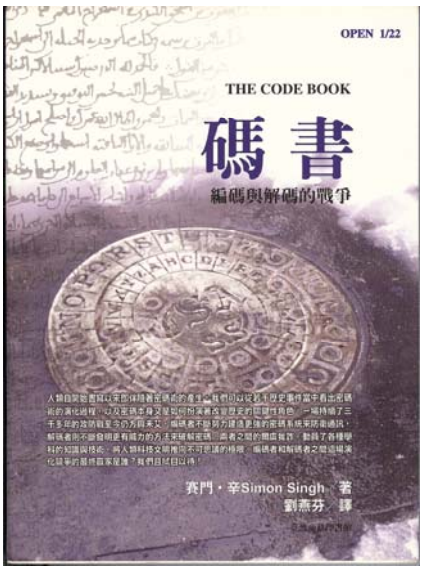
# 評論《碼書：編碼與解碼的戰爭》

黃哲男
台南女中

書名：碼書：編碼與解碼的戰爭 (The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography)[1]
作者：賽門・辛 (Simon Singh)
譯者：劉燕芬
出版社：台北：臺灣商務印書館股份有限公司
出版年份：2000
出版資料：平裝共 464 頁，定價 390 元
國際書碼：ISBN957-05-1672-0




## 一、前言

數千年來，不管是君王或將領，都需要一套很有效率的通訊模式來治理國家、指揮軍隊。他們當然也深知萬一訊息落入不當人士手裡，讓敵國窺知機密，或讓反對勢力獲取關鍵資訊時，所會產生的嚴重後果。密碼術——種僞裝訊息，唯有指定的收信人才能讀出原意的技術一就是因應敵人攔截機密的威脅而發展出來的。

爲了保密，每個國家都設立了密碼部門，發明及使用最好的密碼來確保通訊安全。相對地，敵方的解碼專家則努力破解密碼以偷取機密。這些解碼專家可說是語言學的煉金術士；就像煉金術士想將石頭煉成黃金，他們則嘗試從無意義的符號堆裡揣度出合理的文字。密碼術的歷史其實就是幾世紀以來編碼者與解碼者之間的戰爭史，他們的戰爭是一場影響歷史走向甚鉅的知識武器競賽。[2]

歷史的標點符號是密碼打上去的。它們決定了戰爭勝敗，也結束了一些國君

[1] 原文版書名爲：The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography.
[2] 作者序 001 頁。

的性命。[3]有人說，首度運用芥子氣與氯氣的第一次世界大戰，可稱之爲化學家的戰爭，以原子彈結束的第二次世界大戰，可稱爲物理學家的戰爭。以此類推，有人相信第三次世界大戰將是數學家的戰爭，因爲數學家將掌控下一場大戰的重要武器—資訊。數學家早已投入研發密碼系統保護軍方資訊的工作。而在密碼戰中負責破解這些密碼的，當然也是數學家。[4]

編碼者與解碼者持久戰事，激發了一連串顯著的科學突破。編碼者不斷努力建造更強的密碼系統來防衛通訊，解碼者則不斷發明更有威力的方法來破解密碼。在這場攻防拉鋸戰中，雙方都廣泛援引了各學科的知識與技術—從數學到語言學，從資訊理論到量子理論無一不被徵召投入戰場。相對地，編碼者與解碼者也豐富了這些學科的內容，他們的工作加速了科技的發展，尤其是現代電腦的研發。[5]

[3] 作者序 002 頁。
[4] 作者序 003 頁。
[5] 作者序 002 頁。

## 二、內容簡介

筆者永遠忘不了小時候讀到福爾摩斯偵探故事中的小人密碼文，還記得那時候好幾天廢寢忘食，就爲了破解那些密碼，也許就如同約翰・查威克所言：「揭開秘密的衝動是人類根深蒂固的天性」，亦可能是爲了與偶像福爾摩斯競賽解密的好勝心。結果？當然是福爾摩斯大勝！筆者對那密碼文一點輒都沒有。

後來雖然早已習慣在電腦的對話框中輸入密碼以保護或解開一些資料，或連上網路進入某個工作環境，但是從來沒有想過，原來密碼與數學理論息息相關（當然也和心理學非常有關！），直到在大學的數學課程中接觸到一些密碼學的理論，才知道原來密碼學其實就是數學的一個分支。

《碼書：編碼與解碼的戰爭》（底下簡稱《碼書》）一書主要是介紹密碼的演化史，以及其在各領域（如戰爭、資訊通訊等）的應用。舉歷史上的實例加以介紹編碼與解碼的理論，就像一位說書人在述說著故事，同時又像一位老師不斷地解釋故事中密碼的理論，非常有趣也非常吸引人，讀者很容易著迷（一本好書理當如此！），並且將會對密碼學的理論有了初步的瞭解。

全書架構共分成八章、十個附錄，以及一個密碼挑戰：「十階通達一萬英鎊」，筆者根據編碼與解碼主要使用的領域或方法及影響，將各章分成五個部分：

| 章　名 | 領域或方法 | 影　響 |
|---|---|---|
| 第一章 蘇格蘭瑪麗女王的密碼 | 語言學、統計學、數學 | 編碼與解碼技術的改良 |
| 第二章 無法破解的密碼 | | |
| 第三章 秘密書寫的機械化 | 心理學、數學 | 電腦的發明 |
| 第四章 破解「奇謎」 | | |
| 第五章 語言障礙 | 語言學、考古學 | 多元文化的研究成果 |
| 第六章 愛麗絲和巴伯公開鑰匙 | 數學 | 密碼學的數學理論及資訊科學等領域的蓬勃發展 |
| 第七章 極佳隱私 | | |
| 第八章 躍進量子世界 | 量子理論 | 量子電腦的研究 |

附錄分別爲：

A：小說《虛空》開頭第一段
B：頻率分析的基本要訣
C：所謂的「聖經密碼」
D：豬圈密碼
E：波雷費密碼
F：ADFGVX 密碼
G：單次鑰匙簿的回收缺點
H：《每日電訊報》縱橫字謎的秘密
I：尚待解譯的古文字
J：RSA 所使用的數學

作者以歷史上非常有名的蘇格蘭瑪麗女王的審判案引入，從歷史上的事件（或者可以輕鬆一點地看待成歷史上的故事）出發，在事件中帶出密碼的關鍵地位，但又不急著解釋該事件中所使用的密碼術，轉而介紹密碼術的演進；將歷史問題留著，改而介紹各種密碼術的歷史與方法，以及利用這些密碼術的事件背後所隱藏的秘密，可以引起讀者極大的好奇心，順著作者的介紹，瞭解了密碼術的演進以及在歷史上的重要性，並且可以學到一些密碼術的原理；最後作者再以瑪

麗女王的事件結束第一章，作爲一個段落的休止。

第二章起，作者介紹了更多的歷史事件以及更複雜的密碼術，大部分的歷史事件皆與寶藏或外交、戰爭有關，也提到了一些耳熟能詳的小說中的密碼故事，其中部分的事件常常是現代電影取材的由來，譬如《國家寶藏》部分的情節便源自於畢爾密碼中使用美國《獨立宣言》一事。

第一章所介紹的密碼術主要是替代法以及移位法等等，第二章則需要比較多的語言學及簡單的統計知識，利用統計分析字母出現的頻率，再比對密碼文中字母或符號所出現的情況，正是統計學與語言學結合應用的好例子。前兩章雖然表面上沒有數學的痕跡，但其實骨子裡還是數學，只是讀者不易發現而已，教師可以稍微解釋，學生便能很快地就理解箇中奧妙。

第三、四章介紹了密碼學的一個新時代，也就是編碼與解碼的機械化；雖然破解密碼還是需要一些語言學或是其他領域的相關知識與洞察力，但機械化的引入，使得數學在編碼與解碼的過程中更顯得重要，也使得編碼與解碼的效率更佳，更符合外交及戰爭的需求，並且因爲這樣的需求從而設計出現代電腦，讀者將可以從此歷史上的事件瞭解，現代電腦的出現並非偶然，而是因爲有外交及戰爭上的需求，並且是和密碼學息息相關的。

第五章算是本書中較爲獨立的一章，所介紹的「密碼」是較爲廣義的，本章提到納瓦荷[6]語在第二次世界大戰時被美國當作通訊的語言，一種尚未被軸心國所瞭解的語言，因此也就不需要特別加密，所以也就不怕被破解，當然缺點就是作爲編碼與解碼之「鑰匙」的通訊兵，如果落入軸心國的手中，那麼這一套「密碼」就可能會被掌握而無法再使用，電影《獵風行動》便是記錄這樣的一段故事。本章所介紹的另外一部份則是破解考古學上的密碼—線形文字 B，許多考古學家將未知的古文字作爲一種挑戰，利用遺跡、文物或是歷史上的紀錄、傳說以及其他文化的遺產來破解這些古文字，這不就像是古人留下了許多的密碼，而後人則靠著考古學所知的蛛絲馬跡去解碼嗎？因此作者在本章也花了一些篇幅敘述了考古學上的解碼成就，以更廣義的方式符合本書的主題，避免讀者誤解編碼與解碼只是書中其他章節所討論的部分而已。

編碼及解碼中所使用的金鑰（key）在傳統的密碼術中扮演著非常關鍵的地位，只要金鑰被得知，密碼就等於被破解了，但保護和傳送金鑰又非常困難，如何順利地將金鑰傳送給正確的人，反而變成傳統密碼術中最重要的部分。第六、七章所介紹的密碼學正是突破傳送金鑰困難的新方法：DES 與 RSA，金鑰不再需要秘密地傳送，而是可以公開；這兩種密碼理論的出現，正是數學力量的展現，密碼學進入了歷史上新的一頁！作者在這兩章舉了許多非常容易理解的例子來解釋相關的理論，對於一本希望讓廣大讀者弄懂密碼學的科普讀物而言，這是非常棒的，但是如果讀者想要完整地瞭解背後的數學理論，則結構性稍嫌不足。其中，第六章主要著重在 DES 與 RSA 的介紹，第七章則討論了在這樣強大的編碼技術出現之後，所引發的國家安全與個人隱私的相關部分。[7]

第八章介紹了目前科技以及密碼學的最新進展—量子電腦與量子密碼，作者舉了許多的例子來介紹這個部分，但可能礙於篇幅以及量子電腦與量子密碼本身就較難以理解，所以本章讀來並不易懂，但筆者相信，讀者仍可從本章窺知密碼學的最新發展。

---

[6] 美國的原住民族。

[7] 建議延伸閱讀《數位密碼》與欣賞《終極密碼戰（Mercury Rising）》。

## 三、評論

讀完本書，讀者將會瞭解許多電影中無法理解的劇情，譬如：在電影《獵風行動》中，爲什麼納瓦荷族密碼兵是如此的重要，以至於尼可拉斯凱吉所飾演的安德斯需要拼命的保護他，以確保解碼順利，另一方面美軍非常擔心密碼兵如果被俘虜，將會造成密碼外流，此時安德斯的任務便是想辦法在密碼兵被日軍屈打成招前殺掉他。或是電影《獵殺 U-571》描述同盟國以擄獲的一艘德軍潛艇爲掩護，假借維修補給之名登上德國的 U 型潛艦，趁機搶奪密碼機（其實密碼簿才是重點），後來不幸困在艦艇 U571 上，從此與德軍及同盟國的軍隊展開了一場混戰。這兩部電影都呈現了一個重點，在兩場戰爭中，雙方都爲了維護或爭奪密碼（如果把密碼兵也視爲密碼的話）而費盡心力，如果只是單純地欣賞電影，大概比較難聚焦在密碼的重要性上吧！如此便難理解密碼爲何如此重要。

《碼書》一書內容豐富，介紹許多歷史上與密碼有關的事例，密碼學的理論介紹亦算清楚，讀完此書會對密碼學有著初步的認識，並且可能因此而喜愛上密碼學。然而《碼書》雖然介紹了不少密碼學的數學理論，但筆者認爲，部分內容可能對高中生而言不夠清楚仔細，所以，另外推薦一本與密碼學相關的科普讀物《數學小魔女》，此書由一位 1999 年愛爾蘭、歐洲青少年科學家首獎得主的女高中生與其數學家父親共同寫成，與《碼書》一書相比，此書沒有精彩絕倫、高潮迭起的歷史事件作爲敘述主軸，而是著重在密碼學的數學理論（當然是高中生能懂的部分，而且有一部分正是高一上學期一開學便會學到的內容），因此，在讀完《碼書》之後再閱讀此書，便會對一些數學理論的部分更清楚。至於《數學小魔女》的後半部，則是敘述作者參加科展的經驗，對於高中生而言，這也是一個非常好的學習榜樣與目標。

《碼書》與《數學小魔女》讀完之後，建議可以再閱讀丹・布朗（即《達文西密碼》的作者）所寫的《數位密碼》，如此一來，除了能享受故事中懸疑緊張的氣氛之外，更能理解書中相關的密碼術語，以及密碼學本身對於國家安全、資訊安全等等的重要性！

從 96 學年度起，筆者所任教的台南女中便將《碼書》、《數學小魔女》、《數位密碼》三本書列入新生入學的閱讀書目，並建議學生應合併閱讀，而非僅讀其中一本；附錄 1 正是節錄自某位學生的心得。附錄 2 則是筆者於高三段考所設計的題目，許多學生表示：那是她們高中三年中所做過最有趣、最有意思的題目了！

解數學問題的過程，不也像是解密一般，充滿思考、洞察、困頓與驚喜！是一種與數學之神或創造該問題的人之競賽與對決！如何讓學生體會破解問題的喜悅，從而喜歡數學、學習數學，正是我們教師所應共同努力的方向。

## 延伸閱讀：

Flannery, S. & Flannery, D. (2001). **數學小魔女**。（葉偉文譯）。台北市：天下文化。
丹・布朗（Brown, D.）(2005). **數位密碼**。（宋瑛堂譯）。台北市：時報文化。

## 延伸欣賞：

《獵風行動（Windtalkers）》。
《獵殺 U-571（U-571）》。
《終極密碼戰（Mercury Rising）》。

《國家寶藏：古籍秘辛（National Treasure II）》。[8]

**附錄：**

1. 看了碼書之後，才知道獵殺 U571 裡面，爲什麼兩邊要去「獵殺」那一艘潛水艇，雖然電影裡面有提到密碼機和密碼，但我從來不知道那密碼有那麼重要，現在終於能理解那是多麼的重要了。

……獵風行動裡面的主角雖然是尼可拉斯凱吉，可是現在才知道那個密碼兵在戰爭中才是真正的主角。

至於數位密碼，以前看的時候就是純粹當小說，裡面有一堆密碼的技術不懂，不過不管還是能看，現在看了碼書，就比較清楚那些技術，也才知道原來密碼對一個國家的安全是這麼大，所以爲了維護密碼，什麼勾當都幹得出來！所以隱私權的維護是很重要的，我們需要更難破解的密碼。

還有啊！我爸爸[9]當初一直覺得很奇怪，怎麼學校會選一本歷史的書、一本數學的書、一本小說[10]合在一起當作指定閱讀，但是他讀了之後，他終於能理解，只不過數學的部分他還是不懂啊～　XDDD　但是他覺得很有趣，他說他以前都以爲瑪麗女王的審判，那些文件是關鍵，沒想到密碼才是關鍵！

2. 將英文字母轉換成數字，底下爲對照表：

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 0＝空格 | 3=C | 6=F | 9=I | 12=L | 15=O | 18=R | 21=U | 24=X |
| 1=A | 4=D | 7=G | 10=J | 13=M | 16=P | 19=S | 22=V | 25=Y |
| 2=B | 5=E | 8=H | 11=K | 14=N | 17=Q | 20=T | 23=W | 26=Z |

假設有一段訊息「WOULD　YOU　MARRY　ME」，透過上述之對照表，即可轉換成一個數列：

23, 15, 21, 12, 4, 0, 25, 15 21, 0, 13, 1, 18, 18, 25, 0, 13, 5

請特別注意，上述訊息中包含 4 個單字，單字與單字間各有 1 個空格，由於空格以 0 代替，故轉換後之數列中有三項爲 0。將轉換後之數列以第一行、第二行、…、第八行之順序，依序填入一個 $2\times 9$ 之矩陣，可得矩陣：

$$A=\begin{bmatrix}23 & 21 & 4 & 25 & 21 & 13 & 18 & 25 & 13\\ 15 & 12 & 0 & 15 & 0 & 1 & 18 & 0 & 5\end{bmatrix}$$

顯然，隨著訊息之長短不同，矩陣 $A$ 之階數便不同，例如有另一訊息，經過轉換之後爲一個 100 項的數列，此時 $A$ 便爲一個 $2\times 50$ 之矩陣。

設矩陣 $K=\begin{bmatrix}1 & 3\\ 0 & 1\end{bmatrix}$，若 $B=KA$，則

$$B=\begin{bmatrix}68 & 57 & 4 & 70 & 21 & 16 & 72 & 25 & 28\\ 15 & 12 & 0 & 15 & 0 & 1 & 18 & 0 & 5\end{bmatrix}$$

將矩陣 $B$ 之諸元以第一行、第二行、…、第八行之順序，依序排成一個數列：

---

[8] 本部電影預告片的部分片段即請《碼書》作者 Simon Singh 解說密碼學的相關理論。

[9] 該名學生的父親爲大學歷史系教授，因《碼書》書後的國家圖書館出版品預行編目資料中， 將本書分類至歷史類。

[10] 從 96 學年度起，筆者任教的台南女中便將《碼書》、《數學小魔女》、《數位密碼》三本書列入新生入學的閱讀書目，並建議學生應合併閱讀，而非僅讀其中一本。

68, 15, 57, 12, 4, 0, 70, 15, 21, 0, 16, 1, 72, 18, 25, 0, 28, 5

則稱此數列爲訊息「WOULD　YOU　MARRY　ME」之密碼文，此過程稱爲加密，矩陣 $K$ 稱爲金鑰。顯然金鑰只能爲加密者與解密者雙方所有，要是被第三者得知，便可以輕易地破解密碼文。

設金鑰爲 $K=\begin{bmatrix}1 & 3\\ 0 & 1\end{bmatrix}$，有一段密碼文如下：

40, 5, 19, 0, 9, 0, 49, 15

請解譯出原訊息爲何？

解答：

法一：

$\because B=\begin{bmatrix}40 & 19 & 9 & 49\\ 5 & 0 & 0 & 15\end{bmatrix}$，$B=KA$

$\therefore A=K^{-1}B$

又 $K^{-1}=\begin{bmatrix}1 & -3\\ 0 & 1\end{bmatrix}$

$\Rightarrow A=K^{-1}B=\begin{bmatrix}1 & -3\\ 0 & 1\end{bmatrix}\begin{bmatrix}40 & 19 & 9 & 49\\ 5 & 0 & 0 & 15\end{bmatrix}=\begin{bmatrix}25 & 19 & 9 & 4\\ 5 & 0 & 0 & 15\end{bmatrix}$

所以原訊息所對應之數列爲 25, 5, 19, 0, 9, 0, 4, 15

$\Rightarrow$原訊息爲「YES　I　DO」

說明：本方法是筆者期待學生使用的解法，希望學生能看得懂題目，並從題目中選取解題所需要的資訊，進而使用反矩陣解題；雖然反矩陣是本題解題的關鍵，但爲了避免學生計算反矩陣時發生計算錯誤的憾事，故矩陣 $B$ 選用 $2\times4$ 矩陣，且矩陣 $K$ 也選用一個容易計算反矩陣的數據。

法二：

設 $A=\begin{bmatrix}a & c & e & g\\ b & d & f & h\end{bmatrix}$

則 $KA=\begin{bmatrix}1 & 3\\ 0 & 1\end{bmatrix}\begin{bmatrix}a & c & e & g\\ b & d & f & h\end{bmatrix}=\begin{bmatrix}a+3b & c+3d & e+3f & g+3h\\ b & d & f & h\end{bmatrix}$

又 $B=\begin{bmatrix}40 & 19 & 9 & 49\\ 5 & 0 & 0 & 15\end{bmatrix}$，$B=KA$

故 $\begin{bmatrix}40 & 19 & 9 & 49\\ 5 & 0 & 0 & 15\end{bmatrix}=\begin{bmatrix}a+3b & c+3d & e+3f & g+3h\\ b & d & f & h\end{bmatrix}$

$\Rightarrow a+3b=40$，$b=5$，$c+3d=19$，$d=0$，$e+3f=9$，$f=0$，$g+3h=49$，$h=15$

$\Rightarrow A=\begin{bmatrix}a & c & e & g\\ b & d & f & h\end{bmatrix}=\begin{bmatrix}25 & 19 & 9 & 4\\ 5 & 0 & 0 & 15\end{bmatrix}$

所以原訊息所對應之數列爲 25, 5, 19, 0, 9, 0, 4, 15

$\Rightarrow$原訊息爲「YES　I　DO」

說明：少部分學生採用此方法，算是一種直接解法，讀懂題意之後，直接利

用數據列式解聯立，因爲本題數據簡單，故採用此法亦可以很快將答案求出。

法三：

設 $A=\begin{bmatrix} a & c & e & g \\ 5 & 0 & 0 & 15 \end{bmatrix}$

則 $KA=\begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & c & e & g \\ b & d & f & h \end{bmatrix}=\begin{bmatrix} a+15 & c & e & g+45 \\ 5 & 0 & 0 & 15 \end{bmatrix}$

又 $B=\begin{bmatrix} 40 & 19 & 9 & 49 \\ 5 & 0 & 0 & 15 \end{bmatrix}$，$B=KA$

故 $\begin{bmatrix} 40 & 19 & 9 & 49 \\ 5 & 0 & 0 & 15 \end{bmatrix}=\begin{bmatrix} a+15 & c & e & g+45 \\ 5 & 0 & 0 & 15 \end{bmatrix}$

$\Rightarrow A=\begin{bmatrix} a & c & e & g \\ b & d & f & h \end{bmatrix}=\begin{bmatrix} 25 & 19 & 9 & 4 \\ 5 & 0 & 0 & 15 \end{bmatrix}$

所以原訊息所對應之數列爲 25, 5, 19, 0, 9, 0, 4, 15

⇒原訊息爲「YES　I　DO」

說明：此解法與法二類似，但假設矩陣 $A$ 之各元時，第二列之各元直接假設真實的數據，主要是學生已觀察到矩陣 $K$ 的特性。這樣的學生，是不是就像《碼書》中提到的，解碼者常需要對密碼進行觀察，需要靈感、需要洞察力，以便可以更快及更順利地破解密碼。

法四：

算一算密碼文的字數，又注意到有兩個零，所以會有兩個空格，題幹中的訊息是「WOULD　YOU　MARRY　ME」，所以猜想答案應是「YES　I　DO」。

說明：本題原爲計算題，所以並沒有學生真正使用此方法，但是不少學生在週記中提到，其實他們算了密碼文的字數以及發現有兩個空格之後，就已經確定答案了，接下來只是需要找一個方法符合考試的需要而已。雖然從「數學的角度」而言，此方法並不具備數學的意涵，但卻再一次驗證《碼書》說言，解碼者常常需要對密碼進行觀察，需要靈感、需要洞察力，需要猜測與驗證，廣義地說，這不也是「數學感」的一部份嗎？

## 優秀數學科普作品的指標

評價方式：指標以五顆星 ☆☆☆☆☆ 爲最高品質。

1. 知識的實質內容 (Intellectual substance of knowledge)
   - (1) 認識論面向：☆☆☆☆☆
   - (2) 方法論面向：☆☆☆☆
   - (3) 歷史或演化面向：☆☆☆☆☆
   - (4) 哲學面向：不適用
   - (5) 教育改革面向：不適用
   - (6) 與自然科學、人文社會乃至生活經驗的連結：☆☆☆☆☆
2. 形式或表達 (Form or representation)
   - (1) 創新手法：☆☆☆☆☆
   - (2) 數學知識的洞察力：☆☆☆

(3) 歷史事實的洞察力（或洞識）：☆☆☆☆☆
(4) 異文化的啓蒙意義：☆☆☆☆☆
(5) 忠實可靠的參考文獻：☆☆☆☆
(6) 敘事的趣味性、可及性與一貫性： ☆☆☆☆
(7) 中譯本的品質（若需要）：☆☆☆☆

3. 內容與形式如何平衡 (Balance in Content vs. Form)
(1) 青少年層次： ☆☆☆☆☆
(2) 一般社會大眾：☆☆☆☆☆

4. 摘錄本書最精彩片段 (excerpt from the most exciting passage)：

揭開秘密的衝動是人類根深蒂固的天性。就是最不好奇的心，也會為即將得知他人的秘密而悸動。有些幸運的人能以解謎為業，我們大部分的人卻得靠解開那些供消遣之用的矯造謎語來滿足這種欲望。對一般人而言，偵探故事或縱橫字謎便已足夠，極少數人則是以破解玄秘的符號為志業。

約翰・查威克—《線形文字 B 的解讀》[11]

[11] 目次前頁。