
SISTEMA DE ENCRIPCIÓN 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 el envío 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 Guatemala" 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, así 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 usada 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.

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

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. Las instrucciones dadas se cargan en una matriz, la cual guarda el orden en el que llegan las instrucciones y por orden de dron, junto con la cantidad de unidades, que se tiene que subir o bajar además de un indicador de que si esa instrucción ya cumplió con la condición de encender la luz de alta energía, para el cálculo de las unidades se resta el valor anterior con el nuevo a ingresar para luego verifica si se debe subir o bajar, luego con la información ya guardada, se procede a encontrar el tiempo mínimo, de forma que todos los drones con que tengan que subir, suban todos al mismo tiempo, luego restando una unidad a cada instrucción, 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. Si el dron con la primera instrucción llega a su altura deseada en el siguiente tiempo encenderá la luz de alta energía, en el momento de que encienda su luz la siguiente instrucción podrá encender su luz, si el dron que acaba de encender la luz, aún tiene que subir o bajar para mostrar otra letra, se eliminara el elemento de la matriz para dejar que se ejecute la siguiente instrucción del dron este proceso se repite hasta que se complete la emisión del mensaje. Los datos luego de cada iteración (una iteración para el caso sería al completar la evaluación de una fila y una unidad) en

otra matriz similar, pero con el valor de la instrucción que se debe enviar, junto con el tiempo y los drones

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 indentación correcta al archivo resultante.

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

e. Gestión de sistemas de drones

Con esta opción el usuario podrá visualizar el listado de sistema de drones de una forma intuitiva a través de un gráfico creado con la librería `Graphviz`

f. Gestión de mensajes

En esta opción se podrá ver el listado de mensajes junto con las instrucciones, ordenadas 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 grafica que ejemplifique el listado de instrucciones que se debe enviar al sistema de drones 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

Esta sección debe orientarse a evidenciar claramente las principales ideas generadas, propuestas que deriven del análisis realizado y si existen, expresar las conclusiones o aportes que autor quiera destacar.

Enfatizando, lo importante es destacar las principales posturas fundamentadas del autor, que desea transmitir a los lectores.

Adicionalmente, pueden incluirse preguntas abiertas a la reflexión y debate, temas concatenados con el tema expuesto o recomendaciones para profundizar en la temática expuesta.

Referencias bibliográficas

CC30A Algoritmos y Estructuras de Datos: Tipos de datos abstractos. (s. f.).

<https://users.dcc.uchile.cl/%7Ebebustos/apuntes/cc30a/TDA/>

Anexos

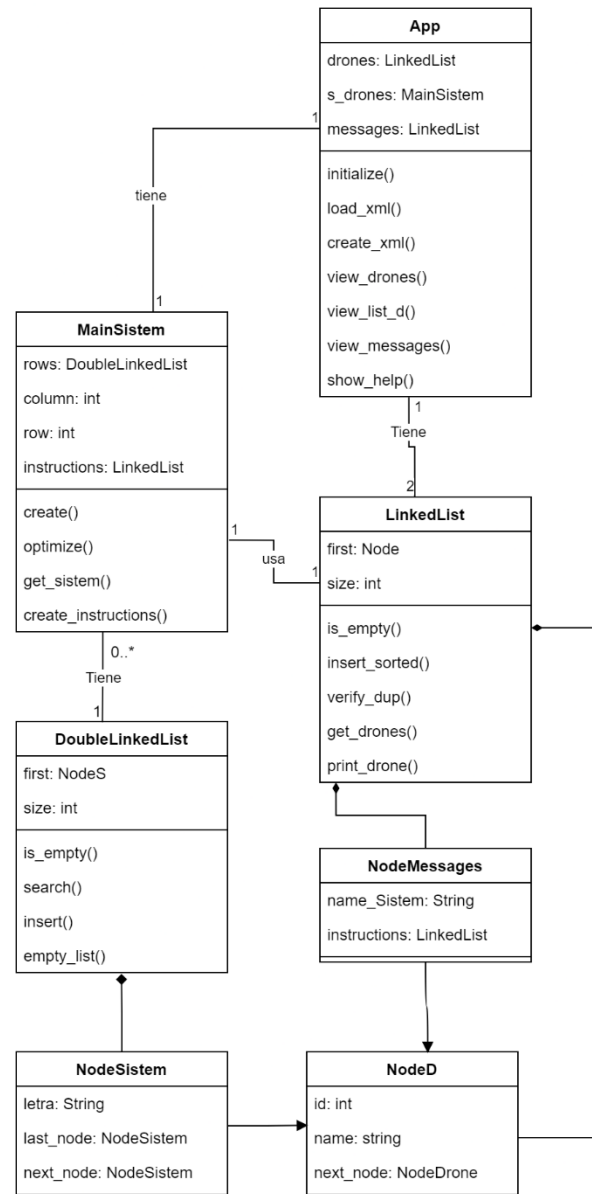


Figura 1. Diagrama de clases de las listas y de la App.

Fuente: elaboración propia