預習閱讀測驗八

姓名：＿＿＿＿＿＿＿＿ 系級：＿＿＿＿ 學號：＿＿＿＿＿＿＿＿＿＿ 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) 準備工作：首先四郎選取 [ ] p_4, q_4，並 [ ] 得 $n_4 =$ [ ]；然後選取與 [ ] 互質的加密次冪 e_4，得到四郎的公開鑰匙 [ ] 而 [ ] 爲其私密鑰匙。另一方的三毛則必須將所要傳送的信息 x 數位化成 m_3 (假設 $m_3 < n_4$)。

   (b) 三毛加密：三毛計算密文 $c_3 \equiv$ [ ]，然後將密文 c_3 公開傳送給四郎。

   (c) 四郎解密：四郎用他的私密鑰匙 [ ]，算出 [ ]；再利用延伸輾轉相除求得解密鑰匙 d_4，滿足 [ ]。最後四郎將密文 c_3 在模 n_4 之下取 [ ] 次冪，即可還原成明文並讀取此信息：[ ]。