期末專題書面報告

讓小朋友也能了解的密碼學

11044127-劉瑀柔

## 研究動機跟目標

1. 為什麼要做這個題目

因為自己本身的兼職是帶夏令營，所以想要讓它們體驗看看密碼學。

1. 預計達到的目標

小朋友可以順利答對我出的題目

## 研究方法及步驟

1. 初始概念及規劃

先製作基本教具，或是圖表、跟基礎題目，讓它們能夠了解其中規律

1. 網頁架設

當它們了解其中規律也可以自己設計密碼的時候，讓它們上我寫的網站去答題，答題成功即達到目標

邏輯:進網頁點即你要測驗的項目(ex:傳統密碼學-換位)然後開始測驗

網頁的部分採用html當框架  
題目放在js裡面依據使用者點選主題然後隨機跑出該主題的題目供選擇

然後回答正確之後一秒跳下一題

## 實驗結果與展示

因為還沒有開始教小朋友，所以只能先展示網頁本身，分成兩種階段

第一個階段是比較初階的，包含了傳統密碼學的換位與取代

第二個階段是比較進階的，包含了finiteField跟AES

網站本身不僅僅是給小朋友驗收成果的，同時也是給我複習的

Github 連結: [期末專題 (xu61029.github.io)](https://xu61029.github.io/112-1-final/)

# 未來規劃

因為是要帶小朋友認識，所以我認為只有文字敘述不好，所以之後應該會做一個3D的unity遊戲讓它們能邊玩邊了解原理，同時網站會在之後增加課堂上其他內容，讓自己也能夠複習並且運用