Reading Quiz #10

姓名：_____ 系級：_____學號：_____ 分數：_____

閱讀第10章第10節(第242頁)並回答下列問題

1. 記得艾爾給默(ElGamal)密碼系統嗎?可簡單敘述如下:

   三毛要傳遞信息x給四郎，所以四郎選取一個大質數p及一個整數$\alpha \pmod p$。他也選取一秘密整數a_4且計算$\beta \equiv \alpha^{a_4} \pmod p$。四郎將$p, \alpha, \beta$公開，但將$a_4$保持私密。三毛選取一個隨機整數$k_3$並算出密文$(y_1, y_2)$,此處

   $y_1 \equiv$ _____ $\pmod p$, 而 $y_2 \equiv$ _____ $\pmod p$。

   她送出(y_1, y_2)給四郎，然後四郎據此解密如下：

   $$x \equiv \text{\_\_\_\_\_} \pmod p。$$

2. 橢圓曲線版的艾爾給默(ElGamal)密碼系統就是把上面艾爾給默(ElGamal)密碼系統中的乘法變加法而次冪變倍數而已。現在描述如下：四郎選取一橢圓曲線$E \pmod p$, p爲一大質數；然後選取橢圓曲線E上一點α及一秘密整數a_4。他得算出

   $$\beta = \text{\_\_\_\_\_}。$$

   四郎將此兩點α, β公開，但將a_4保持私密。三毛將她要送給四郎的信息表示成橢圓曲線E上的點x(見第二節)；然後選取一個隨機整數k_3並算出

   $$y_1 = \text{\_\_\_\_\_} \quad 與 \quad y_2 = \text{\_\_\_\_\_}。$$

   她送出(y_1, y_2)給四郎，而四郎據此解密如下：

   $$x = \text{\_\_\_\_\_}。$$