序

本書為密碼學與網路安全的相關理論與實務上所涉及的概念作介紹。在本書中，共分成 10 章，第一章的“**密碼學的故事**”至第十章的 “**數位鑑識**”。由最原始的安全概念直至近來 Internet 上最新主題/應用/趨勢皆囊括於其中。在第一章中，介紹密碼學這門學問的源起與發展，直至最新量子電腦/密碼的發展。在撰寫本章時，Simon Singh 所著的一本書：The Code Book：The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 1999，及相關的附錄文獻，給了相當有趣/玩味/深入的觀點，得以窺探密碼之妙與神奇。在參閱之下亦豐富了本章的撰寫。在此對於各式密碼學的研究學者/作者抱以誠摯的尊崇。

在第二章至第六章為密碼學與資訊安全的相關技術/原理/發展與應用的討論，盼讀者能透過相關範例的導入了解密碼學不再只是理論，而是可以用簡潔的方式表現，並藉此來拉近我們生活的距離。在第七章至第八章的內容，則為資訊科技社會所得面臨的資訊安全危機/事件/應用問題，諸如 CYBERCRIME/IDS/IPS/HONEYPOT 等，此部分皆有深入/實務的討論。最後 2 章的第九章與第十章，討論了未來的資訊安全偵查趨勢的電腦/網路數位證據觀念/技術/法律等主題。在資安危機意識逐漸高漲的時代，如何建立一套標準的證據鑑定程序，並與資訊安全所發展的技術結合，實為一門有趣且值得深入探究的新領域學問。

吾人一直以 Team Work 為研究/討論/決策的主軸。再次地這本書的完成，依然是群策群力的工作模式。ICCL(Information Cryptology & Construction Lab.)的伙伴/研究人員(黃嘉宏/柯宏叡 林錦新 張智暐 陳世豪 郭至桓 鍾佩芳 黃彥琳)為此本書的付出之心力，吾人銘記在心。尤其學生之一**宏叡**對本書後半章節的繆力整理，更是舒緩不少我在本書付梓時間上的壓力。我在辦公室/研究室門上擺滿了許多的鐘/錶，其一之意是提醒時間的珍貴，得把握一天 24n，n>0，小時的分/秒時間啊! 對於宏叡的努力與對此書的表白，在以下的兩段的自

序文中可看出端倪。

近幾年來電腦與網路的快速發展，從得資訊相關領域也跟著蓬勃發展。然而，隨著以往所強調的方便、快速等，到現在更加強調的是安全。如同早期製作網頁者，多是以美工排版、內容、互動性為主要考量，安全被視為未節。而如今，在追求建立優良網站時，就一定也要重視到資訊安全。否則，辛苦的成果可能就會在片刻間遭人摧毀殆盡。

每個人的看法或同或不同，都有賴每個人對事物所具備知識與想法而定。這本書提供了一個有關資訊安全領域中的廣泛介紹，也提供了我們的看法與想法，乃至於我們所認為可行對策。這可能是我們的洞見，也可能是我們的一廂情願。實情為何，都是需要大家共同去思考，並不吝於提供建議，方能使我們所提出解決方案更為完備。此次，能有機會在吾師的指導之下，能夠將所知、所學化為文字，成為篇章，在資訊安全這個領域的推展上，略盡棉力，在此對吾師致上衷心的感謝。

努力的背後，Family 絕對是最重要的支柱，In Particular for Rebecca/G.Y./G.R.， My Love。 最後吾人以經常對 ICCL 的期許(禪語)與讀者分享：

「學習 as well as 忘」;

「研究 as well as 痴」;

「做事 as well as 心」;

「生活 as well as 混」;

「情感 as well as 容」。

並盼此書得以為科技發展/研究之文獻做初淺整理，以為此相關領域的參酌。

王旭正/柯宏叡

于 ICCL

April 2004