離散期末報告 0417081 楊賀傑

A.解決問題定義：要AC&&!TLE，AC要了解rsa encryption and decryption的原理。
Encryption:
C＝（M＾E）％N
Decryption:
N=p*q, r=(p-1)(q-1), ED=1mod r求出D, M=(C^D)%N, then convert to char and string。
ＴＬＥ：
質因數分解：Fermat’s factorization theorem
求Ｄ：用ext_gcd演算法
大指數取模：modular exponentiation
B.所使用之演算法：encrypt，用modular exponentiation，decrypt用 Fermat’s factorization theorem, ext_gcd and modular exponentiation
C.自己想的演算法：最直覺就是用暴力解，之後有想到用指數折半的方式再相乘取模
D.結果：在加密那題，在沒有用演算法的情況下得到了15分，之後改了modular exponetiation後就全對了，可能是在取模卡太久了，導致TLE。
第二題只拿到18分可能大數的部分沒處理好。

E.團隊分工：
自己一個人一組，一個人理解個目，不會時問問助教，一個人寫code，一個人debug，一個人寫報告。
F. 程式建置環境：
原本在xcode用c寫，但因為遇到大數的問題，所以改用mac os內建的terminal python2。
G.參考文獻：wikipedia、博客園