Proyecto Final de Matemáticas Discretas
Fractales Aplicados a la criptografía
Grupo: K-ON

David Ricardo Dager
Manuel Arturo Ramírez
Ciro Iván García
Presentado a: Andres Villaveces Niño
Universidad Nacional de Colombia
Facultad de Ingeniería
Departamento de Ingeniería de Sistemas e Industrial

11 de junio de 2014

Fractales

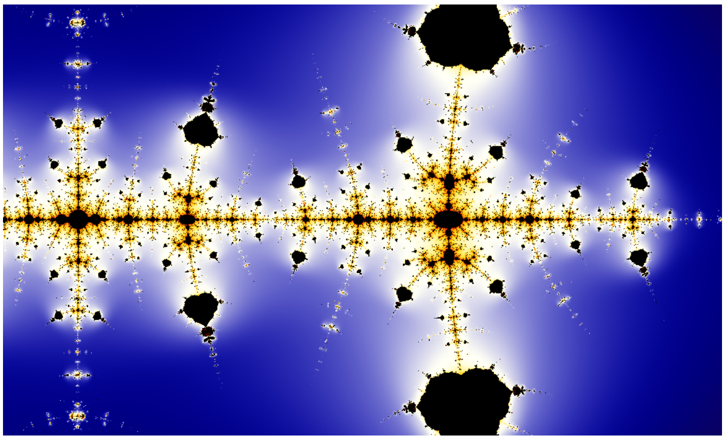
"Un fractal es la representación gráfica del caos" (Gutierrez y Hott).
Características a resaltar:

- Comportamiento caótico.
- Autosimilares.
- Representación algorítmica "simple".

Caos (matemático)

- Análisis no convencional.
- Ligado fuertemente a condiciones iniciales.
- Efecto mariposa es una poripiedad intrínseca del caos.
- Trayectoras cuasi periódicas.
- Atractores extraños.

Conjetura de Collatz :

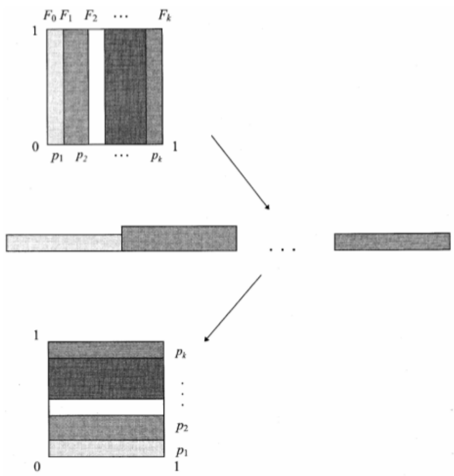


Versión general: Sea U el cuadrado unitario se define la transformación de Baker de la siguiente manera:

$$T(x,y) = (\frac{1}{p_i}(x - F_i), p_i y + F_i) \tag{1}$$

De donde (x,y) ϵ $[F_i, F_i + p_i)\times$ [0,1).

Tomado de Jiri:



Transformación de Baker II

Sea N en conjunto N={0,1,2..,n-1} de números enteros y sea λ un conjunto de enteros, λ={$\lambda_1, \lambda_2, ..., \lambda_k$}, que satisface las siguientes propiedades:

- $\lambda_1 + \lambda_2 + ... + \lambda_k$=n.
- $\lambda_i \mid n$ $\forall$ i ϵ {1,2,...,k}

Definimos la transformación discreta de Baker $B_{N,\lambda}$: N $\times$ N $\longmapsto$ N $\times$ N de la siguiente manera:

$$B_{N,\lambda}(x,y) = (n - \sigma_i - \lfloor \frac{n-(x+1)}{q_i} \rfloor - 1, \frac{y-\sigma_i}{q_i} + [n-(x+1)] \ mod \ q_i) \qquad (2)$$

De donde $\sigma_1 := 0$ y $\sigma_i := \lambda_1 + ... + \lambda_{i-1}$ para $1 \leq i < k$, $q_i := \frac{n}{\lambda_i}$ y (x,y) ϵ $N \times [\sigma_i, \sigma_i + \lambda_i)$.

Cifrar el mensaje

El cifrado del mensaje se hace caracter a caracter:

- Tomar el caracter de la cadena, α_i.
- Elegir un número, entero, aleatorio dentro del dominio [a,b], φ_i.
- Evaluar $f_{encp}(\alpha_i, \varphi_i)$ obteniendo μ_i.
- Almacenar φ_i,α_i,μ_i.
- Si aún quedan caracteres volver a 1, si no transmitir.

La función de encriptación (basada en la conjetura de Collatz) es la siguiente:

$$x_1 = \begin{cases} \frac{x}{2} \bmod 9 & \text{si } x \text{ es par} \\ (3x+1) \bmod 9 & \text{si x es impar} \end{cases}$$

Por la naturaleza de la conjetura se realiza un casteo para los valores 3, 7 y 8.

Para descifrar el mensaje debemos conocer la matriz de cifrado, ubicaremos el caracter cifrado μ en la matriz con la siguiente función

$$\mu_{decrypted} = \begin{cases} 0 & \text{si } \mu = 0 \\ 2 * \mu & \text{si } 0 < \mu < 4 \\ 1 & \text{si } \mu = 4 \\ 3 & \text{si } \mu = 5 \\ 8 & \text{si } \mu = 6 \\ 5 & \text{si } \mu = 7 \\ 7 & \text{si } \mu = 8 \end{cases}$$

El proceso se realiza φ veces, que es la cantidad de iteraciones usadas para cifrar a μ.

Gracias.