預習測驗10

姓名：_____ 序號：____ 學號：_____ 分數：6 5 4 3 2

預習第十講 (215-227頁) 並完成下列問題

1. 固定一質數 p。 令 α 與 β 為模 p 之下的兩個非零整數並考慮方程式

$$\alpha^x \equiv \beta \pmod{p}。$$

(a) 上面同餘式中，解 x 的問題稱之為 $\boxed{}$

(b) 上面同餘式中，若 $p = 17, \alpha = 2, \beta = 7$ 則 $x =$ $\boxed{}$

(c) 上面同餘式中，若 $p = 17, \alpha = 3, \beta = 7$ 則 $x =$ $\boxed{}$

2. 寫下艾加莫密碼系統演算法的六大步驟。

3. 若艾加莫演算法之公開鑰匙為 $p = 31, \alpha = 3, \beta = 17$ ，則解密用的私鑰 a 為何？

4. 承上題，若密碼文為 $(y_1, y_2) = (13, 27)$ ，則明文為何？