INGENIERÍA INFORMÁTICA

UNIVERSIDAD DE SANTIAGO DE CHILE

Algoritmos Avanzados

Enunciado Laboratorio nro. 3

Profesor: Cristián Sepúlveda S.

7 de junio de 2022

Tabla de contenidos

1. Introducción

En la industria y en situaciones diarias existen muchas instancias en las cuales se debe resolver problemas mediante el uso de algoritmos. Muchas veces estos problemas son resueltos gracias al conocimiento de un experto o con el apoyo de tecnologías, cuando el problema ha sido exitosamente modelado y se ha construido una herramienta para apoyar en su resolución. En este laboratorio se trabajará con un problema de optimización de la literatura y se deberá construir una solución computacional con técnicas y conocimientos vistos en el curso.

2. Resultados de aprendizaje (RdeA)

- Formular algoritmos para un problemas computacionales.
- Resolver problemas mediante la aplicación de herramientas computacionales, en base a su clasificación.
- Mostrar disposición al trabajo en equipo.
- Desarrollar la capacidad de comunicarse efectivamente en español de forma oral y escrita.
- Demostrar capacidad crítica en el análisis de resultados.

3. Instrucciones

1. El trabajo se realizará en grupos de a lo más dos personas.
2. Describir en pseudocódigo un algoritmo para cada problema propuesto utilizando el enfoque ***ramificación y acotamiento***.
3. Calcular la complejidad de tiempo para el algoritmo descrito.
4. Implementar el algoritmo propuesto utilizando el lenguaje de programación C.
5. Resolver los ejemplos disponibles en Campus Virtual, registrando los valores de las soluciones entregadas por el algoritmo diseñado y los tiempos de ejecución.
6. Analizar los resultados obtenidos respecto a los cálculos teóricos y a los resultados obtenidos en los laboratorios anteriores.
7. Generar un reporte de los experimentos realizados, con las siguientes secciones:
   - **Introducción**
     Se proporciona el contexto y la motivación para el experimento. Se explica

brevemente la teoría relevante con suficiente detalle como para introducir leyes, ecuaciones o teoremas relevantes. Se Indica claramente el objetivo el/los objetivo/s o la pregunta de investigación para el que está diseñado el experimento.

- **Método**
  Se describen el equipo, los materiales y los procedimientos utilizados en los experimentos. Se describen procesamientos o cálculos realizados sobre los datos utilizados. Se menciona cualquier dificultad experimental encontrada y cómo se solucionó.
- **Resultados y Análisis**
  Se presentan los resultados de los experimentos de forma gráfica o mediante tablas debidamente etiquetadas. Se discute acerca de cómo se analizaron los resultados.
- **Discusión**
  Se Interpretan los resultados más relevantes en relación con los objetivos/pregunta de investigación. Se resumen los principales hallazgos y limitaciones. Se identifican y comentan tendencias que se hayan observado. Se realizan recomendaciones para superar las limitaciones y se sugieren mejora para futuras investigaciones.
- **Conclusiones**
  Se recuerda al lector qué problema se estaba investigando. Se resumen los hallazgos en relación con el problema/hipótesis. Se Identifican brevemente las implicaciones generales de los principales hallazgos.
- **Apéndice** (opcional)
  Se agrega información que ayuda a los lectores a comprender el proceso de investigación.
- **Referencias**
  Se enumeran los detalles de todas las publicaciones citadas en el texto, permitiendo a los lectores localizar las fuentes de forma rápida.

4. Evaluación y fechas

- **Entrega nro. 1**
  Entregable: pseudocódigo del algoritmo. En formato PDF.
  Ponderación: 10 %.
  Entregable: cálculo de la complejidad de tiempo del algoritmo. En formato PDF.
  Ponderación: 10 %
  Canal: Campus virtual.
  Fecha de entrega: 14 de junio.
- **Entrega nro. 2**
  Entregable: informe en formato PDF e implementación.
  Ponderación: informe 60 %. implementación 20 %
  Canal: Campus virtual.
  Fecha de entrega: 21 de junio.

5. Problema propuesto

5.1. Descripción problema

El criptosistema Merkle-Hellman, publicado por Ralph Merkle y Martin Hellman en 1978, fue uno de los primeros criptosistemas de clave pública. En un criptosistema de clave pública se utilizan dos claves, una clave pública para el cifrado y una clave privada para el descifrado. En 1984 Adi Shamir publicó un ataque de tiempo polinomial. Como resultado, hoy en día el criptosistema es considerado inseguro.
Con el fin de fortalecer la seguridad del esquema Merkle-Hellman, en 2006 Kasahara y Murakami propusieron una variación, que permite al criptosistema resistir el ataque de Shamir y los ataques de baja densidad. Actualmente el esquema Kasahara y Murakami continúa considerándose seguro.
La fortaleza de las claves generadas por el esquema se fundamenta en la dificultad de resolver el siguiente problema perteneciente a la clase NP-completo:

"Dado un conjunto de números enteros, cada uno de ellos con una ponderación asociada, se busca determinar un subconjunto de números, de modo que la suma total de las ponderaciones sea menor o igual que un valor límite dado y la suma total de los valores sea lo más grande posible."

El esquema Kasahara-Murakami hace uso de información extra para resolver el problema anterior disminuyendo drásticamente su complejidad, utilizando la solución de problema para la generación de claves privadas.

5.1.1. Datos

Disponibles en archivos con extensión .txt en Campus Virtual.

5.1.2. Formato de archivos

Nombre de archivo: *kp_n_pmax*
n: cantidad de números del ejemplo
pmax: valor máximo para la suma de las ponderaciones del conjunto seleccionado

El contenido de los archivos tiene el siguiente formato para cada línea:

v_1	p_1
v_2	p_2
v_n	p_n

v_i: valor del i-ésimo número
p_i: ponderación del i-ésimo número