HW2 說明文件

分工

四資工三甲 B10632026 吳苡瑄 Encrypt + Decrypt

四不分三戊 B1063043 林玉庭

開發環境

Windows10 Python3

結果與截圖

```
PS D:\school\Security\Information_Security_Class\hw2> python3 ./EncryptDES.py 0xAFAFAFAFAFAFAFAF 0xabcdef0123456789
0x4C30FC30FB2B0BFF
PS D:\school\Security\Information_Security_Class\hw2> python3 ./DecryptDES.py 0xAFAFAFAFAFAFAFAF 0x4C30FC30FB2B0BFF
0xabcdef0123456789
```

遇到困難與心得

只要先花時間了解 DES 的運作方式之後，實作部分都很簡單，而且加密寫完以後基本上解密也只需要再多改一些小小的地方就能完成了，只是比較繁瑣而已，而且比較難 debug，所以我一開始就先把 function 都列出來再一一去實作就很快，debug 的時候也可以一部分一部分慢慢追，印出來也比較方便，跟上次比起來我覺得這次作業比較簡單的多，好像沒有遇到什麼困難，底下還有好多空白我不知道要打什麼我就多打一點流程好了。

我有特別分出來的 function 部分

permutation

參數分別是 permutation 要用的表跟要被 permutation 的 block，幾乎整個程式裡面都會一直用到，使用率很高的一個 function。

s_box

在 f_function 裡面會被呼叫到，因為 S box 的部分比較特別所以特別分出來寫，參數是要處理的 block 和這個 block 是第幾小塊。

f_function

就是做 f_function 裡面的內容，被 feistel 呼叫

feistel

主要就是叫了 f_function、做 XOR、左右交換

key_shift

就是負責 shift，在製作 key 的時候會常常被用到