密碼學 回家作業

班級：資網三 A　　學號：D1094181017　　姓名：張育丞

前言

本次將介紹並推薦為「碼書：編碼與解碼的戰爭」，這本書的來歷與我高中的密碼學體驗課程有關，再修習該課程的同時正在進行基於區塊鏈完成智慧電網的實驗被老師所悉知，後因正逢高三即將畢業之時，因此老師將其書贈予於我，為紀念該書除了加裝書套，更連同原文音譯版本都進行納入收藏。

基本資料

原文書名：The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography.

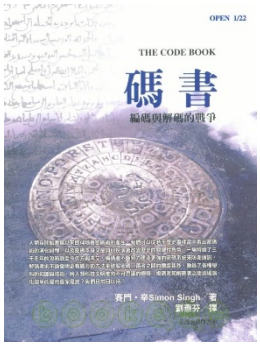
中文書名：碼書:編碼與解碼的戰爭

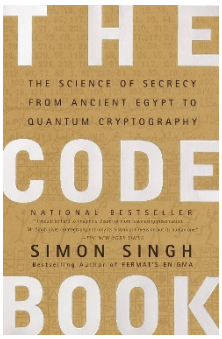
ISBN：9789570516722

作者：Simon Singh

翻譯：劉燕芬

出版年：2000





簡介

此書分為八大章節與 8 個附錄，並設有一套解碼挑戰和對應的解答，內文中穿插許多古人的畫像與名言，甚至古早加密法的示意圖，隨然文字較多，但已經夠吸引人了。書籍內容從原始的凱薩加密至量子密碼的世界觀相當多元且富有歷史與教育意義，真誠推薦給想要聽故事學習數學的人，雖然此書早已絕版。

章節節錄與重點段落分享

節錄章節為第八章-躍進量子世界，第八章是書籍中最尾段的章節，敘述的是前人應用生活中的例子去思考密碼學，在現代我們將採用電腦與許多公式進行包裝與加密。

對於內文中讓我們思考的點有幾個，其一關於暴風雨攻擊為最常見的一種手段，這種就像是隔牆有耳的概念，也就是利用電磁訊號再目標地點附近以高強度訊號進行低強度訊號的擷取，此方法可以在訊號傳遞於對方之前或者當事人接收當下進行訊號取得，優點在於可以不受到加密技術影響取得資訊，這也是許多港

片演的竊聽橋段，值得一提的是美國對於裝設屏蔽材料需政府許可，這樣感覺美國的偵搜手法都這樣？

接下來關於新型科技的密鑰取得，這部分作者舉特洛伊木馬病毒為例，從中可以清楚知道其實我的隱私無法完全不被洩漏，除了網路使用使得個資被上傳，其次就是有些軟體於後台進行監控，當收到對應私密金鑰派發就進行監聽，從而在有心人士需要私密金鑰時，能為他所用。

接踵而來的內容就是我較為熟悉的 RSA，此命名來自三位作者的姓氏縮寫，而此加密法也是目前現代較為常用的，從敘述中可以清楚知道採用為非對稱加密，此時會疑問是何謂非對稱加密，以及對稱加密為何？對此以我認知帶來一個簡單得例子：

- ✧ 對稱性加密：傳統門鎖，所有人鑰匙規格相同，任何名單成員都可以使用自身鑰匙進行開鎖與上鎖。
- ✧ 非對稱性加密：特製保險箱，鑰匙分別有兩把，其一負責開鎖，另一把為上鎖，若要開啟該保險箱或進行上鎖都需要專用的才能進行。
- ✧ 新型加密(認證)：現在許多平台會傳送簡訊或者使用 Auth 每 20 秒進行更換認證金鑰的形式。

該文章接下來就在講量子力學與密碼學需要推倒要使用幾千億年，以及後密碼學的深度探索以及映射條件等。

吸引我的原因/心得

主要吸引我的原因是 RSA 我有使用過，雖然不清楚大家對於密碼學是否有相對的認知，但是密碼學並非等同於區塊鏈以及加密貨幣，後兩者皆是逐步延伸的技術而已，從密碼學的微觀視野我們可以悉知的就是許多機率數學在更加聚焦會發現其實就是物理，以加密的過程就是許多鏡像處理，當 A 能映射出 A，B 能映射出 B 那就是加密，同時也牽涉到所謂的共鳴，因為兩者的認同及共識產生的演算法機制，因此有些人在密碼學學習的過程會講述共識演算法的概觀思維，此外若以巨觀來看密碼學其實應用領域真的不少，防毒軟體、對抗網路思維、防火牆等以及大家耳熟能詳的區塊鏈都是。

那到底區塊鏈是甚麼與密碼學的關係何在？首先區塊鏈的重點來自於去中心化，也就是無中心集權管制的概念，那很多人一定會好奇那他為甚麼可以做為一個貨幣的底層技術，主要是帳本與協議，先說明帳本概念，此帳本擁有者為所有參與區塊鏈的人，而帳本將記載關於大家交易的信息，再來說說協議，協議主要就是大家互相約定俗成的產物，簡單說就是今天有 A、B、C、D 四人，他們各自有帳本，他們約定不要有人管理班費問題，每當有人要借錢或領錢時需要由另外兩人進行驗證確保過程正常，當正常時就將其記錄至帳本中，因此若還款時同

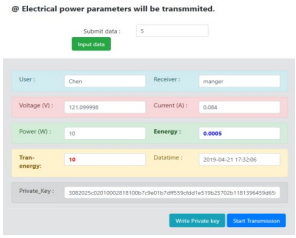
樣有公證人在場並且記載於帳本中，此好處為何？當有人挪用公款或者另一人試圖包庇，就可以快速查驗，此外若有新成員加入時也能讓他快速知道金流狀況。而比特幣就是延續此方法並衍生進行的貨幣，此外因為帳本的存在以及交易紀錄的連續性使得區塊鏈可以不受干擾進行，每當包庇或肆意修改帳本，被覺察時亦可透過觀察大家的帳本一致性並且採多數決以及最常驗證資訊來驗證，使得包庇與肆意修改帳本的人進行裁決並恢復其內容，因此可以相當穩定，由此可以建立良好的信任機制，此思維也呼應現階段許多法幣的價值。

關於法幣的價值來自信任，因為失去信任的法幣將會導致鮮少與市面流通匯率不正等間接使其殞落，至於法幣的匯率與黃金從量有關就不在此探討。

技術分享

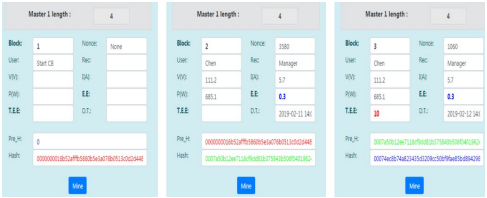
4 年前在因緣際會下開啟智慧電網的建設與實作，並在當時的 GitHub 提供相關的 Source Code，因此結識密碼學，相關案例的附圖如下，爾後再利用報告好好分享操作與細節。

圖一、金鑰產生



圖二交易介面

挖礦界面



礦池檢視