預習測驗八

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 m 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, 假設 $m < n$ 。
   (d) 計算密文 c 如下: [ ], 然後將密文 c 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 [ ]，如此即可還原成明文並讀取此信息： [ ] 。