

---

## PROYECTO 2 – IPC2

---

202101927 – Miguel Adrian Tubac Agustin

### Resumen

La implementación del proyecto consiste en la creación de un algoritmo de programación que utiliza el lenguaje Python, el mismo es utilizado para la creación del programa encargado de analizar señales de varios drones a distintas distancias.

Las señales que analiza este programa corresponden a datos correspondiente altura y emisión de luces. Estos datos son empleados para el almacenamiento de mensajes para la comunicación del ejercito del Guatemala.

Durante la creación del programa se empleó el paradigma de programación orientado a objetos, comúnmente conocido como (POO). Este paradigma se empleó con la finalidad de mejorar la abstracción del programa y al mismo tiempo la legibilidad de la información a tratar.

La implementación de este cuenta con las opciones de generar gráficas y archivos de salida con extensión XML.

### Palabras clave

Algoritmo, Memoria Dinámica, Optimización, Análisis, Discreción.

### Abstract

*The implementation of the project consists of the creation of a programming algorithm that uses the Python language, which is used to create the program responsible for analyzing signals from several drones at different distances.*

*The signals analyzed by this program correspond to data corresponding to height and light emission. These data are used to store messages for the communication of the Guatemalan army.*

*During the creation of the program, the object-oriented programming paradigm, commonly known as (OOP), was used. This paradigm was used in order to improve the abstraction of the program and at the same time the readability of the information to be processed.*

*The implementation of this has the options of generating graphs and output files with an XML extension.*

### Keywords

*Algorithm, Dynamic Memory, Optimization, Analysis, Discretion.*

## Introducción

El acuerdo de colaboración entre el Ministerio de la Defensa de Guatemala y la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala tiene como objetivo el desarrollo de una tecnología innovadora para el envío de mensajes encriptados. La meta es garantizar que estos mensajes no puedan ser interceptados ni descifrados por personas o instituciones no autorizadas.

El sistema creado consta de dos componentes principales: un emisor de mensajes y un receptor de mensajes. La propuesta de la Facultad de Ingeniería implica el diseño de un sistema que emplea "n" drones. Estos drones tienen la capacidad de elevarse a diferentes alturas y emitir una luz led de alta intensidad. Dependiendo del dron que emita la luz y la altura a la que lo haga, se asignará una letra del alfabeto. De esta manera, el componente receptor puede medir las alturas, identificar qué dron emitió la luz, decodificar cada letra y, finalmente, obtener el mensaje que se pretende transmitir.

## Desarrollo del tema

Este sistema de mensajería encriptada basado en drones. La propuesta de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala es

realmente interesante y promete ser una solución avanzada para garantizar la seguridad de las comunicaciones.

En este sistema, los drones desempeñan un papel crucial. Cada uno de estos drones tiene la capacidad de ascender a diferentes alturas y emitir una luz led de alta emisión. Esta luz no solo cumple la función de señalización, sino que también lleva consigo información encriptada. La clave para entender el mensaje reside en la combinación de la altura a la que el dron emite la luz y el propio dron que la emite.

Cada altura y dron se asocian con una letra específica del alfabeto. Por ejemplo, si un dron se eleva a cierta altura y emite la luz, esa combinación representa una letra particular. De esta manera, el mensaje completo está codificado a través de las diferentes alturas y drones utilizados.

El componente receptor del mensaje, diseñado en colaboración con el Ministerio de la Defensa, está equipado para medir con precisión las alturas y determinar qué dron emitió la luz en cada caso. A través de este proceso, el receptor puede decodificar cada letra asociada a esa combinación específica de altura y dron, revelando así el mensaje original.

Este enfoque no solo proporciona un nivel avanzado de seguridad al utilizar alturas y drones como elementos clave en la codificación, sino que también aprovecha la movilidad y versatilidad de los drones para la transmisión de mensajes en diversos entornos y situaciones. Además, al ser una colaboración entre la academia y el sector de defensa, demuestra el

potencial innovador cuando se combinan conocimientos especializados de diversas disciplinas.



*Figura 1. Sistema de 4 Drones*

Fuente: Pngtree.

Los sistemas de encriptación de mensajes que involucran drones representan una convergencia emocionante entre la tecnología aérea y la seguridad de la información. Estos sistemas buscan abordar desafíos específicos relacionados con la privacidad y la seguridad de las comunicaciones, aprovechando la movilidad y la capacidad de maniobra de los drones.

#### Encriptación Dinámica:

Un aspecto clave de estos sistemas es la encriptación dinámica. A diferencia de métodos estáticos de encriptación, donde una clave se utiliza para todo el mensaje, los drones permiten la variación constante

de variables como alturas, ubicaciones geográficas, e incluso la propia identidad del dron emisor. Esto agrega una capa adicional de seguridad al mensaje.

#### Diversidad de Rutas:

Los drones pueden seguir rutas diversas y cambiar su posición rápidamente. Esto complica significativamente cualquier intento de interceptación, ya que la ubicación del emisor varía constantemente. La capacidad de cambiar rápidamente de posición también hace que sea difícil predecir el próximo punto de transmisión.

#### Identificación de Drones:

La identificación precisa de cada dron es esencial en este sistema. Cada dron podría tener una firma única, ya sea en términos de la luz que emite o de otros parámetros específicos. Esto permite al receptor no solo identificar la altura desde la cual se emitió la luz, sino también determinar qué dron en particular llevó a cabo la transmisión.

#### Integración con Tecnologías Emergentes:

Estos sistemas pueden integrarse con tecnologías emergentes como la inteligencia artificial (IA) para mejorar la capacidad de decisión del dron. Por ejemplo, un dron podría ser programado para adaptarse a las condiciones del entorno y ajustar dinámicamente su comportamiento en respuesta a posibles amenazas.

#### Resiliencia ante Interferencias:

Dado que los drones pueden operar en altitudes variables y cambiar rápidamente su posición, son

menos susceptibles a interferencias y bloqueos de señales. Esto aumenta la resiliencia del sistema ante posibles intentos de interferir con la transmisión de mensajes.

#### Aplicaciones Específicas:

Estos sistemas podrían ser especialmente útiles en situaciones críticas donde la seguridad de la comunicación es fundamental, como operaciones militares, respuesta a emergencias o transmisión de información confidencial.

### Conclusiones

#### Innovación en Seguridad:

La integración de drones en sistemas de encriptación de mensajes marca una innovación significativa en la seguridad de la comunicación. Al aprovechar la movilidad y versatilidad de los drones, se pueden superar desafíos tradicionales asociados con la interceptación de mensajes.

#### Diversificación de Enfoques de Seguridad:

Los sistemas de encriptación de mensajes con drones amplían la diversidad de enfoques de seguridad, ofreciendo una alternativa a los métodos convencionales. Esta diversificación es esencial para mantener la seguridad en un mundo digital en constante evolución.

#### Adaptabilidad a Diversos Escenarios:

La capacidad de los drones para adaptarse a diferentes escenarios y entornos hace que estos sistemas sean versátiles. Pueden ser implementados

en situaciones militares, emergencias, o cualquier contexto donde la seguridad de la información sea prioritaria.

#### Resiliencia ante Amenazas Cibernéticas:

Al reducir la dependencia de infraestructuras de comunicación tradicionales, los sistemas de encriptación con drones ofrecen una mayor resiliencia ante amenazas cibernéticas. La movilidad de los drones dificulta los ataques dirigidos a puntos fijos de transmisión.

#### Colaboración Interdisciplinaria:

Estos sistemas representan la colaboración exitosa entre disciplinas, como la ingeniería, la informática y la defensa. La intersección de conocimientos especializados es esencial para desarrollar soluciones avanzadas que aborden desafíos complejos.

#### Potencial para el Futuro:

La tecnología de encriptación con drones está en una etapa temprana, pero su potencial para el futuro es prometedor. A medida que la tecnología evoluciona, es probable que estos sistemas se perfeccionen y encuentren aplicaciones más amplias en la seguridad de la información.

### Referencias bibliográficas

"Cryptography and Network Security: Principles and Practice"

Revista Académica: IEEE Transactions on Information Forensics and Security

"Introduction to UAV Systems"

DroneMagazine.com

