Reading Quiz #7

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，

   稱之爲_____ 。

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) 然後選取加密次冪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$\{m_1, m_2, m_3, \cdots, m_k\}$,使得所有的區塊$m_i$都小於$n$。

   (d) 計算密文$\{c_1, c_2, \cdots, c_k\}$如下：_____,然後將密文$\{c_1, c_2, \cdots, c_k\}$傳送給四郎。

   (e) 因爲只有四郎知道_____ ,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 $y_2 \equiv$ ________________ $\pmod{p}$。

(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β^k來偽裝產生密文y_2,而α^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冪a,故可透過α^k之值來算出β^k之值;然後他再將y_2除以β^k來解除偽裝得回原有的信息x。