預習閱讀測驗八

姓名：_____ 系級：_____學號(序號)：_____ 分數：_____

閱讀第五章第二節(第116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：_____ 。