預習閱讀測驗九

姓名：_____ 系級：_____ 學號：_____ 分數：_____

閱讀第八章第一及第二節 (pages 177-179) 並回答下列問題

1. 何謂離散對數問題？

2. 離散對數的困難性造就另一個非常實用的密碼系統，稱之爲 [ ] 。

3. 上題所回答的密碼系統中：假設三毛要傳遞數位信息 m_3 給四郎，演算法如下

   (a) 準備工作：四郎選 [ ] p_4 及 [ ] $\alpha_4 \pmod{p_4}$，也選秘密整數 a_4 並計算 $\beta_4 \equiv$ [ ]；將 [ ] 公開，但 a_4 保持私密。

   (b) 三毛加密：根據四郎的公鑰，選 [ ] k_3 並計算 (c_1, c_2)，此處 $c_1 \equiv$ [ ] $\pmod{p_4}$ $c_2 \equiv$ [ ] $\pmod{p_4}$。她送出密碼文 (c_1, c_2) 給四郎。

   (c) 四郎解密：四郎計算 [ ]，此乃原來的明文 m_3。

   這就是 [ ] 於 [ ] 年所提出的密碼系統。這個系統是一個 [ ] 系統。因爲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：

   [ ]