

# Reading Quiz #08

姓名：\_\_\_\_\_ 系級：\_\_\_\_\_ 學號：\_\_\_\_\_ 分數：\_\_\_\_\_

閱讀第5章第2節(第116頁)及第8章第2節(第179頁)並回答下列問題

1. 分解因數的困難性造就出一個非常實用的密碼系統，  
稱之為\_\_\_\_\_。
  
2. 將上題所回答的密碼系統中，如何個加解密描述如下：  
(三毛要傳遞信息  $x$  給四郎)
  - (a) 四郎選取\_\_\_\_\_, 並\_\_\_\_\_得  $n =$ \_\_\_\_\_。
  - (b) 然後選取加密次幂  $e$  使得\_\_\_\_\_, 將\_\_\_\_\_ 經由公開的頻道告知三毛，但\_\_\_\_\_ 則保密。
  - (c) 三毛將欲傳送的信息轉換成一個數  $m$ , 如果  $m > n$  三毛必需將  $m$  分割成區塊  $\{m_1, m_2, m_3, \dots, m_k\}$ , 使得所有的區塊  $m_i$  都小於  $n$ 。
  - (d) 計算密文  $\{c_1, c_2, \dots, c_k\}$  如下: \_\_\_\_\_, 然後將密文  $\{c_1, c_2, \dots, c_k\}$  傳送給四郎。
  - (e) 因為只有四郎知道\_\_\_\_\_, 所以他可以算出\_\_\_\_\_。
  - (f) 再透過延伸輾轉相除法求得解密鑰匙  $d$ , 滿足\_\_\_\_\_。
  - (g) 最後四郎將密文  $c_i$  \_\_\_\_\_, 如此即可還原成明文並讀取此信息: \_\_\_\_\_。

3. 離散對數的困難性造就另一個非常實用的密碼系統，

稱之為\_\_\_\_\_。

4. 將上題所回答的密碼系統中，如何個加解密描述如下：

(三毛要傳遞信息  $x$  給四郎)

(a) 四郎選取\_\_\_\_\_及\_\_\_\_\_。

(b) 四郎也選取一秘密整數  $a$  且計算\_\_\_\_\_。

(c) 四郎將\_\_\_\_\_公開，但將  $a$  保持私密。

(d) 三毛則根據四郎所公開的鑰匙，選取\_\_\_\_\_

並算出  $y_1$  與  $y_2$ , 此處

$y_1 \equiv$  \_\_\_\_\_ 而  $y_2 \equiv$  \_\_\_\_\_ (mod  $p$ )。

(e) 三毛送出  $(y_1, y_2)$  給四郎，然後四郎據此解密如下：

\_\_\_\_\_。

這就是\_\_\_\_\_於\_\_\_\_\_年所提出的密碼系統。這個系統是一個\_\_\_\_\_系統。因為密文不僅僅與明文有關，而且跟三毛所選取的\_\_\_\_\_有關。所以同一明文就會產生許許多多不同的密文。用口語化的方式來描述，這個系統是如此運作的：

明文  $x$  透過乘以  $\beta^k$  來偽裝產生密文  $y_2$ , 而  $\alpha^k$  之值也當成密文的一部分一起送過去。四郎因為知道秘密次幂  $a$ , 故可透過  $\alpha^k$  之值來算出  $\beta^k$  之值; 然後他再將  $y_2$  除以  $\beta^k$  來解除偽裝得回原有的信息  $x$ 。