UNIVERSIDAD ICESI

Departamento de TIC
Algoritmos y Estructuras de Datos
Unidad 1 Laboratorio

Objetivos

Unidad 1: Análisis de Algoritmos

OE1.1. Calcular la complejidad temporal de algoritmos iterativos.
OE1.2. Calcular la complejidad espacial de algoritmos iterativos.
OE1.3. Caracterizar la entrada de un algoritmo iterativo con el fin de calcular la complejidad para el mejor y peor caso.
OE1.4. Analizar algoritmos independiente de una implementación concreta (no dependiente del lenguaje de programación).
OE1.5. Utilizar notación asintótica para describir la complejidad de algoritmos.
OE1.6. Evaluar varios algoritmos que resuelven el mismo problema en términos de sus complejidades computacionales.
OE1.7. Comprender la importancia del Modelo RAM en el proceso de análisis de algoritmos.

Enunciado

Una parte fundamental de la mayoría del software producido actualmente es la seguridad de los datos, esto es, mantener la triada CID: Confidencialidad, Integridad y Disponibilidad de la información. Para esto, hay una rama de la informática que juega un papel muy importante llamada Criptografía, la cual se ocupa, entre otras cosas, de generar técnicas (algoritmos) de cifrado que permitan mantener segura la información. Para lo anterior, la criptografía se apoya de una gran aliada de la ingeniería (aunque frecuentemente vista como enemiga por los ingenieros en los primeros semestres de su carrera): la matemática, usualmente utilizada como herramienta para definir algoritmos de encriptación que aprovechan las propiedades de los números primos, números muy curiosos que sólo son divisibles por ellos mismos y por el 1 (a partir de esta definición nacen discrepancias sobre si el 1 es verdaderamente un número primo o no, usted puede asumir cualquier posición para este laboratorio).

Ahora bien, la pequeña empresa para la que usted trabaja ha decidido tomarse en serio la seguridad de sus sistemas y realizar sus propias implementaciones de algunos algoritmos de encriptación. Para esto, una de las tareas más básicas que deben realizar (que por esto se la confiaron a su equipo de desarrolladores junior), es poder contar con un programa que permita la **generación de números primos** que posteriormente podrán ser utilizados por los algoritmos. Como es bien sabido, el proceso puede ser riguroso y dispendioso en tiempo, por tal su jefe le ha pedido implementar tres (3) algoritmos que cumplan con este propósito, para posteriormente seleccionar el mejor.

El sistema debe contar con una Interfaz Gráfica de Usuario que permita ingresar el número máximo o tope (n) para la búsqueda de los números primos (es decir, sólo encontrará los números primos menores o iguales a ese n) y seleccionar qué algoritmo (de los tres implementados) se quiere utilizar para la generación de los primos. Además, para evaluar el comportamiento de los algoritmos y de su desarrollo, la salida debe verse como una matriz de números (desde 1 hasta n) lo más cuadrada posible (es decir, si n=100 la matriz debería ser 10x10, pero si n=20, la matriz no debería ser 10x2, sino 5x4 o 4x5) y debe pintar de verde los números primos y de rojo los que no lo son **conforme el algoritmo encuentre que el número es o no es primo, es decir, que permita mostrar en tiempo real el proceso que realiza el algoritmo para encontrar estos números primos.**

Usted debe utilizar el método de la ingeniería para resolver este problema y dejar evidencia en su informe de los resultados de cada fase. Por ejemplo, en la fase 1 deben identificar claramente el problema, justificarlo y especificar los requerimientos funcionales. Recuerde revisar el Resumen del Método de la Ingeniería y el ejemplo del Método de la Ingeniería aplicado a un problema.

UNIVERSIDAD ICESI

Departamento de TIC
Algoritmos y Estructuras de Datos
Unidad 1 Laboratorio

Entregables. 1. Análisis de complejidad temporal de cada uno de sus algoritmos **2.** Análisis de complejidad espacial de cada uno de sus algoritmos **3**. Especificación de Requerimientos y Diseño. **4.** Implementación del programa con todo los requerimientos en su lenguaje de programación favorito.

El laboratorio debe ser desarrollado en grupos de máximo 3 estudiantes. Tenga en cuenta la rúbrica de evaluación para esta actividad: Rúbrica del Laboratorio 1.

Nota: Usted debe entregar un archivo comprimido en formato zip de un directorio con únicamente 2 archivos: 1 archivo de informe en formato pdf con toda la documentación (de cada una de las fases del método y el análisis) y otro archivo comprimido de un directorio con los archivos de codificación en sus respectivos paquetes.

El nombre del archivo comprimido debe tener el formato: PRIMERAPELLIDOEST1_PRIMERAPELLIDOEST2_PRIMERAPELLIDOEST3.zip (tenga en cuenta que el separador entre cada apellido es un guion al piso).