

CENTRE D’ESTUDIS AULA CAMPUS

CICLO FORMATIVO DE GRADO SUPERIOR

DESARROLLO DE APLICACIONES MULTIPLATAFORMA

Proyecto de Fin de Ciclo

**Calliope: Acomplejando el algoritmo e implementándolo**

Mario Delgado Martínez

Tutor: Mario García Atienza

Curso: CURSO 2023/2024

**Resumen**

El Proyecto Fin de Ciclo se centra en elaborar un esquema de cifrado denominado Calíope (del inglés Calliope) para acomplejar el estándar para algoritmos de encriptación de clave simétrica (AES), esto considerando la relevancia de que dicho esquema permita realizar sus funciones de forma eficiente y sin grandes pérdidas de tiempo respecto al estándar actual. Lo mencionado anteriormente incluye no solo el diseño de Calíope, sino también su implementación en una aplicación de escritorio visualmente intuitiva y fácil de usar. A lo largo de la memoria se detallará las operaciones usadas y sus demostraciones matemáticas correspondientes, así como el proceso de desarrollo de la aplicación tanto por la parte de la interfaz de usuario como por la parte del código fuente que permite la encriptación y la desencriptación de texto, incluyendo tiempos de ejecución obtenidos de las pruebas.

**Agradecimientos**

A todos aquellos que han velado por mí cuando no estaban obligados a hacerlo.

**Portada con el título del proyecto**

**Resumen**

**Agradecimientos**

**Índice general**

**Capítulo 1. Introducción**

* 1. Objetivos
  2. Contextualización

**Capítulo 2. Gestión del proyecto**

2.1 Método de trabajo

2.2 Planificación temporal

**Capítulo 3. Herramientas hardware y software utilizadas**

**Capítulo 4. Desarrollo del Proyecto**

**Capítulo 5. Pruebas y resultados**

5.1 Descripción de experimentos

5.2 Resultados y discusión

**Capítulo 6. Conclusiones y trabajos futuros**

**Bibliografía**

**Anexos**

**Introducción**

A continuación, se detallará lo que el proyecto trata de resolver junto con cierta información sobre la empresa en la que se realizaron las prácticas.

**Objetivos**

Desde hace siglos, el estudio de la escritura secreta (criptología) ha sido crucial para mantener la confidencialidad de la información. Cerca del 1500 A.C. en Egipto y Mesopotamia, ya surgió la necesidad de comunicarse entre los suyos por medio de mensajes que no puedieran ser leídos por sus enemigos. Si miramos el desarrollo del ser humano a lo largo de la historia, vemos que cada vez se necesitan métodos más complejos para ocultar la información. Por ejemplo, los romanos inventaron su propio sistema (Cifrado César) en el año 60 A.C. y los alemanes su propio hardware (1918) que apodaron Enigma, cuyo algoritmo descifrado por Alan Turing daría paso a la Informática tal y como la conocemos hoy en día.

A día de hoy, la criptografía (práctica de la criptología) juega un papel cada vez más importante en la preservación de la privacidad, evitando que usuarios no autorizados accedan a datos sensibles. Gracias a la globalización, la hiperconexión que proporciona Internet y la velocidad de los computadores, la información sensible es cada vez más vulnerable y fácilmente adquirible.

El avance exponencial de la tecnología trae con el paso de los años el peligro de romper con los esquemas de cifrado actuales. Se cree que dichos esquemas seguirán siendo útiles en los años venideros, pero ante tal incertidumbre se ha decidido, con este proyecto, aportar una posible solución que, aunque es posible que no sea definitiva, sí sería suficiente en caso de que los algoritmos estándar fuesen finalmente incapaces de hacer frente a la capacidad de cómputo de un ordenador. Para conseguir esto, el objetivo es elaborar un esquema de cifrado basado en AES que, posteriormente, pueda ser implementado en cualquier clase de aplicación como la que se va a presentar en el proyecto.

Parte de la finalidad de este proyecto no solo es desarrollar el esquema ya mencionado, sino también ponerlo en práctica mediante una aplicación de escritorio que sea fácil de usar. La aplicación deberá ser capaz de encriptar y desencriptar texto y documentos de diferentes formatos, además de cambiar el tamaño de letra y el tema para que sea más accesible.

**Contextualización**

Las prácticas se han realizado en DISID, una consultora tecnológica valenciana que, por medio de un modelo de socio tecnológico, realiza proyectos de transformación digital.

La empresa cuenta con más de 300 proyectos en más de diez países y una plantilla bilingüe (entre 100 y 200 empleados) con una media de 32 años, todos certificados en Scrum.

Algunas de las tecnologías en las que se especializa DISID son Spring, Angular, Cloud, MuleSoft, IBM Cloud Pak for Data y Appian.

DISID se sitúa en:

* Av. Menéndez y Pelayo - 46010 Valencia (España), Sede Central.
* Upper Ground London SE1 9PD (Reino Unido).

Principales clientes de la empresa:

* Servicios urbanos e interurbanos: Aceinsa, Alvac, Stadler, SAV Agricultores de la Vega de Valencia, Becsa, Innovia Coptalia, Sacyr, Sandetel, Moa, Ferroser, Los Serranos.
* Tráfico y transporte: Stadler, Indra, Hytera, Nasa.
* Administraciones públicas: Turisme Comunitat Valenciana, Ayuntamiento de Alicante, Diputación de Castellón, Ajuntament de València, Cabildo de Tenerife, Diputación de Sevilla, Diputación de León, Consell Insular de Menorca, Generalitat Valenciana, Junta de Castilla y León, Diputació de València, Junta de Andalucía, Diputación de Valladolid, Diputación de Badajoz, Diputació Tarragona, Generalitat de Catalunya.
* Retail: Domingo Alonso, Mango, Lladró.
* Consultoría tecnológica: Ciber, Deutsche Börse, Alfatec, Planes.
* Sanidad: Sanitas, Centro Nacional de Dosimetría, IVO, Ministerio de Sanidad y Consumo, La Fe.

**Gestión del proyecto**

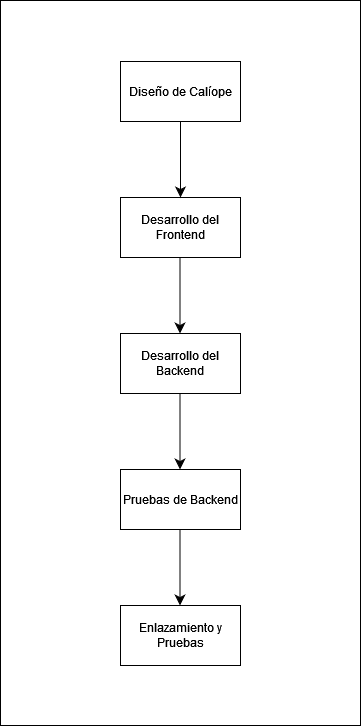
Para gestionar el proyecto es importante tener en cuenta dos factores: la planificación de las tareas distribuidas por semanas y el orden en el que se realizarán. A continuación se matizan ambos puntos.

**Método de trabajo**

El diseño, desarrollo, implementación y pruebas del proyecto se divide en cinco semanas, que tienen que cubrir las siguientes tareas:

* ***Diseño de Calíope***: diseño esquemático del algoritmo, tanto de la encriptación como de la desencriptación. Inlcuye también qué operaciones matemáticas se usarán y el flujo de datos, así como las normas de uso y recomendaciones del mismo
* ***Desarrollo del front end de la aplicación***: programación de la interfaz de usuario y de las interacciones que habrá a disposición.
* ***Desarrollo del back end de la aplicación***: implementación de Calíope en código fuente. Además, el back end se encargará del tratado de texto y documentos de varios formatos.
* ***Realización de pruebas del back end***: comprobar que Calíope se ha implementado de forma correcta y que es eficiente, tomando tiempos de ejecución del código.
* ***Enlazamiento del front end con el back end y realización de pruebas de la aplicación final***: una vez se han desarrollado ambas partes por separado, conectarlas para que trabajen en conjunto y realizar las pruebas necesarias para asegurar el correcto funcionamiento de la aplicación.

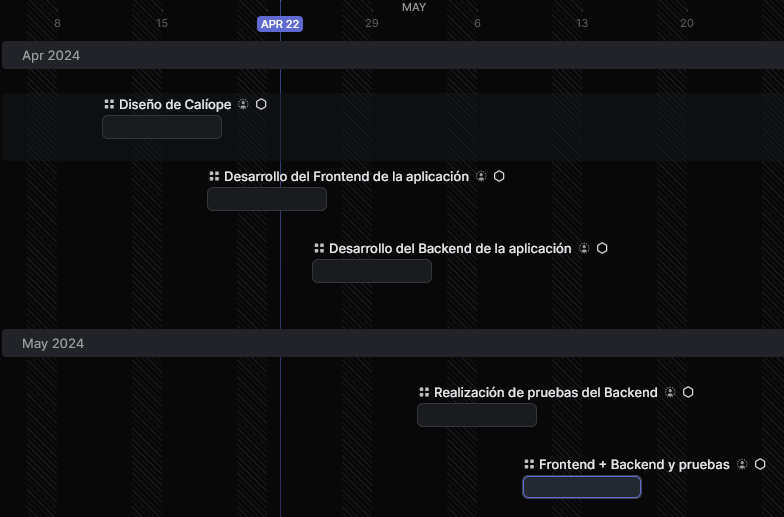
Las fechas en las que se realizarán las tareas quedan detallas en el próximo apartado. En cuanto al orden de las mismas, se muestran de forma simplificada en la siguiente imagen (ver siguiente página):



*Esquema realizado con draw.io*

**Planificación temporal**

Las tareas se desarrollarán a lo largo de cinco semanas tal y como se muestra en la siguiente línea de tiempo:



*Planificación realizada con Linear*

Las semanas se distribuyen en los siguientes días:

* ***Del 11 al 18 de abril***: diseño de Calíope.
* ***Del 18 al 25 de abril***: desarrollo del front end de la aplicación.
* ***Del 25 de abril al 2 de marzo***: desarrollo del back end de la aplicación.
* ***Del 2 al 9 de marzo***: realización de pruebas del back end.
* ***Del 9 al 16 de marzo***: enlazamiento del back end con el front end y realización de pruebas de la aplicación final.

**Herramientas Hardware y Software utilizadas**

A pesar de la complejidad de Calíope, solo se requiere de tres tecnologías para el desarrollo del proyecto en cuanto a software se refiere:

* ***Python***: es un lenguaje de programación de alto nivel, interpretado y multiparadigma diseñado por Guido Van Rossum en 1991. El principal motivo por el cual se ha escogido este lenguaje es la gran reducción de costes de producción que implica hacer uso del mismo. Se utilizará para la construcción de todo el proyecto, tanto del back end, como del front end, como de la implementación de Calíope.
* ***Flet***: es un framework para Python que permite desarrollar aplicaciones móbiles, web y de escritorio incluso sin disponer de experiencia en desarrollo front end. Flet está basado en Flutter, un framework de desarrollo de aplicaciones multiplataforma hecho por Google. La facilidad con la que Flet permite desarrollar aplicaciones es el motivo por el cual se ha escogido dicho framework. Se usará para todo el desarrollo de la interfaz de usuario, es decir, el front end.
* ***JSON***: es un formato ligero de intercambio de datos fácil de leer y escribir para los humanos, a la vez que fácil de interpretar y generar para las máquinas. Es independiente del lenguaje de programación pero usa convenios similares a lenguajes de programación de la familia de C. Este formato se utilizará para el archivo de configuración de la aplicación por su simplicidad y facilidad de uso.

Para la realización de todas las pruebas de la aplicación, se hará uso de un ordenador con las siguientes especificaciones:

* [Seagate BarraCuda 3.5" 2TB SATA 3](https://www.pccomponentes.com/seagate-barracuda-35-2tb-sata-3).
* [***Kioxia EXCERIA 480GB SSD SATA***](https://www.pccomponentes.com/kioxia-exceria-480gb-ssd-sata).
* [***Corsair Vengeance LPX DDR4 3200MHz PC4-25600 32GB 2x16GB CL16***](https://www.pccomponentes.com/corsair-vengeance-lpx-ddr4-3200mhz-pc4-25600-32gb-2x16gb-cl16).
* [Gigabyte B660M DS3H DDR4](https://www.pccomponentes.com/gigabyte-b660m-ds3h-ddr4).
* [***MSI GeForce RTX 3070 Ti VENTUS 3X OC 8GB GDDR6X***](https://www.pccomponentes.com/msi-geforce-rtx-3070-ti-ventus-3x-oc-8gb-gddr6x).
* [***Intel Core i5-12400F 2.5 GHz***](https://www.pccomponentes.com/intel-core-i5-12400f-25-ghz).
* [Thermaltake Toughpower GF1 750W 80 Plus Gold Full Modular](https://www.pccomponentes.com/thermaltake-toughpower-gf1-750w-80-plus-gold-full-modular).

Es importante remarcar que se han señalado en negrita las especificaciones que más influyen directamente en la ejecución de la aplicación, así como de todas las funciones con las que cumple.

El proyecto se programará en Visual Studio Code, un entorno de desarrollo potente y ligero disponible para Windows, macOS y Linux. Se puede integrar con Git para el control de versiones y permite depurar y refactorizar código. Hay muchos motivos por los que usar este IDE: es fácil de usar, intuitivo y satisface cualquier clase de necesidad que un programador pueda llegar a tener por la amplia variedad de extensiones que son facilitadas por la comunidad (actualmente una de las comunidades con mayor cantidad de usuarios del mundo). Además, dispone de resaltado de sintaxis y autocompletado inteligente de código.