

預習測驗九

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

閱讀第八章第一及第二節 (pages 177-180) 並回答下列問題

1. 何謂離散對數問題?

2. 離散對數問題的困難性造就出一個非常實用的密碼系統，稱之為

。

3. 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

$y_1 \equiv$ $(\text{mod } p)$ 而 $y_2 \equiv$ $(\text{mod } p)$ 。

(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幂 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 。