HW3

分組及分工

- B10415041 曾增宇
  - 加密
  - IP, PC-1 ... 抄寫
  - 置換演算法
  - f-function
- B10415049 陳祐丞
  - 解密
  - SBox 抄寫
  - round-key function
  - main function

建置環境

- Python 3.6.5 :: Anaconda, Inc. on windows 10

使用方式

- 命令列輸入 `python main.py -e <plaintext> <key>` or `python main.py -d <ciphertext> <key>`
- 明文、密文、key 輸入 16 進制，ex `0x1234567890abcdef` or `1234567890abcdef`

實作過程困難與心得

- 在實做的過程中，將每一步驟都寫出來所花費的時間其實不長，但是因為我們沒辦法比對每一步驟的結果，因此輸出結果與網路上的加密不符時很難除錯，只能一小部分一小部分仔細看，最後發現整體邏輯沒錯，僅僅是幾個字元的錯誤就造成結果完全不一樣，因此下一次撰寫程式時一定要更加仔細!

截圖

```
D:\AllProjects\python\Information-Security-Homework\HW3\Code>python main.py -e 0xabcdef0123456789 0xafafafafafafafaf
0x4c30fc30fb2b0bff

D:\AllProjects\python\Information-Security-Homework\HW3\Code>python main.py -d 0x4c30fc30fb2b0bff 0xafafafafafafafaf
0xabcdef0123456789

D:\AllProjects\python\Information-Security-Homework\HW3\Code>python main.py -e 0xabbccddeeff11223344 0xaaaa1234ffff5678
0x296213ab041afd5bee004579adf6081

D:\AllProjects\python\Information-Security-Homework\HW3\Code>python main.py -d 0x296213ab041afd5bee004579adf6081 0xaaaa1234ffff5678
0xabbccddeeff11223344
```