

數普書籍推薦~《世界第一簡單密碼學(修訂版)》

一、書籍資料

書名：世界第一簡單密碼學(修訂版)(マンガでわかる暗号)

作者：三谷政昭, 佐藤伸一

漫畫：Hinoki Iderou

譯者：林羿紋

出版年：2020 年

出版社：世茂出版社

二、難度：☆☆

三、標記：數學小說、數學學習

四、書介

本書為「世界第一簡單」系列中的一本，兩位作者的專業領域都是數位通訊處理工學。本書維持一貫的風格，以幾位人物配合簡單的情節推進數學知識的說明與應用，漫畫風格明快有趣，數學知識配合漫畫圖形、簡化的事例來做說明，讓讀者可以比較容易地吸收生硬的數學知識。

本書解釋密碼學的觀念與幾種常用的編碼與解碼系統，其目錄如下：

第一章 密碼學基礎

第二章 共通金鑰(對稱金鑰)加密系統

第三章 公開金鑰加密系統

第四章 實際的密碼應用

以公開金鑰加密系統為例，作者從質數與質因數分解的概念說起，到模數運算、費馬小定理與歐拉定理，將此加密系統需要的數學概念做簡單的說明，之後再到密碼系統的生成與解密，算是相當完整的過程解說。

為了不讓生硬的數學知識影響讀者閱讀的意願，以及帶出密碼學的需求感，本書的數學知識配合某位「怪盜」留下的密碼線索而推進，由女主角(高中生)負責解說數學、另一位女記者擔任附和者的角色，適時充當數學概念的進一步解說，同時由女高中生的哥哥(警察)來擔任插科打諢的角色，以平衡書裡生硬的數學知識，讓讀者可以在較輕鬆的心情下閱讀與學習。