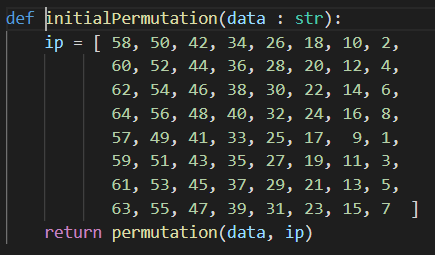
HW2 - DES

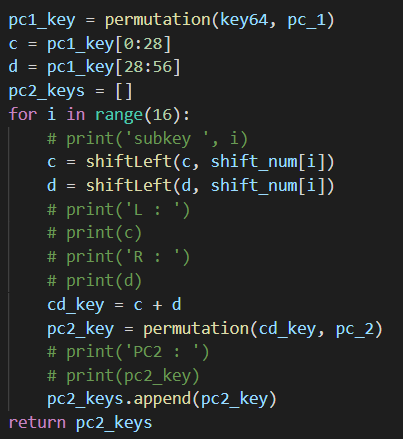
這次使用的語言為Python，實作方式為，首先將輸入字串以8個字元為單位分割放入陣列中，未滿8字元則塞入空白。接下來進FOR迴圈，FOR迴圈疊代次數依據陣列大小而定，進入FOR迴圈後會先將字元轉成ASCII，然後再轉成二進制數字。



接下來做IP，由於後面寫Code時發現permutation的動作都一致，僅差在Table不同，因此將permutation獨立成一個函式



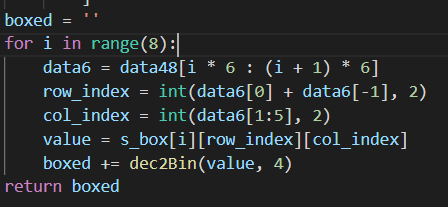
再來將IP後的結果切成兩半，此時開始處理KEY，將KEY讀入轉成二進制，並做PC1，然後切割成C、D。再來做位移，並將C、D合併做PC2，以上PC1後的流程重複16次，並將結果存於陣列。



回到主程式

接下來就是照換位的順序，將Subkey與右邊資料做F-Function

而F-Function就跑一堆S-Box將每個S-Box上的6 bit位元依index找到相應的值並轉成2進制回傳(4 bit)



F-function的結果與左邊資料做XOR，再來重複16次，最後左右合併，再將結果做FP，存入一個字串，結束此次LOOP，最後所有的字元都處理完後，將此字串轉成16進制Print出來即完成。

