

《認識密碼學的第一本書》

图书基本信息

书名：《認識密碼學的第一本書》

13位ISBN编号：9789861372008

出版时间：2015-2-26

作者：王旭正

页数：208

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu111.com

《認識密碼學的第一本書》

內容概要

中央警大教授親自解密！

從故事中認識「密碼學」，了解這門

資訊安全、資料藏密、數位鑑識、防範犯罪等領域都需要的重要學科！

密碼，無所不在！

密碼學，助你守住你的秘密！

帳號密碼的祕密、身分的祕密、私密相簿的祕密、戰爭的祕密、外交與軍事的祕密……

一旦遭人竊取或揭露，後果不堪設想！

為什麼看似平常的搜尋關鍵字，能暴露深藏在我們心中的祕密？

社交網路與朋友的互動，竟然正是歹徒蒐集資料的天堂？

讓人無所遁形的「人肉搜索」真能彰顯正義？

為了國家安全而全面監控，個人隱私可有保障？

數字密碼無所不在的今天，如何透過了解其中機制，保護自我安全？

中央警大的專家團隊，以故事教你由淺入深認識這門關於如何隱密傳遞資訊的科學，理解網路時代加密與解密的危機與關鍵知識。

我們用我們個人的隱私作為貨幣，來換取網路的「免費服務」。

我們需要真正意識到目前正發生在我們身上的隱私問題，了解免費的代價，認識網路定義隱私、個人空間及「人」的方式。

《認識密碼學的第一本書》

書籍目錄

第1章 遲來二十年的情書

繩結 / 羅馬數字系統 / 古巴比倫數字系統 / 阿拉伯數字系統

第2章 獨一無二？孤芳自賞？

質數與合數 / 質數的個數 / 梅森質數 / 費馬質數1231 / 中國剩餘定理 / 摩斯密碼

第3章 密碼？亂碼？傻傻分不清楚

快樂數 / 親和數 / 哥德巴赫猜想 / 斯巴達密碼棒 / 凱薩密碼法 / 維吉尼爾密碼法 / 英格瑪密碼機

第4章 不是不可能的鹹魚翻身

對稱式及非對稱式金鑰密碼系統 / 著名加密標準：DES / 3-DES、AES、RSA

第5章 金鑰也能這樣飛舞

混合公開金鑰密碼系統與對稱式密碼系統 / HASH函數 / HASH函數檢查訊息「正確性」與「完整性」 / 數位簽章 / 數位簽章的特性 / 雙重簽章 / 中間人攻擊 / 憑證 / 公開金鑰基礎建設

第6章 永恆的唯一

網路相簿私密照曝光 / 維基解密 / 憂患意識 / 自我的唯一

第7章 數位放大鏡

數位證據 / 數位鑑識的必要程序 / 數位證據的特性 / 鑑識陣線聯盟 / 反鑑識 / 數位浮水印

《認識密碼學的第一本書》

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu111.com