RSA加解密程式設計作業說明

(I)輸入資料:

1.公鑰e, 至少可允許 $1 < e < 10^5$

2. p, q兩個質數, 至少可允許 $1 < p < 10^9$, $1 < q < 10^9$

(若你的程式能支援長整數運算，例如: p、q的值可分別允許

至10^{20}，或更大的值，請特別註明，可獲得額外的Bonus加分)

3.原始字串資料M, (如HELLO, 最長可允許256個字元)。

(II)輸出資料:

1.用e將M加密後的資料C

2.私鑰d

3.用d將C解密出的資料M

注意事項:

(1) 明文字串與整數之間的對應關係，請依照課本的字母轉換表:

(A=00, B=01, C=02, D=03, … , Z=25, 以及「空白」= 26)。

(2) 加解密的區塊大小，請設為每區塊2個字元，不滿2個字元的區塊，

請於其後補上「空白」(即對應之整數值為26)。

(例如: 「HELLO」，對應整數爲 0704 1111 1426)