

資訊與網路安全－秘密通訊與數位鑑識新技法



- 作者：[王旭正，柯宏叡，ICCL-資訊密碼暨建構實驗室](#)
- 出版社：[博碩](#)
- 出版日期：2006 年 03 月 28 日
- 語言：繁體中文 ISBN：9575278909
- 裝訂：平裝

- 定價：[580](#) 元 優惠價：9 折 522 元

內容簡介

[top](#)

本書資訊與網路安全-秘密通訊與數位鑑識新技法 (Information and Network Security:Eyes of Secret – State of the Art on Internet Security and Digital Forensics)為古往今來秘密通訊、密碼學(Cryptography)與網際網路安全 (Internet Security)的相關理論與實務上所涉及的概念作介紹。

書中共分五大部分，由第一部分的“人類的秘密開始”為開端介紹盤古說地的秘密故事，藉此了解秘密隱藏此奧妙學問的來龍去脈，並體會科學數學之美妙與神奇；接著探討網路通訊密碼解譯的藝術與技巧。

第二部分則為“密碼學的基礎、技術與應用”。在這個部分中筆者安排了數論的基礎知識，並介紹現代密碼學的重要發展/技術/應用。

第三部分開始進入“網際網路安全與實務”的範疇，介紹現在目前網路通訊的主軸 VPN、加密軟體 PGP(Pretty Good Privacy)、Web-mail 的機制、討論 PKI 世界的組成架構及使用 / 操作方式、電子商務需注意的安全協定 ..等等。

第四部分為“資訊隱藏的玄機”，介紹資訊隱藏並以「數位浮水印技術」、「偽裝法」等議題切入，探討如何運用之及其所產生的問題。另外專章介紹視覺的秘密及其發展與應用。

第五部分則為“新興網路犯罪與電腦鑑識科學”。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 CYBER-CRIME：詐欺/賭博/洗錢/...等新興網路犯罪的資訊安全議題，進行深入/實務的討論。

作者簡介

王旭正

中央警察大學資訊管理學系 副教授

學歷：國立臺灣大學電機工程所資訊科學組博士

專長：資訊安全技術、密碼學、資料工程處理

網站：資訊密碼暨決策管理實驗室 (ICCL)

詳細資料

[top](#)

- 規格：平裝 / 720 頁 / 普級 / 部分彩頁 / 初版
- 出版地：台灣

目錄

[top](#)

Part I 人類的秘密

1 秘密通訊的故事 Stories of Ciphers and Communications

2 古典密碼的設計與破譯 Art of Classic CryptanalysisPart II 密碼學的基礎、技術與應用

- 3 數的世界 Fundamental Number Theory
- 4 對稱式金鑰系統 Symmetric Key System
- 5 新加密標準-AES Advanced Encryption Standard
- 6 公開金鑰系統 Public Key System
- 7 HASH 技術與秘密分享 HASH and Secret SharingPart
- III 網際網路安全與實務
- 8 IP 安全通訊協定 IPSEC
- 9 PGP, S/MIME, SSL&SET
- 10 電子郵件安全 Email Security
- 11 公開金鑰基礎建設 Public Key Infrastructure
- 12 電子付款與交易證據 Electronic Payments and Evidence Clues
- 13 無線通訊安全 Wireless Security
- 14 網路安全防衛 Network Intrusion/Protection SystemPart
- IV 資訊隱藏的玄機
- 15 資訊隱藏 Information Hiding
- 16 視覺密碼與安全 Visual CryptographyPart V 新興網路犯罪與電腦鑑識科學
- 17 電腦犯罪的偵查與資訊安全 Cyber-crime Investigation and Information Security
- 18 數位證據 Digital Evidence
- 19 數位鑑識 Digital Forensics
- 20 新興鑑識工具 Emerging Toolkits in Computer Forensics
- 附錄
- A ICCL 技術報告附錄
- B 推薦網站附錄
- C 索引