

# Reading Quiz #9

姓名：\_\_\_\_\_ 系級：\_\_\_\_\_ 學號：\_\_\_\_\_ 分數：\_\_\_\_\_

閱讀第 10 章第 1-4 節 (第 217-227 頁) 並回答下列問題

1. 何謂橢圓曲線? 請舉例並畫出其圖形.

2. 何時何人將橢圓曲線引進密碼術當中?

3. 何人指出可使用橢圓曲線來分解因數?

4. 選取你自己的瑞沙葉 (RSA) 密碼系統公鑰, 並書寫在此

$n =$  \_\_\_\_\_

$e =$  \_\_\_\_\_

5. 選取你自己的艾爾給默 (ElGamal) 密碼系統公鑰, 並書寫在此

$p =$  \_\_\_\_\_

$\alpha =$  \_\_\_\_\_

$\beta =$  \_\_\_\_\_