Programación y Algoritmos
Parte 1: Lenguaje C

Tarea #7 **Fecha de entrega: 1/11/2021**.

1. Realizar un análisis de complejidad (O(n)) del algoritmo Quicksort.
2. Implementar un sistema de cifrado para imágenes basado en una red de generadores de números aleatorios basado en teoría de caos. El sistema debe funcionar de acuerdo a una red de mapas caóticos que se definen:

$$\begin{aligned} X_{1,j} &= f\left(X_{1,j-1}\right) + \varepsilon \& H(X_{1,j-1}, X_{2,j-1}, X_{3,j-1}) \\ X_{2,j} &= f\left(X_{2,j-1}\right) + \varepsilon \& H(X_{1,j-1}, X_{2,j-1}, X_{3,j-1}) \\ X_{3,j} &= f\left(X_{3,j-1}\right) + \varepsilon \& H(X_{1,j-1}, X_{2,j-1}, X_{3,j-1}) \end{aligned} \quad (1)$$

Donde & es el operador AND, y

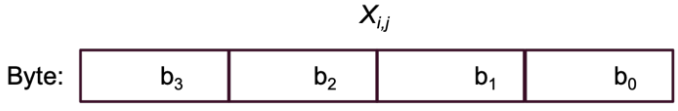
$$H\left(X_{1,j-1}, X_{2,j-1}, X_{3,j-1}\right) = \oplus_{i=1}^{3} X_{i,j-1}$$
$$\oplus = XOR\ Operator\ \hat{}$$

Con mapa caótico ($f \circ f \circ f \circ \ldots \circ f$),

$$X_{i,j} = f\left(X_{i,j-1}\right) = \left(b \cdot X_{i,j-1} + \left\lfloor \frac{X_{i,j-1}}{2^m} \right\rfloor\right)$$
$$X \in N\colon 1,2,3,4,\ldots,2^L - 1;\ 3 < m < 8$$

El sistema de cifrado es simétrico (el que envía como el que recibe tiene las mismas condiciones iniciales) y trabaja de la siguiente manera:

- Definir las condiciones iniciales, m, ε, y tres llaves $X_{i,0}$ (una para cada mapa).
- Se evalúa cada uno de los mapas en cada iteración *j,* y al final se calcula *H*.
- El resultado de H se suma con los valores de $f\left(X_{1,j-1}\right)$ en cada mapa de acuerdo a ec.1.
- Cada mapa provee un valor entero de 32 o 64 bits (dependiendo de la computadora de cada estudiante), de donde se pueden obtener 4 ú 8 bytes. Extraer cada uno de los bytes para encriptar un pixel distinto de la imagen de entrada, esto es:



La imagen de entrada es I(m,n) y la imagen cifrada es J(m,n):

J(0,0) = I(0,0)^ b_0;
J(0,1) = I(0,1)^ b_1;
J(0,2) = I(0,2)^ b_2;
J(0,3) = I(0,3)^ b_3;

Y así sucesivamente.

Escribir dos programas, uno para cifrar la imagen y escribirla en un archivo de texto, y el otro para leer la imagen del archivo y descifrarla. Se tendrá que desplegar la imagen original y cifrada.