預習閱讀測驗九

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

閱讀第八章第一及第二節(pages 116-118, 119-123)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. 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

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

   (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:

   明文x透過乘以β^k來僞裝產生密文y_2,而α^k之值也當成密文的一部分一起送過去。四郎因爲知道秘密次冪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來解除僞裝得回原有的信息x。