportamientos en complejidad, propiedades, sensibilidad a las condiciones iniciales, reacción a las perturbaciones aplicadas. Es deseable tener alguna independencia entre el criptosistema y el mapa caótico.

El generador no Lineal conocido como Renyi Map tiene la siguente forma:

$$\begin{aligned} f(k) = 2^n \tilde{\phi}_\beta(2^{-n}k) &= \lfloor \beta \cdot k \mod 2^n \rfloor \\ &= \lfloor \beta \cdot k \rfloor \mod 2^n. \end{aligned} \tag{1}$$

Otra forma de ver la expresión anterior es de la siguiente manera:

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

Los mapas que se generan por medio del Método de Renyi Map, se aplican en Criptografía de la siguiente manera:

$$X_n = f(X_{n-1}) = \lfloor \lambda \cdot X_{n-1} \rfloor \quad \text{mód } 2^{PR} \tag{3}$$

donde $1 < \lambda \in \mathbf{R}$ y $X \in 1, 2, ..., 2^{PR} - 1$. La expresión anterior puede ser implementado utilizando aritmética de enteros, solo se necesita una multiplicación, una suma y una operación de desplazamiento a la derecha. Un total de $PR \cdot 2^{PR}$ mapas diferentes son definidos en la ecuacion anterior. Con un periodo máximo de $2^{PR} - 1$.

2. Generadores de números pseudoaleatorios.

Los generadores de números pseudoaleatorios se utilizan para generar imitaciones de variables que tienen una distribución uiniforme sobre el intervalo (0,1)

Email address: marcos.calderon@cimat.mx (Marcos Daniel Calderón Calderón)

3. Algunos conceptos importantes del lenguaje C.

1. **unsigned long** Es un tipo de dato utilizado en C, es una variable para almacenar números en 32 bits (4 bytes). Por el contrario que las variables long estándar, las unsigned long no almacenan números negativos, haciendo que su rango sea de 0 a 4,294,967,295 ($2^{32} - 1$).
2. **Máscaras.** Son secuencias de bits que tienen la finalidad de ocultar o mostrar bits específicos de otra secuencia de bits. Esto se logra al aplicar un operador lógico a la máscara con la secuencia original.
3. **Hexadecimales en C.** La representación de Hexadecimales en C se realiza al anteponer los caracteres "0x" al número que estará en Hexadecimal.
4. **Operacion módulo en bits.** A la hora de utilizar esta operación en generación de números pseudoaleatorios, se utiliza la operación lógica de & con una máscara de bits.

4. Demostraciones.

Dado $\beta_0 = b_0 + \gamma_0 > 1$, existe un conjunto contable infinito de valores racionales $\beta > 1$, tal que $\forall k \in A_n \ \lfloor \beta_o k \rfloor \mod 2^n = \beta k \rfloor \mod 2^n$ en este caso b_0 es un entero, y γ_0 es una fracción, ademas, $(A_n = k \in \mathbf{N}, 0 \leq k \leq 2^n)$,

5. Resultados.

A continuación se muestran algunos resultados acerca del comportamiento del Generador Renyi Map, se muestran los parámetros que se han utilizado y también en qué momento se ha encontrado un ciclo.

5.1. Ejemplo 1. Elegir el valor del parámetro de manera arbitaria.

En este ejemplo se eligió el valor del parámetro β de una manera arbitraria, esto significa que no se siguieron los criterios definidos por [1] para obtener un buen tamaño de ciclo, también se eligió el valor de $j = 15$. Los resultados obtenidos se muestran en la gráfica y en la tabla siguiente.

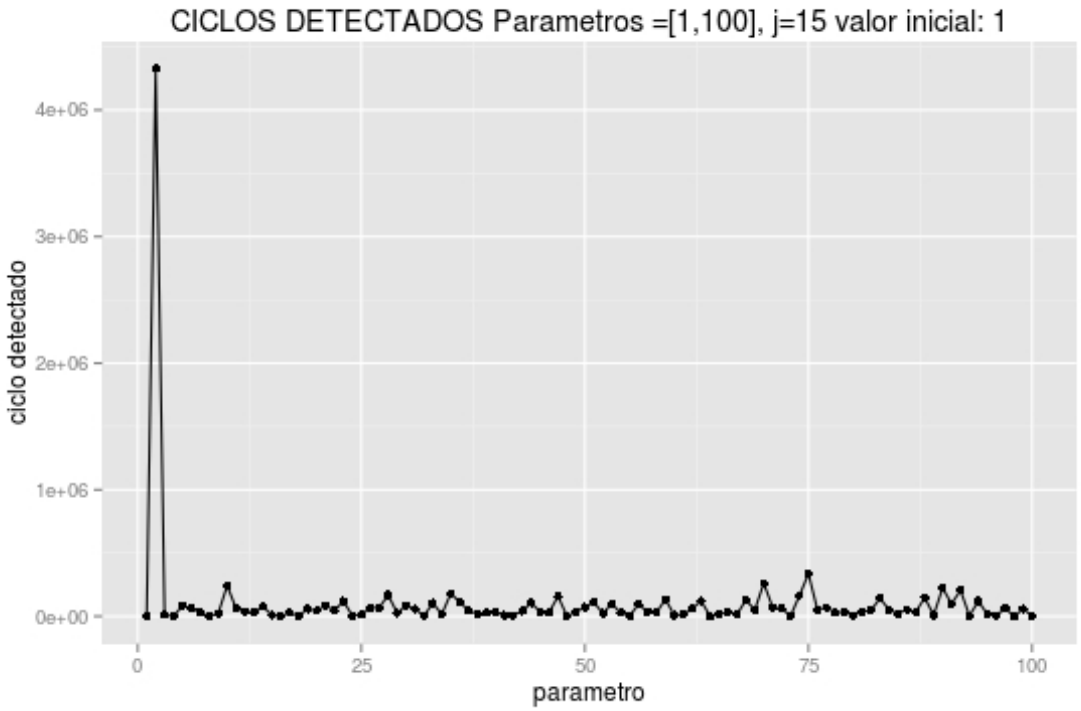

Figura 1: Gráfica de Ciclos con Parámetros arbitrarios para β.

5.2. Ejemplo 2. Parámetros dados por [1]: $n = 15$, $i = j = 14$, $q = [501, 701]$, .

En este ejemplo, el rango de q es de 501 a 701, pero solo se toman los valores impares. Los resultados obtenidos fueron los siguientes.

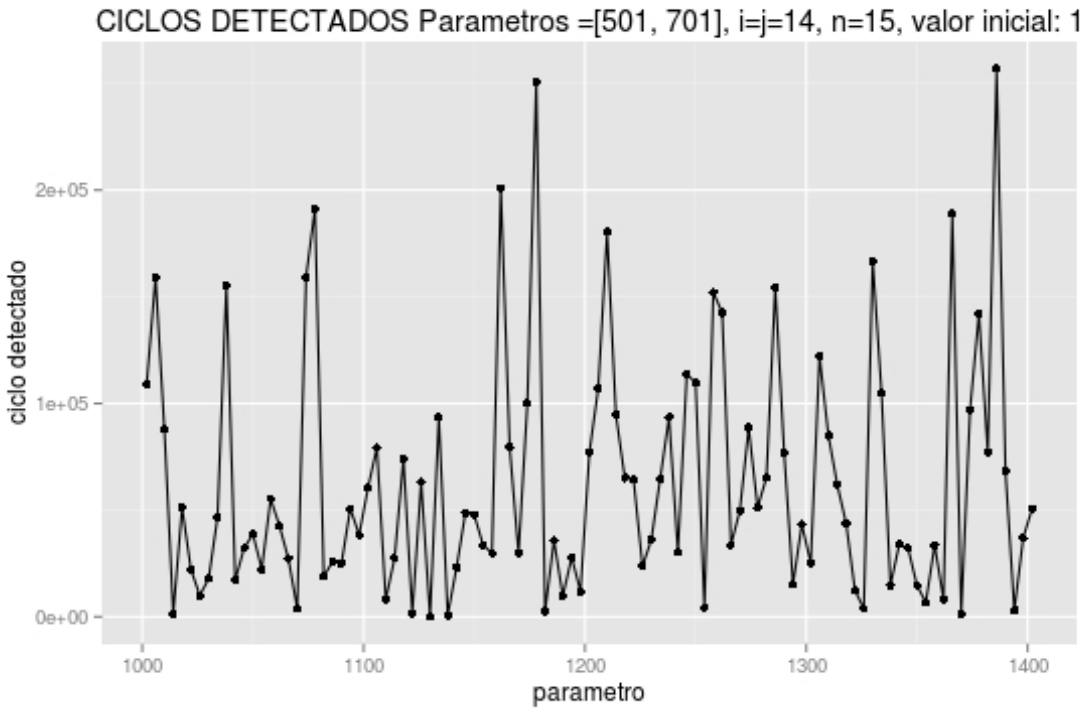

Figura 2: Gráfica de Ciclos con las especificaciones: $n = 15$, $i = j = 14$, $q = [501, 701]$.

Como se puede ver en la gráfica anterior, el tamaño promedio del ciclo depende mucho de las especificaciones dadas, al especificar $n = 15$, el tamaño del ciclo disminuye. A continuación, vamos a ver una gráfica de ciclos con $n = 32$.

5.3. Ejemplo 3. Se especificaron los siguientes parámetros: $n = 32$, $i = j = 15$, $q = [1, 1001]$.

En este ejemplo, el rango de q es de 1 a 1001, pero solo se toman los valores impares. Los resultados obtenidos fueron los siguientes.

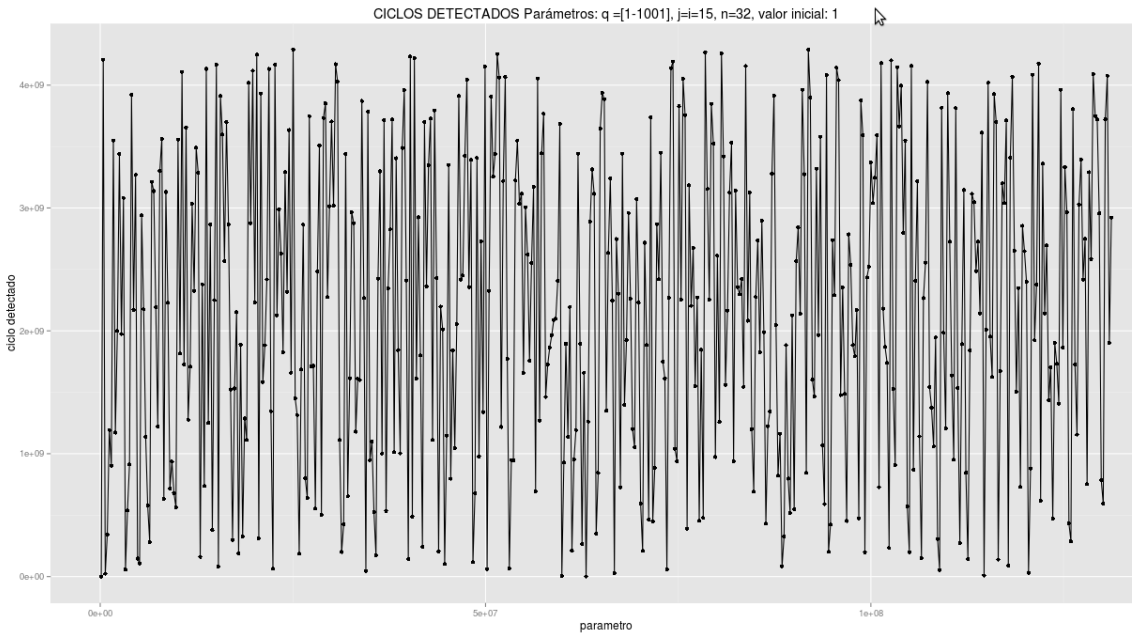

Figura 3: Gráfica de Ciclos con las especificaciones: $n = 32$, $i = j = 15$, $q = [1, 1001]$.

Se puede ver que el tamaño de los ciclos ha aumetado de manera considerable, sin embargo, para mayor claridad mostramos una gráfica donde solo se muestran los resultados de $q = [1, 101]$, el rango corresponde a 50 parámetros por la restricción de que sólo se toman valores impares para q.

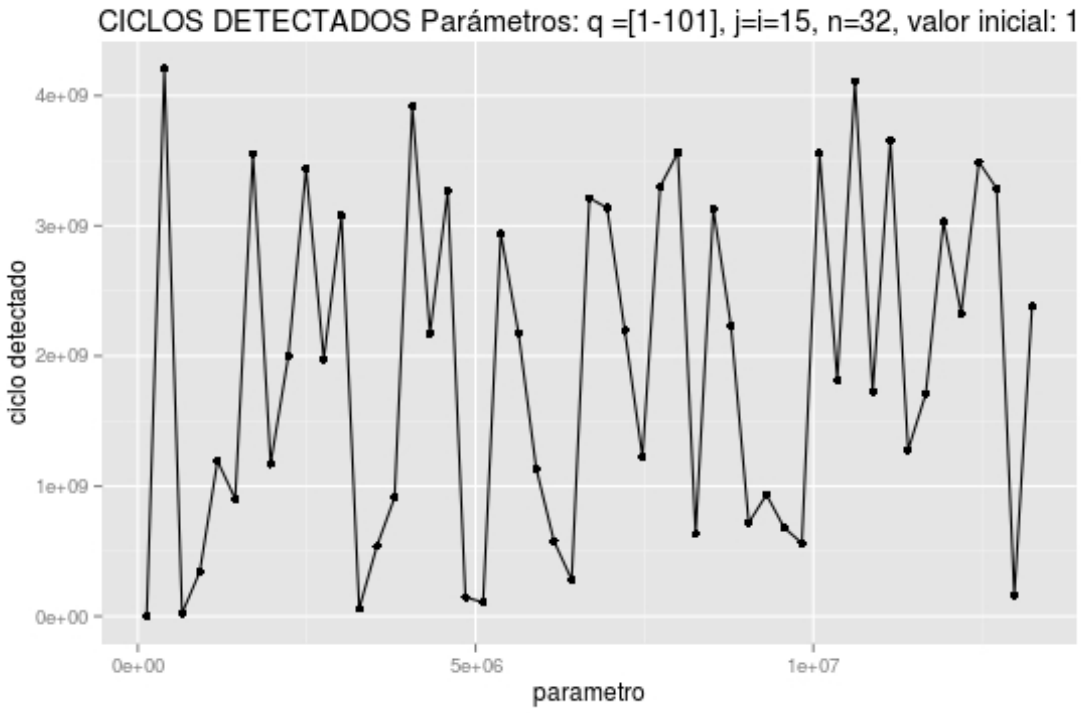

Figura 4: Gráfica de Ciclos con las especificaciones: $n = 32$, $i = j = 15$, $q = [1, 101]$.

5.4. Ejemplo 4.

En este ejemplo, el valor de q es de 1 a 101, pero solo se toman los valores impares. También, a comparación del ejemplo anterior, se ha cambiado el valor de i y j. Las especificaciones utilizadas son las siquientes: $n = 32$, $i = j = 10$, $q = [1, 101]$. La gráfica de resultados muestra que se obtuvieron tamaños de ciclo grandes.

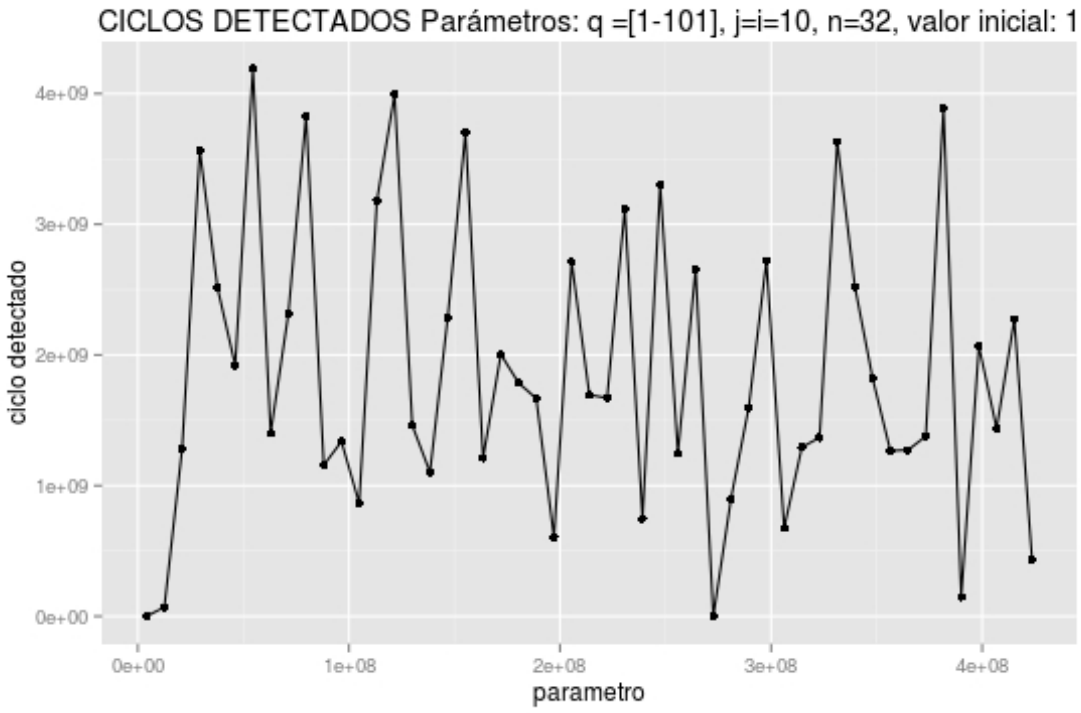

Figura 5: Gráfica de Ciclos con las especificaciones: $n = 32$, $i = j = 10$, $q = [1, 101]$.

Como podemos ver, se obtuvieron tamaños de ciclo pequeños, esto se puede deber a muchas causas, pero pensamos que puede ser por la elección de la semilla. Por lo tanto, vamos a elegir una semilla que sea un número primo, en este caso será el número: 2147483647, de hecho este es un número primo de Mersene, porque es igual al valor de una potencia de dos, pero se le resta una unidad. A continuación se muestran los resultados obtenidos, como se puede observar, cuando se utiliza un número primo, se obtienen menos ciclos de corta longitud. A continuación, se muestra una gráfica que nos muestra la diferencia. Sin embargo, no se obtuvo una mejoría notable: en algunos valores poara q el tamaño del ciclo aumenta, pero en otros disminuye.

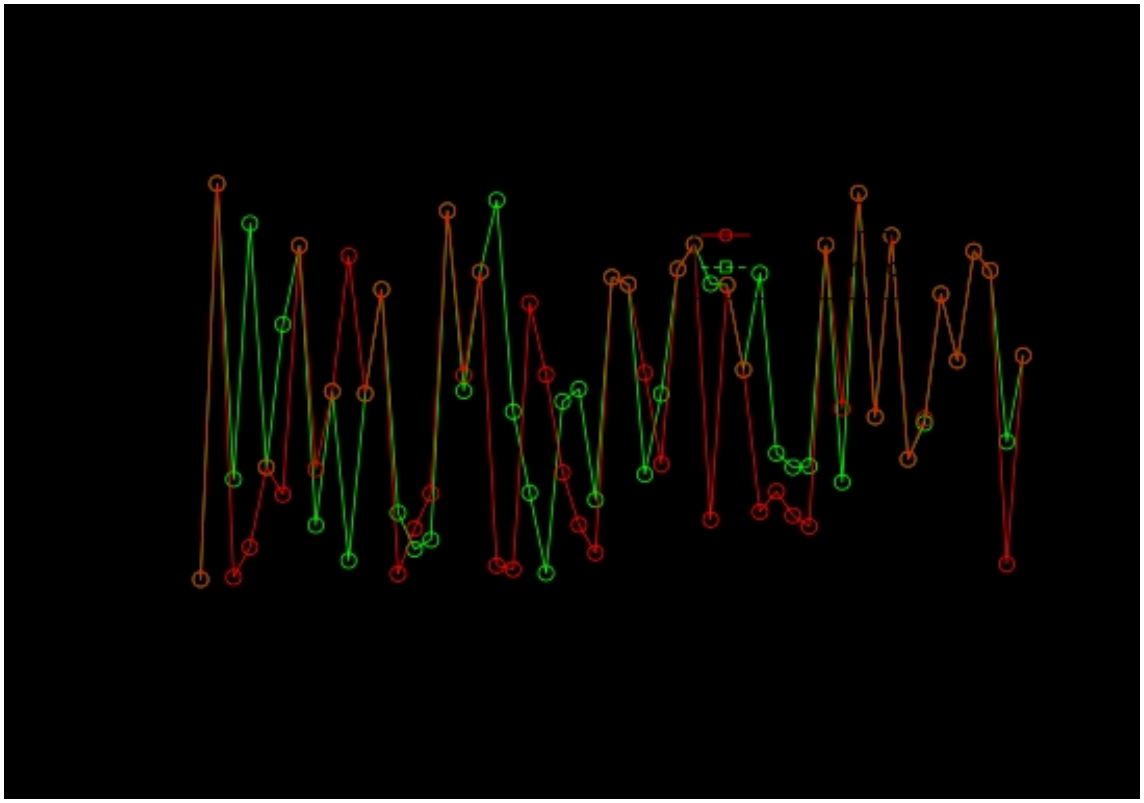

Figura 6: Gráfica de Ciclos con las especificaciones: $n = 32$, $i = j = 10$, $q = [1, 101]$.

6. Referencias.

[1] T. Addabbo, M. Alioto, A. Fort, A. Pasini, S. Rocchi and V. Vignoli, A Class of Maximum-Periodo Nonlinear Congruential Generators Derived From the Rényi Chaotic Map. IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS, 2007.