Concurs de treballs de **Recerca-Blanes 2021**

Títol del treball: Estudi matemàtic i programació de la màquina Enigma

Autor/a: Ivan Endrino

Tutor/a: Ivan Fernández

Introducció:

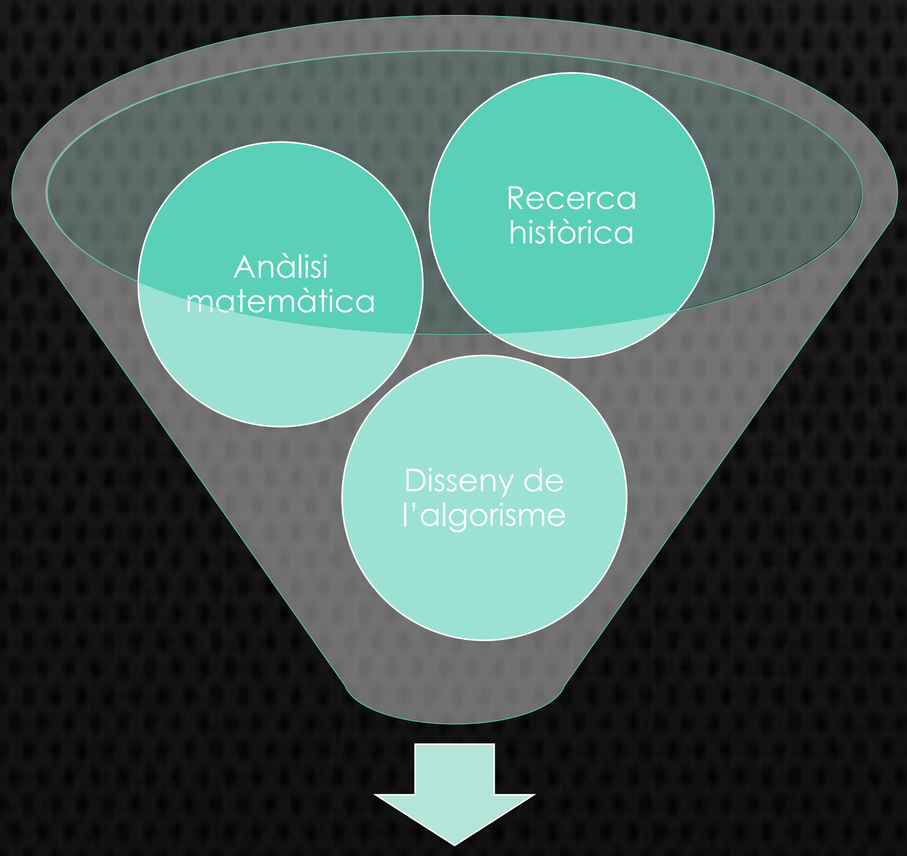
La màquina Enigma va ser una eina utilitzada per l'armada alemanya durant la Segona Guerra Mundial per **garantir** una **comunicació segura**. Aquest aparell electromecànic va ser el maldecap de la intel·ligència aliada, ja que xifrava els missatges dels nazis mitjançant un sistema de **rotors**.

Objectiu:

L'objectiu final de la recerca és la **creació d'un programa** que simuli la màquina Enigma I mitjançant el llenguatge **Python.**

Metodologia:

- **Investigar** la seva història per contextualitzar el seu sorgiment i detectar els possibles precursors alhora que s'aprofundeix en el seu funcionament.
- **Analitzar** l'Enigma matemàticament i dissenyar l'algorisme de xifrat per tal de facilitar la programació.
- **Representar** l'algorisme mitjançant diagrames de flux.
- **Deduir i descriure** la relació matemàtica entre la lletra real i la xifrada.
- **Programar** l'algorisme amb Python dividint-lo en petits mòduls utilitzant els diagrames de flux com a base. Alhora, fer ús de la relació matemàtica trobada amb l'objectiu de simplificar la programació.



Conclusions:

Envers la part més històrica, s'ha conclòs que l'Enigma troba els seus precursors en els seus models anteriors que anaven afegint a poc a poc millores fins a arribar a ella.

S'ha assolit l'objectiu de crear un programa que simuli el funcionament de l'Enigma i aquest ha superat diverses proves de funcionament satisfactòriament. Gràcies a haver descrit la relació matemàtica i haver representat l'algorisme a programar en diversos diagrames, la programació ha estat més senzilla. Tot i això, per culpa dels desconeixements en l'àmbit informàtic, el programa no té interfície gràfica i s'executa directament a la consola.

AJUNTAMENT DE BLANES

ins sa palomera

Agraïments: Agraeixo al tutor, als professors que m'han ajudat i a la meva família.