資訊安全導論HW2

B10815044 謝鈞曜 解密

B10815057 廖聖郝 加密

### 加密

讀取輸入，用strtoull讀取16進制數字，放到bitset裡



Permutation function，輸出的每一位元為輸入經過index 對應table轉換

因為bitset與table的位元順序是相反的，所以要做一些特別處理



根據DES演算法，將plaintext經過IP permutation轉換

Key經過PC1 permutation轉換，從64bit變為56bit



Plaintext與key都切割為左右部分



進行16輪的加密，每輪根據shift table對Key做左旋位元，我的做法是將左旋1bit與2bit直接寫成permutation table，讓程式一致性更高。



然後將左右部分的key combine起來，concat的原理是將bitset轉成string去相連，再轉回bitset。



對combine後的key做PC2 permutation，產生這個round的48bit key



F function輸入右半部的plaintext與round key，輸出與plaintext左半部XOR，最後將plaintext左右部分交換



組合plaintext左右部分，然後經過FP就是加密完成的密文



輸出經過16進制與大寫轉換，並且設定不到16個字最前面要補零



F function 內容:

將右半部plaintext從32bit 擴充成48bit，再與round key XOR



跑過8個S box，迴圈每次會計算該6 bit對應到S box中的row col



根據row col從當前S box中取出4bit輸出，assign到輸出變數

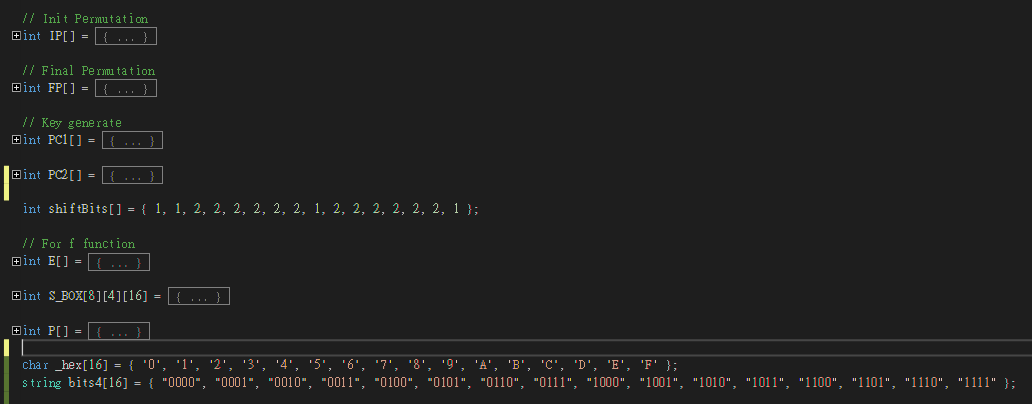


輸出再經過P permutation轉換



### 解密

先將會使用到的table全部列出來



將input做一些基本的處理，例如補0



生成16個subkey



F function實做



解密主要演算法



將輸出從bitset<64>轉成0x

