

Reading Quiz #6

姓名：_____ 系級：_____ 學號：_____ 分數：_____

閱讀第8章第1及第2節 (pages 116-118, 119-123) 並回答下列問題

1. 分解因數的困難性造就出一個非常實用的密碼系統，
稱之為 _____ 。
2. 何謂離散對數問題？
3. 離散對數問題的困難度與分解因數的困難度相比如何？
4. 離散對數的困難性造就另一個非常實用的密碼系統，
稱之為 _____ 。
5. 將上題所回答的密碼系統中，如何個加解密描述一下。