Universidad de San Carlos de Guatemala
Escuela de Ingeniería en Ciencias y Sistemas, Facultad de Ingeniería
Introducción a la programación y computación 2, 2do. Semestre 2023.

SISTEMA DE ENCRIPTACIÓN Y DESCIFRADO DE MENSAJES MEDIANTE TDA'S

202200135 – Joab Israel Ajsivinac Ajsivinac

Resumen

El "Ministerio de la Defensa de Guatemala" requiere el desarrollo de una nueva tecnología que permita él envió de mensajes encriptados mediante el uso de drones los cuales tendrán la capacidad de subir una cantidad de metros (representando un carácter), y emitir una luz led de alta intensidad, esto para que los mensajes no puedan ser interceptados por terceros.

El programa carga datos de entrada mediante archivos XML para luego hacer uso de TDA'S de manera que se facilite el manejo de la información relevante como: alturas, drones, sistema de drones, instrucciones y mensajes, la solución optimiza los tiempos en los cuales se encienden las luces de alta intensidad, dando como resultado el menor tiempo en el cual se puede llegar a emitir un mensaje encriptado. Finalmente, la solución genera diferentes archivos de salida como: gráficas utilizando nodos, o archivos con la misma extensión que los archivos de entrada

El sistema busca simplificar el análisis que efectúan los operarios, al momento que se desee decodificar una señal encriptada.

Palabras clave
Drones, optimización, encriptar, mensaje, altura

Abstract

The "Ministerio de la Defensa de Guatemla" requires the development of new technology that allows the transmission of encrypted messages using drones, which will have the ability to ascend a certain number of meters (representing a character) and emit high-intensity LED light, in order to prevent messages from being intercepted by third parties.

The program loads input data through XML files and then utilizes data structures (TDA's) to facilitate the management of relevant information such as altitudes, drones, drone system, instructions, and messages. The solution optimizes the timing of when the high-intensity lights are turned on, resulting in the shortest possible time to transmit an encrypted message. Finally, the solution generates different output files, such as graphs using nodes or files with the same extension as the input files.

The system aims to simplify the analysis performed by operators when they need to decode an encrypted signal.

Keywords
Drones, optimization, encryption, message, altitude.

Introducción

El sistema de encriptación y descifrado de mensajes a través de drones es una herramienta que resulta de gran importancia en la industria de la tecnología de la información y ciberseguridad junto con el gobierno y defensas, ya que facilita la comprensión de los mensajes a su vez que hace que los mismos sean difíciles de interceptar asegurando que el mensaje llegue solamente a los receptores deseados, asi mismo para que al momento de interpretar los diferentes mensajes se hagan de una forma eficiente.

El software proporciona la forma de poder generar gráficas para los diferentes tipos de datos que se utilizan durante el proceso, como lo son los sistemas de drones y la información necesaria de los mensajes, esto para que la comprensión de los resultados sea más eficiente.

Desarrollo del tema

El sistema se basa en la utilización de TDA'S las cuales son estructuras de datos que se utilizan para organizar y manipular datos de manera estructurada y coherente. Se asemeja a la forma en que en la vida cotidiana se agrupan objetos similares en categorías para simplificar su comprensión y manejo.

Las TDA'S usadas para la implementación de la solución de la problemática son:

Lista Simplemente Enlazada: Tiene como base el almacenar una colección de elementos, donde cada elemento se denomina nodo que contiene dos partes principales: el valor del elemento, y una referencia o enlace al siguiente nodo de la secuencia

Lista Doblemente Enlazada: Es una estructura de datos similar a la lista simple, pero con la característica que cada nodo tiene dos punteros, uno que apunta al siguiente nodo y otro que apunta al nodo anterior, lo cual permite la navegación en ambas direcciones, lo que significa que se puede acceder a los elementos tanto hacia adelante como hacia atrás.

Los datos como los nombres de drones, los nombres de sistemas o nombres de mensajes son ordenados alfabéticamente de A-Z siendo sensible a mayúsculas lo que significa que cuando se realiza el ordenamiento las letras mayúsculas se consideran diferentes de las letras minúsculas, el ordenamiento se basa en el valor Unicode de los caracteres en las cadenas. Cada carácter en una cadena tiene un valor numérico asociado según la codificación Unicode (Unicode es un estándar de codificación de caracteres diseñado para representar a todos los caracteres de escritura utilizados en el mundo)

El sistema utiliza como lenguaje de programación principal Python, el cual es un lenguaje de alto nivel y orientado a objetos. Se usó dicho lenguaje por su sintaxis legible y clara, que se asemeja al lenguaje humano lo que facilita la comprensión del código. Además, se hace uso de PySide6 en su versión 6.5.2 (o superior) por lo que usa la versión 3.11.5 (o superior) de Python para la implementación de una interfaz gráfica, para poder hacer más amigable el uso del sistema a los usuarios.

Interfaz Gráfica

La interfaz está dividida en 4 grupos, los cuales son:

- Inicio: En esta parte se puede cargar archivos, generar archivos de salida, procesar los datos, e inicializar el sistema
- Drones: En este apartado se pude agregar y ver los drones ingresados en el sistema, asi como graficar los sistemas de drones ingresados mediante la carga de archivos.

- Mensajes: En este apartado se pueden ver los mensajes junto con sus instrucciones, además de poder ver la información importante de un mensaje como lo es: sistema de drones a usar, mensaje enviado y tiempo óptimo, junto con la opción de ver la información se puede generar una gráfica con los movimientos (subir, bajar, esperar, emitir luz) necesarias para poder emitir el mensaje encriptado.
- Ayuda: En este apartado se puede visualizar la información del estudiante, junto con un botón que abrirá una pestaña del navegador con la documentación del sistema.

a. Inicialización

Esta opción le permitirá al usuario limpiar todas las variables, listas y cálculos realizados para poder volver a ejecutar el sistema de forma que los datos anteriormente ingresados ya no existan dentro del contexto del programa.

b. Carga de Archivos

Los datos se cargan al sistema mediante el ingreso de archivos XML, para que luego poder almacenar la información relevante de los drones, sistema de drones e instrucciones en memoria en diferentes listas para su posterior procesamiento. Este proceso se puede llegar a realizar "n" veces con diferentes archivos XML.

El sistema cuenta con la verificación de nombre de nodos, para que no se lleguen a repetir.

Para el ingreso de los drones se precisa de un ingreso de datos ordenado, dado a que se necesita tener los datos ordenados de forma alfabética, para ello primero se pregunta si está vacía, si lo está, se ingresa el primer nodo, si no está vacía se tiene como segunda condición se pregunta si el primer dato es mayor al nuevo nombre, si lo es, el nuevo dato toma el lugar de primer valor, por último si no cumple con las dos condiciones anteriores, se itera los valores hasta encontrar un dato mayor al nuevo, para poder asignarle como puntero siguiente el valor siguiente del elemento ya perteneciente a la lista, para luego asignarle el nuevo valor, al siguiente del elemento encontrado.

c. Optimización

El sistema tiene el objetivo de optimizar el tiempo en que se muestra un mensaje encriptado, para eso las instrucciones dadas se cargan en una lista doblemente enlazada, la cual guarda las instrucciones conforme el orden en el que están en el archivo de entrada, guardando información como la altura destino del dron, para poder saber en qué posición final debería estar el dron luego de los movimientos, también guarda la cantidad de veces que debe subir o bajar un dron esto se logra mediante la resta del valor de la altura del dron actual menos la altura en la que se quedó en la instrucción anterior (si es que existe una posición anterior) para encontrar los dos datos, se hace una búsqueda desde el final hasta encontrar una coincidencia con el nombre del dron actual, obteniendo ese valor se resta las alturas, para poder obtener la cantidad de movimientos que debe hacer un dron, si la resta da como resultado un número positivo entonces quiere decir que tiene que subir, si la resta da un número negativo entonces quiere decir que tiene que bajar.

Luego con la información anterior ya guardada, se procede a encontrar el tiempo mínimo, iniciando con obtener una lista doble, con los datos de las instrucciones sin repetir, de forma que todos los drones no repetidos hagan sus respectivos

movimientos, luego restando o sumando una unidad a cada valor de movimiento calculado anteriormente , si una señal llega a la altura deseada, antes de que llegue su turno, quedara esperando a que le llegue su tiempo, si aún no está en su altura deseada, se procederá a seguir subiendo o bajando según sea el caso. Si el dron con la primera instrucción llega a su altura deseada en el siguiente tiempo encenderá la luz de alta energía, para posteriormente eliminar el elemento de la lista doble para dejar que se ejecute la siguiente instrucción, creando una nueva lista de datos no repetido, este proceso se repite hasta que se complete la emisión del mensaje. Los datos de los movimientos se agregan otra matriz con los mismos drones que el sistema de drones elegido, para luego ser agregados a una lista que contiene la matriz, el tiempo, el mensaje decodificado, y el sistema de drones a utilizar.

c. Generar archivos de salida

Esta opción genera un archivo con extensión XML, con las librerías xml.tree.ElementTree y xml.dom, la primera es para manipular y escribir archivos en formato XML, y la segunda es para agregar la identación correcta al archivo resultante. Los datos mostrados en el XML, son las instrucciones que se deben enviar para poder enviar un mensaje encriptado, junto con el nombre del mensaje, el nombre del sistema de drones que se debe utilizar, y el tiempo óptimo para poder mostrar el mensaje.

d. Gestión de drones

Con esta opción se podrá ver los drones que se tienen registrados, ordenados de forma alfabética, además cuenta con la posibilidad de agregar un dron, bajo las restricciones de que no pueden existir dos drones con el mismo nombre.

Dentro de esta sección se tiene una opción para generar la gráfica de sistemas de drones, la cual es una tabla donde se muestra los drones y las alturas de cada sistema, junto con su respectivo nombre de sistema, Si un dron/altura no viene dentro del archivo de entrada, la celda donde debería ir su valor se tornará de color gris, lo que indica que no hay datos ingresados para esa celda, de lo contrario se vera el valor alfanumérico ingresado en el archivo de entrada.

f. Gestión de mensajes

En esta opción se podrá ver el listado de mensajes junto con las instrucciones que vienen en el archivo de entrada, los mensajes están ordenados de forma alfabéticamente en base al nombre del mensaje

Adicionalmente, se puede seleccionar un mensaje para mostrar: el nombre del sistema de drones que se debe utilizar, el mensaje que se enviará, el tiempo óptimo para que el sistema de drones pueda mostrar el mensaje. Finalmente, se podrá generar una gráfica que ejemplifique el listado de instrucciones que se debe enviar al sistema de drones para el mensaje elegido, para lograr generar el mensaje en el tiempo optimizado.

d. Ayuda

En esta opción tiene el propósito de ayudar al usuario a conocer a la persona que desarrollo el sistema, además de contar con la opción de poder abrir la documentación del proyecto que esta subida en la red.

Conclusiones

Con base en el análisis de los datos y la comprensión del software para el encriptado y desencriptado de

señales de audio, se puede resaltar la eficacia y las posibles áreas de mejora en esta solución innovadora.

El uso de TDA'S para el almacenamiento y procesamiento de información ha demostrado ser eficiente en términos de memoria, ya que permite la asignación dinámica de recursos, lo que resulta importante para el rendimiento. Además, resulta ser muy flexible el uso de las listas ya que se pueden agregar nodos con diferentes atributos

El uso del software de diseño de diagramas Graphviz permite la visualización de la información relevante del sistema, de forma que sea más fácil de comprender para los usuarios

El software representa un avance prometedor en el campo de la defensa nacional. Los resultados obtenidos indican su potencial y eficacia, sin embargo, persisten desafíos y oportunidades para mejorar que invitan a futuras investigación y desarrollo.

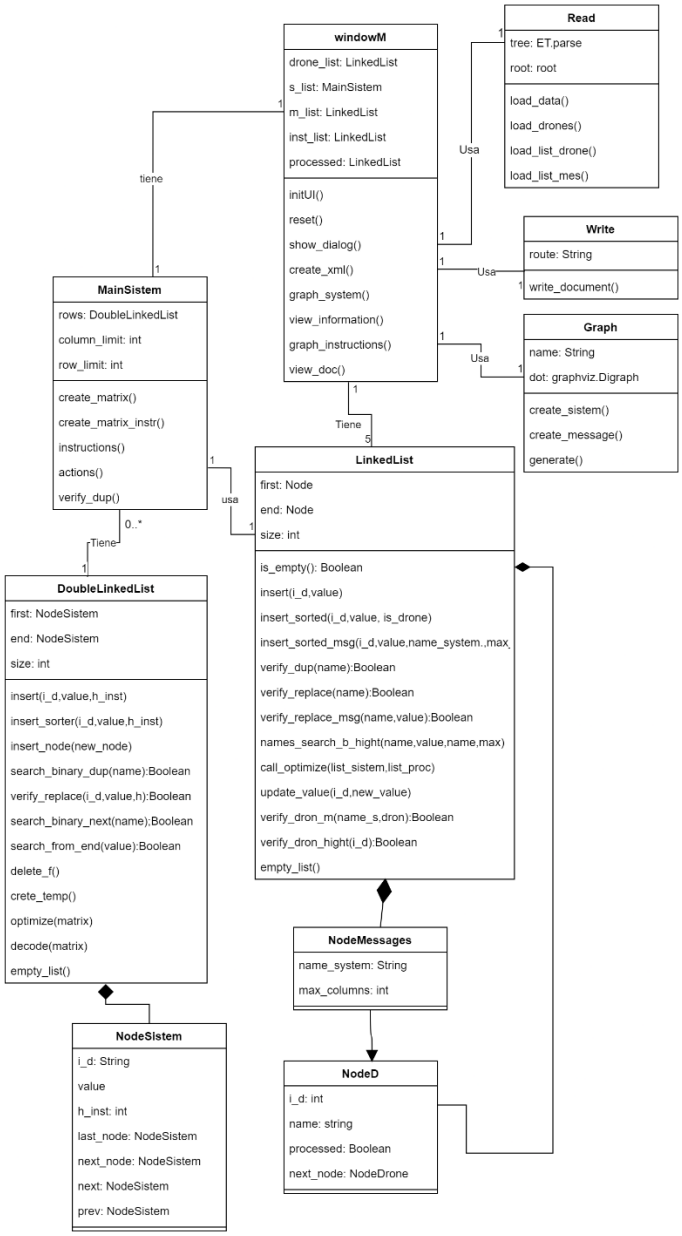

Figura 1. Diagrama de clases de las listas y de la App.

Fuente: elaboración propia

Referencias bibliográficas

CC30A Algoritmos y Estructuras de Datos: Tipos de datos abstractos. (s. f.). https://users.dcc.uchile.cl/%7Ebebustos/apuntes/cc30a/TDA/

H. Costa Guzmán, (2021). *Instalación y configuración de PySide.* https://docs.hektorprofe.net/qt-pyside/preparacion-previa/instalacion-pyside/

Anexos

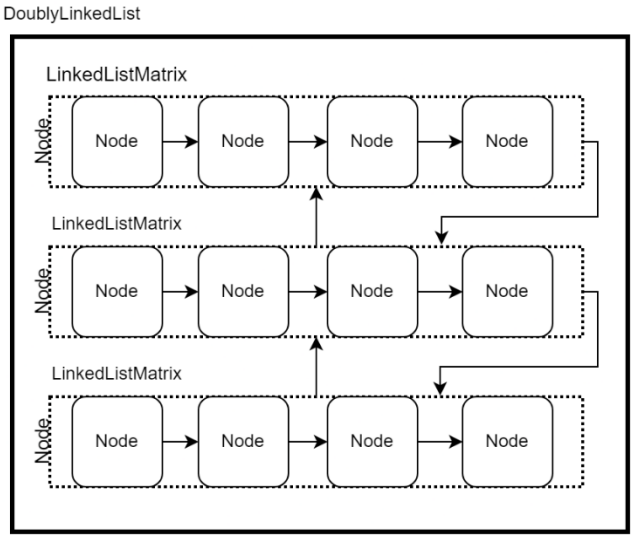

Figura 2. Representación gráfica de la Matriz.

Fuente: elaboración propia

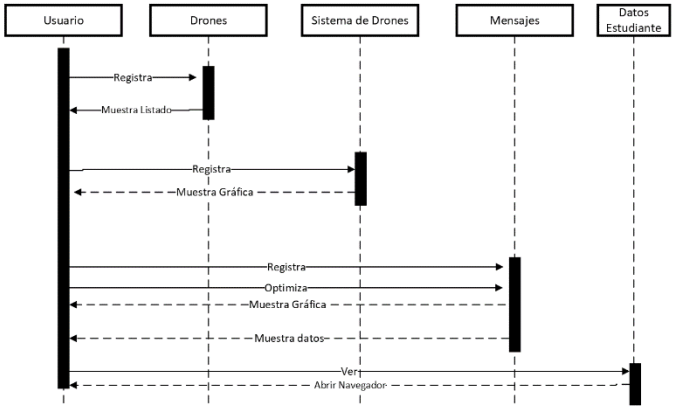

Figura 3. Diagrama de Secuencia.

Fuente: elaboración propia