11 模數運算-在亂數產生器與密碼學的運用

指導教授	桑慧敏 教授
參與學生	u870840 曾立維 u870847 陳昶旭

摘　　要

模數運算是一種看似簡單易懂的運算方法，然而運用在某些方面卻能產生關鍵性的效果。模數運算最特別之處，在於它對應的值域是一個有限場(Finite Field)，也就是它運算後可能出現的解是有限的，本次專題所欲探討的也就是利用模數運算的這種特性，在不同領域中的應用。我們提出兩個主要部分來做討論，一個是模數在亂數產生器上的應用，另一個則是模數在密碼學中所扮演的角色。

在亂數產生器的領域，雖然有各種不同的產生器型式，然而目前所使用最普遍的仍然是線性同餘法，然而在幾個產生器之間，我們如何比較它們孰優孰劣呢？我們討論其隨機性、週期性便可得到結果。我們透過幾種檢定方法來判斷亂數產生器的隨機性，包括全域性之理論檢定與區域性之經驗檢定，前者例如有光譜檢定；後者又分兩類：一種檢驗其獨立性，例如相關檢定；另一種檢驗其均勻分布性，例如卡方檢定、序列檢定。本次專題我們由現有的數種商業軟體中所使用的亂數產生器挑選出若干個，並進行檢定與討論。

密碼學是模數運算的另一個重要應用領域。本次專題我們主要在探討對稱性密碼系統與非對稱性密碼的功能與差異，我們集中焦點在使用模數運算做為加密手段的幾種加密系統：秘密鑰匙系統的密碼轉盤、凱撒密碼，以及公開鑰匙加密系統的RSA加密方法，尤其是RSA加密方法，它是目前為止最被廣泛使用的公開鑰匙系統，在電子交易、網路銀行與電子資料交換等必須在公開網路下從事的秘密訊息傳遞更是產生了革命性的影響。我們分別開發不同之加密程式實際測試加密與解密的過程，並探討不同加密系統背後的理論，以了解其之所以可以確保安全性的關鍵所在，以及各種加密方法的優缺點。

回目錄