少年科技人

Young Maker 雜誌

讀書做善事、寫書做公益 – 歡迎程式人認養專欄或捐出您的網誌

參考價： NT 50 元，如果您喜歡本雜誌，請將書款捐贈公益團體

羅慧夫顱顏基金會 彰化銀行 (009) 帳號： 5234-01-41778-800

0123778

愛心條碼

少年科技人雜誌

2015 年 4 月

本期焦點：圖靈與 Enigma 密碼機

少年科技人雜誌

- 公益資訊

前言

編輯小語

最近由於電影『模仿遊戲』的上演，讓我也再次探索了圖靈這位資訊領域先驅者的傳奇人生，雖然電影和真實的歷史似乎有相當的差距，但仍然讓我更能夠理解當時的技術背景，因此在本期中，我們將帶您重新探索圖靈與 Enigma 密碼機的故事。

---- （「少年科技人雜誌」編輯 - 陳鍾誠）

授權聲明

1. 標示原作者姓名 (包含該文章作者，若有來自維基百科的部份也請一併標示)。
2. 採用 創作共用：姓名標示、相同方式分享 的方式公開衍生著作。

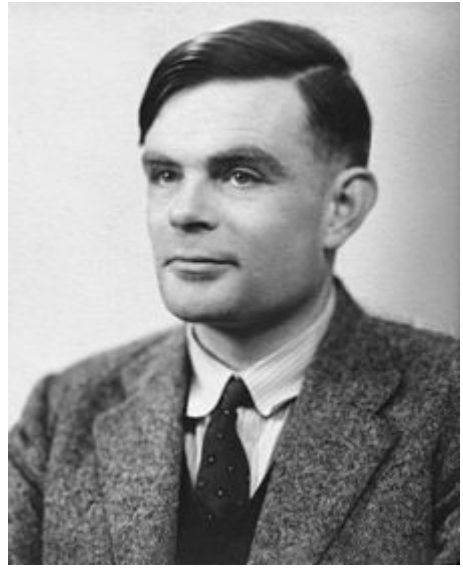
另外、當本雜誌中有文章或素材並非採用 姓名標示、相同方式分享 時，將會在該文章或素材後面標示其授權，此時該文章將以該標示的方式授權釋出，請修改者注意這些授權標示，以避免產生侵權糾紛。

例如有些文章可能不希望被作為「商業性使用」，此時就可能會採用創作共用：[姓名標示、非商業性、相同方式分享] 的授權，此時您就不應當將該文章用於商業用途上。

最後、懇請勿移除公益捐贈的相關描述，以便讓愛心得以持續散播！

本期焦點： 圖靈與 **Enigma** 密碼機

模仿遊戲：圖靈的一生



電影 模仿遊戲 是描述圖靈在二次大戰時參與破解德軍密碼機 Enigma 的故事，

這部電影讓圖靈再次進入許多人的眼裡，並讓二次大戰的密碼技術再次得到關注。

電影裡的主角『艾倫·圖靈』（Alan Mathison Turing）生於 1912年6月23日，卒於 1954年6月7日，只活了短短的 42 年，但他卻是電腦領域公認的先驅，甚至被認為是近代電腦之父。

圖靈的成就不僅僅在破解德軍密碼這件事情上，對於電腦領域的人們而言，創造出「圖靈機」的架構與理論，證明「停止問題」不可解，以及提出用「圖靈測試」來驗證電腦是否俱有智慧等等，都是圖靈一生當中對電腦領域的重要貢獻。

如果您想進一步瞭解上述這些圖靈的貢獻，可以參考下列文章：

- 停止問題不可判定 -- 以 C 語言實證
- 維基百科:圖靈機
- 維基百科:圖靈測試

我們在這期的雜誌中，會將焦點鎖定在德軍密碼機 Enigma 這個主題上！

參考文獻

- Wikipedia:Alan Turing
- 維基百科:艾倫·圖靈

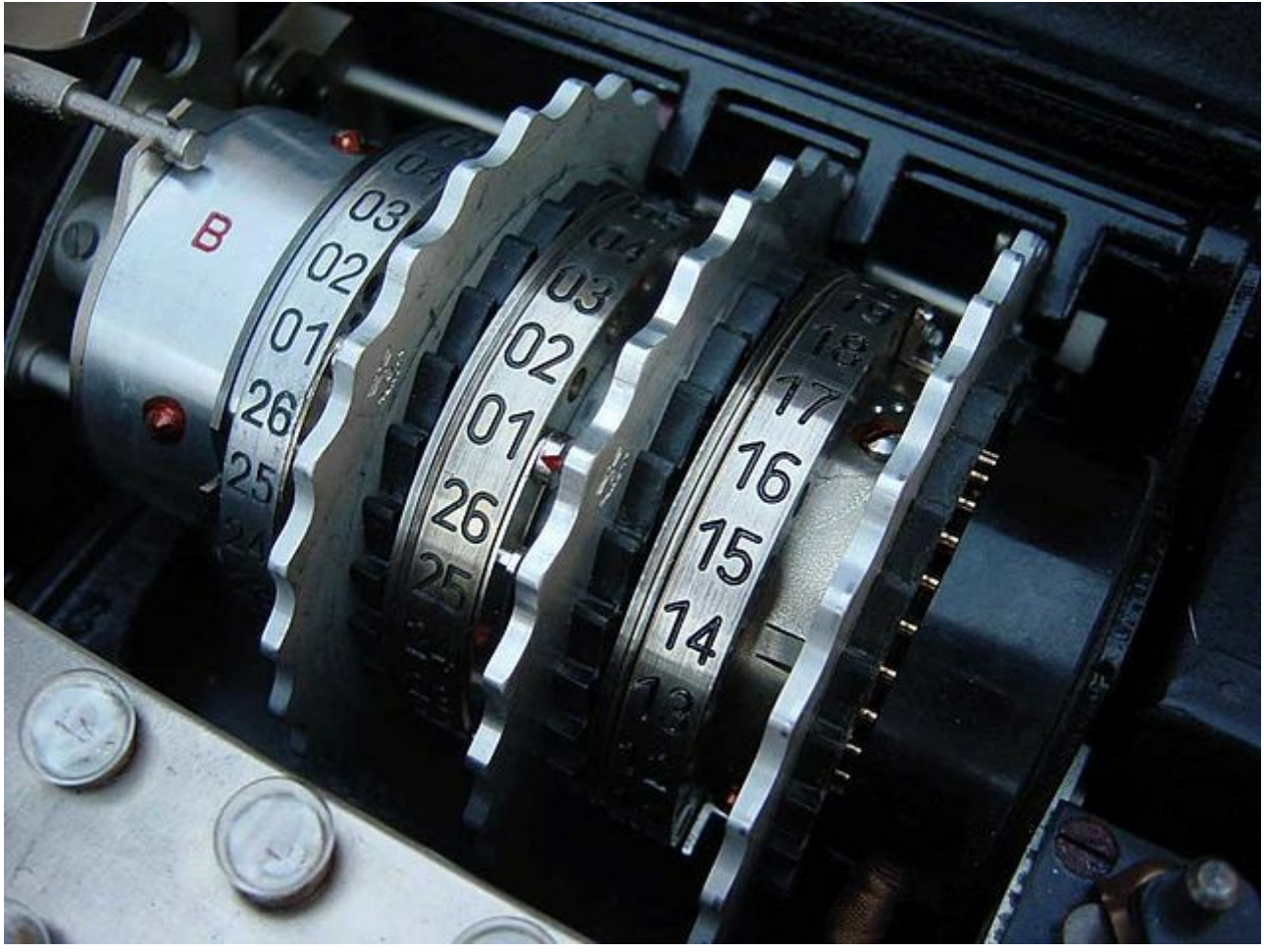
Enigma 密碼機的運作原理

簡介

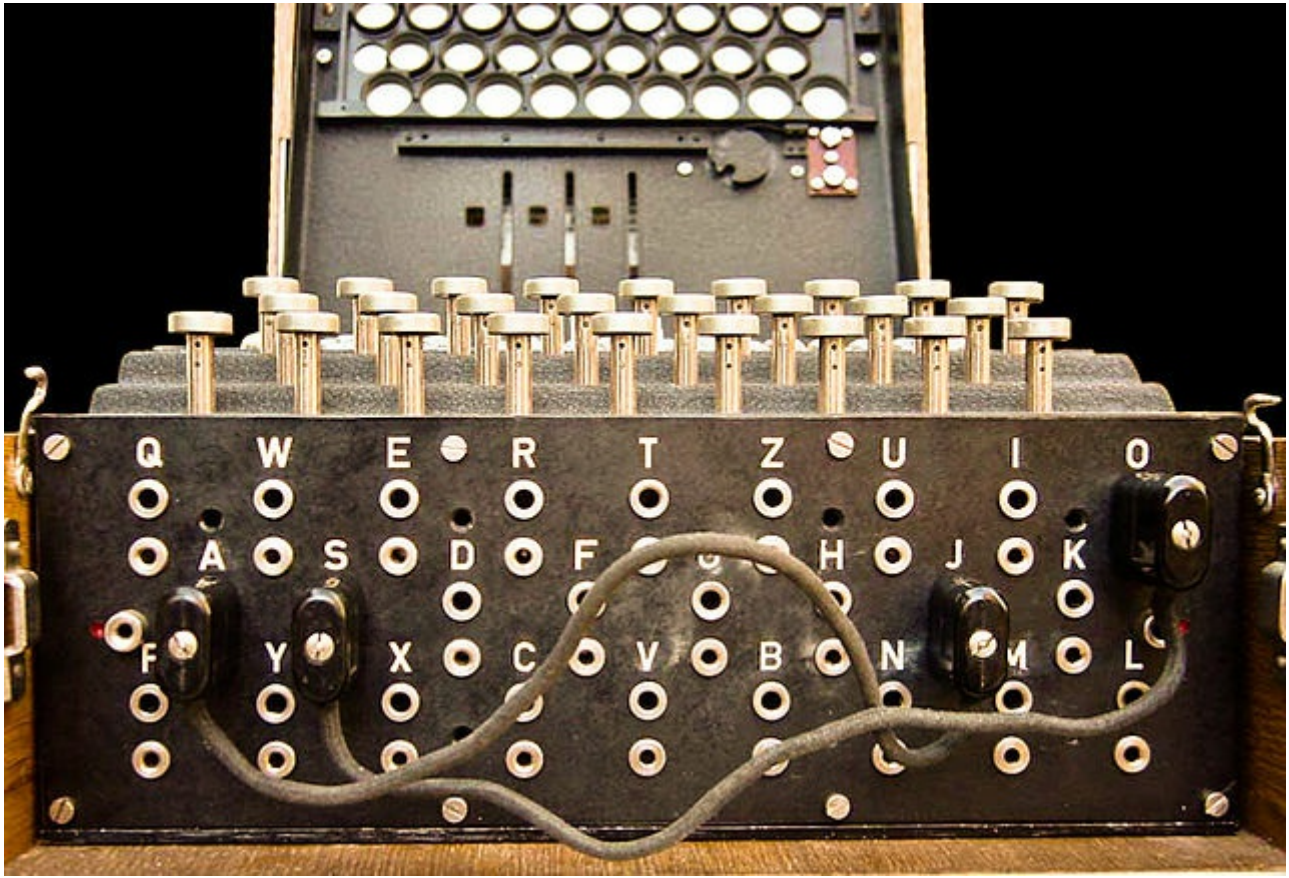

Nur Glühlampen mit 12 mm Durchmesser verwenden.
T 259

圖、Enigma 密碼機

Enigma 密碼機是德軍在二次大戰時期所採用的加解密機器，這台密碼機曾經是希特勒口中無法破解的機器，但是在戰爭的後期，德軍的密碼幾乎都被英國破解了，因此後來很多關鍵性的戰役都因為機密被英軍知道而導致戰情逆轉，因此二次大戰除了是強大武器的戰爭之外，也是一個密碼學的戰爭。


B
03
02
01
26
25
03
02
01
26
25
17
16
15
14

圖、Enigma 的旋轉輪



圖、Enigma 的接線板

觀看影片

對於想要瞭解 Enigma 密碼機的運作原理的人，強烈建議先看完下列文章以及其中的兩個影片後，在繼續閱讀我們的解說，這樣您才會有一個清楚的概念。

- 究竟圖靈是怎樣破解德軍的密碼系統 Enigma？
- YouTube: 158,962,555,217,826,360,000 (Enigma Machine) - Numberphile
- YouTube: Flaw in the Enigma Code - Numberphile

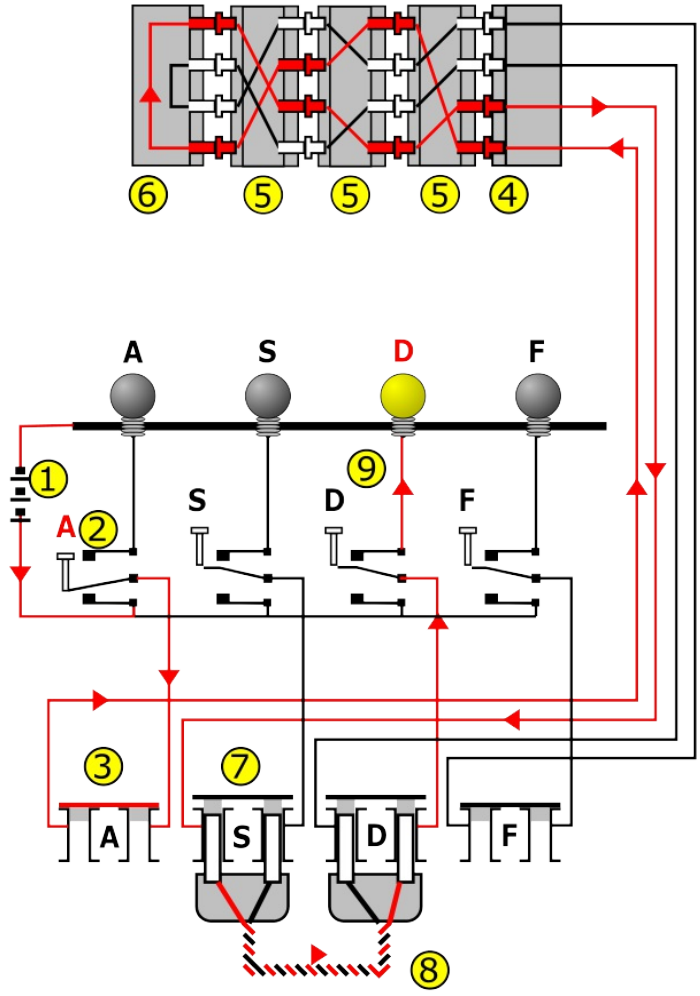
從上面影片中您可以看到，同樣一個字母透過 Enigma 會編成不同的字母。舉例而言， Y 可能這一次編為 W，下一次又邊為 T 。而且兩個不同的字母，像是 P 和 Z ，也有可能都被編成 S。

Enigma 之所以會有這樣的編碼行為，是因為最右邊的旋轉輪在每打一個字之後就會旋轉一格，然後前面的輪子在某個時候又會帶動後面的輪子，這些旋轉輪

的不同狀態讓同一個字母會被編成不同的碼。

運作原理圖

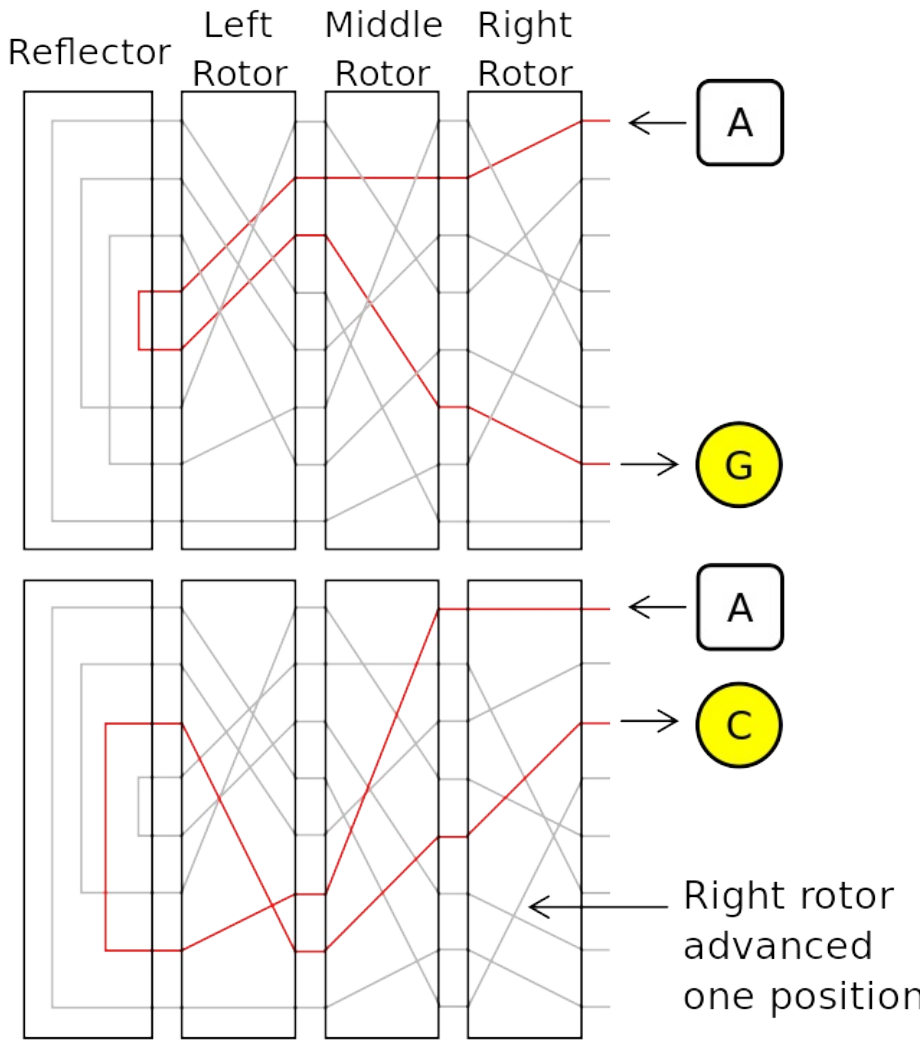
以下這張是 Enigma 密碼機的原理圖，該圖顯示了按下A鍵後機器是如何將它顯示成D鍵的（燈D發亮），而按下D鍵的同時燈A也會發亮，因為此時 Enigma 的轉輪與接線板在 D 和 A 之間建立了一條電路通道。


6
5
5
5
4
A
S
D
F
1
9
A
2
S
D
F
3
7
A
S
D
F
8

圖、Enigma 的運作原理

為了使讀者更容易理解，上圖只顯示4個鍵和4個燈。實際上，Enigma 密碼機擁有顯示燈、按鍵、插孔和線路各26個。電流首先從電池①流到雙向開關②，再流到接線板③。接線板的作用是將鍵盤②與固定介面④連接起來。接下來，電流會流到固定介面④，然後流經3個（德國防衛軍版）或4個（德國海軍M4版和德國國防軍情報局版）旋轉盤⑤，之後進入反射器⑥。反射器將電流從另一條線路向反方嚮導出，電流會再一次通過旋轉盤⑤和固定介面④，之後到達插孔S，又通過一條電線⑧流到插孔D，最後通過另一個雙向開關⑨去點亮顯示燈。

下圖顯示了簡化後的電流圖，連續按兩次A鍵後，電流會流經所有旋轉盤，通過反射器後分別向反方向流到G燈和C燈。 注意：旋轉盤上的灰色線條代表了其它可能的線路，這些線條與旋轉盤以硬接連方式連接起來。 連續按兩次A鍵會得到不同的結果，第一次得到的是G，第二次是C。這是因為最右邊的旋轉盤在第一次按下A鍵後會旋轉一點點，這就將A鍵發出的電流送到了一個完全不同的路線上。


Reflector
Left Rotor
Middle Rotor
Right Rotor
A
G
A
C
Right rotor advanced one position

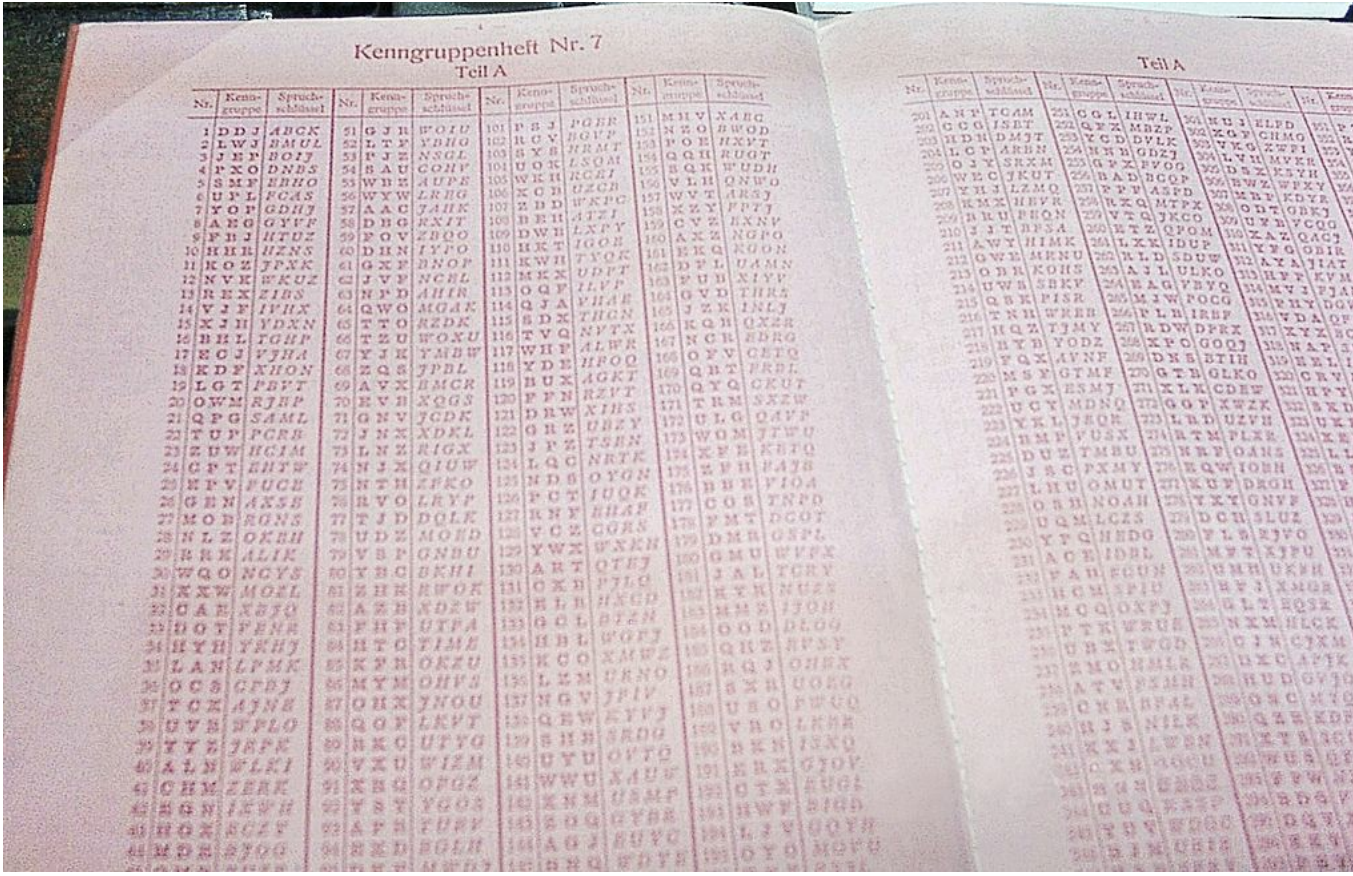
圖、Enigma 的運作原理

Enigma 對每個字母的加密過程可以以數學的角度看作為一個組合過程。假設我們有一台德國陸軍/空軍版3旋轉盤 Enigma 密碼機，讓P表示接線板的連線，U表示反射器，L、M、R表示左、中、右旋轉盤。那麼加密後的訊息 E 就可以表示成如下公式。

$$E = PRMLUL^{-1}M^{-1}R^{-1}P^{-1}E_0$$

操作過程

德軍密碼機的操作者每天都會收到一份密碼本，然後根據密碼本來設置 Enigma 的旋轉盤與接線板，以下是英軍從 U-505 號潛艇上繳獲的一本密碼本，或許您可以從中看出德軍是如何設置機器的。



圖、Enigma 的密碼本

為了使一條訊息能夠正確地被加密及解密，發送訊息與接收訊息的 Enigma 密碼機的設置必須相同；旋轉盤必須一模一樣，而且它們的排列順序，起始位置和接線板的連線也必須相同（在末期版本中由於反射器也可設定，因此反射器的線路也必須相同）。所有這些設置都需要在使用之前確定下來，並且會被記錄在密碼本中。

另外、在每條訊息發送時，操作員都會透過「指示器步驟」設定一組「旋轉盤起始位置」，這個「指示器步驟」是為了防止敵軍透過大量文本的「頻率分析」進行密碼破解而設立的。

如果您覺得光是看上述操作影片還不過癮，您可以從下列網址下載 Enigma 模擬器，這個程式可以讓你親自感受一下自己動手操作密碼機的樂趣。

- Enigma Simulator v7.0 -- http://users.telenet.be/d.rijmenants/en/enigmasim.htm

如果您不瞭解怎麼操作上述程式，可以參考下列的使用手冊，應該就會清楚了。

- ENIGMA CIPHER MACHINE SIMULATOR 7.0.6 (PDF)

該如何破解呢？

若要破解德軍的密碼，就得要將上述的這些未知資訊都搜集到，換言之、也就是要取得那份密碼本。

問題是、密碼本每天都更換一次，即使英軍取得了當天的密碼本，也只能用一天，隔天該密碼本就作廢了，於是整個破解程序又得重新來過！

但是、任何保密程序的關鍵都必須要人與裝置的完美配合，即使在電腦發達的今天，如果你的密碼總是設定成很容易記的數字、生日、身分證字號或電話號碼，那麼破解程式就很容易找到突破口，進而破解並入侵你的電腦。

即使你的密碼設得很難又很長，但你也很難保證電腦的軟體沒有漏洞，而那些駭客正是利用這些漏洞或後門來取得你電腦中的資料，並植入後門以便為所欲為的。

言歸正傳，到底英軍是如何破解德軍密碼的呢？且讓我們賣個關子，請讀者繼

續看下一篇文章！

參考文獻

- 恩尼格瑪密碼機
- Wikipedia:Enigma machine

從波蘭數學家到圖靈 - 德軍密碼是如何被破解的？

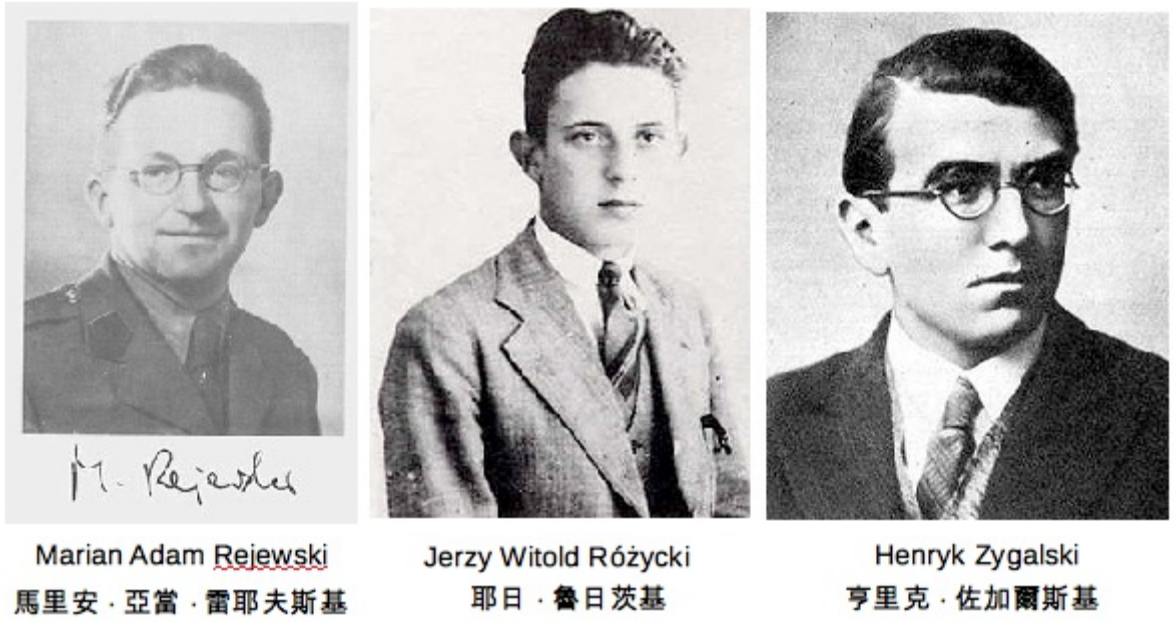
Enigma 密碼機在1920年代早期開始被用於商業，一些國家的軍隊與政府也曾使用過它，其中的主要使用者是第二次世界大戰時的納粹德國。

在 Enigma 密碼機的所有版本中，最著名的是德國使用的軍用版本。但事實上，德軍所使用的 Enigma 有好幾版，旋轉輪的數量也有三輪到五輪的，破解的難度也稍有不同，五輪的破解會比較難一點。

由於設計的機構相當複雜，而且排列組合數眾多，很多人一開始認為 Enigma 密碼機是無法破解的。舉例而言，德軍通訊部門長官的弟弟，漢斯-提羅·施密特就

曾經因為討厭納粹而向法國情報人員提供了兩份關於德軍所用 Enigma 密碼機的內部線路結構，但是法國並沒有因此而發展出破解密碼的能力。（或許是因為法國有一次大戰結束時簽訂的凡爾賽條約保護，所以感覺不到破解該密碼的急迫性，因此也沒有全力投入的關係）

但是一次大戰中獨立的波蘭的處境卻很危險，因為西邊的德國根據凡爾賽條約割讓給了波蘭大片領土，德國人對此懷恨在心，而東邊的蘇聯也在垂涎著波蘭的領土。所以波蘭需要時刻了解這兩個國家的內部訊息。



圖、最早破解 Enigma 密碼的三位波蘭數學家

這種險峻的形勢造就了波蘭一大批優秀的密碼學家，包含密碼學家馬里安·雷耶夫斯基 (Marian Adam Rejewski)、傑爾茲·羅佐基 （Jerzy Witold Różycki）和亨里克·佐加爾斯基 （Henryk Zygalski）等人。他們持續的監控住德軍內部的通訊系統，

但是1926年德軍啟用 Enigma 密碼機卻給他們造成了很大的困難。

還好、波蘭後來得到了施密特交給法國的情報，也就是 Enigma 密碼機的內部線路結構與手冊，他們從在手冊「操作步驟」的「指示器」一節中，找到了指示器步驟的嚴重缺點，進而找到了破解的關鍵。

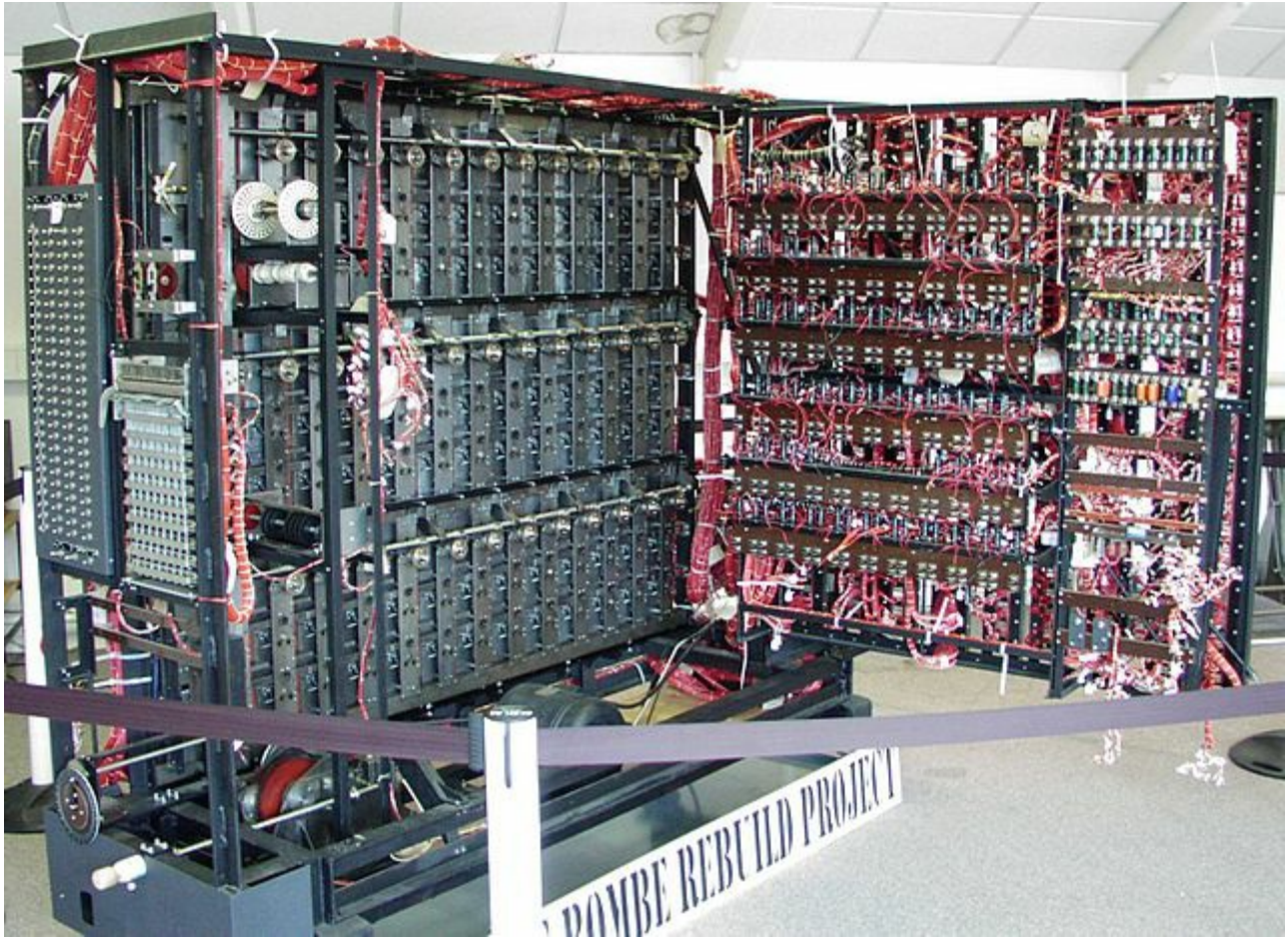
1939年圖靈被英國海軍招聘，並在英國軍情6處監督下從事對德國機密軍事密碼的破譯工作。後來圖靈還曾經向那些波蘭的密碼學家請教破解的方法，而這些波蘭的英雄們也將破解方法告知了英國和法國的密碼破解工作者。

圖、圖靈在二戰時為英國軍情六處所工作的地點 - 布萊切利莊園

儘管如此，破解的工作仍然不是很順利，因為德軍的密碼變得更加複雜了，因此初期的破解工作並沒有很大進展。

直到1941年、英國海軍捕獲德國 U-110 潛艇，並且繳獲德軍的密碼機和密碼本之後，破解 Enigma 的工作才有了重大的進展。

因為 U-110 潛艇上繳獲德軍的密碼機和密碼本所提供的訊息，圖靈的小組才得以進一步改良炸彈機，也才能真正成功的破解德軍的 Enigma 密碼，從而使得英國軍情六處對德國的軍事指揮和計劃瞭如指掌。


ROMBE REBUILD PROJECT

圖、一台接近完成的「炸彈」機複製品

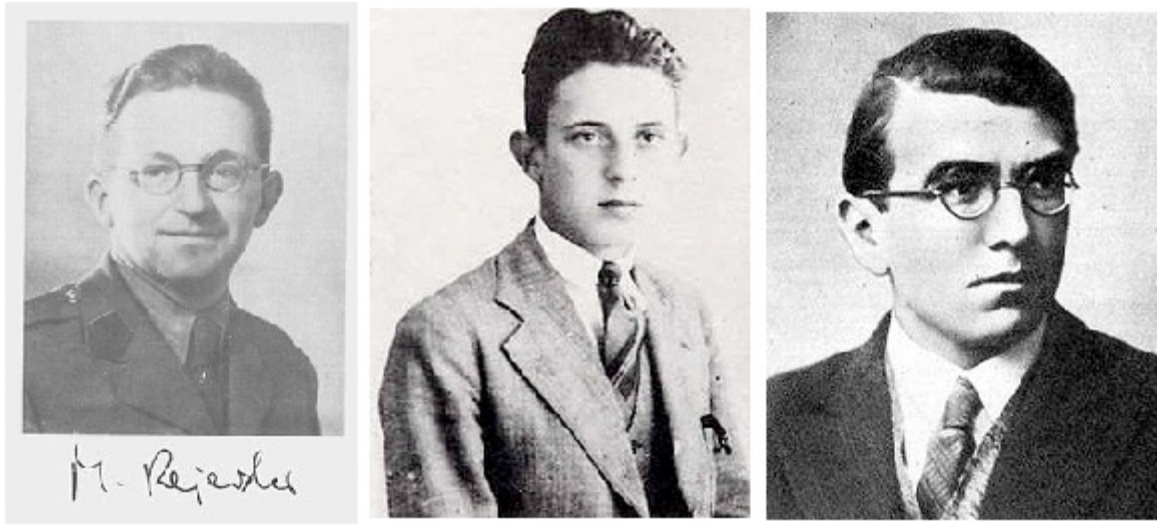
在戰爭結束以後，英國人並沒有對破解恩尼格瑪一事大加宣揚，因為他們想讓英國的殖民地用上這種機器。1967年，波蘭出版了第一本有關恩尼格瑪破解的書，1974年，曾在布萊切利園工作過的英國人F.W.溫特伯坦姆寫的《超級機密》（The Ultra Secret）一書出版，這使外界廣泛地了解到了第二次世界大戰中盟軍密碼學家的辛勤工作。

科技人物

破解 **Enigma** 密碼的三位波蘭英雄

在『模仿遊戲』這部描述圖靈在二次大戰破解德軍密碼機故事的電影裡，或許是為了戲劇效果，也或許是為了避免故事太過複雜，在電影裡完全略過了波蘭三位研究密碼數學家的貢獻，因此很容易讓觀賞者認為破解德軍密碼完全是圖靈小組的功勞，這是有所誤導的。

事實上、在圖靈之前，Enigma 密碼機就曾經被破解過了。而破解 Enigma 密碼機的主角，正是下圖中的三位波蘭數學家 -- 馬里安·雷耶夫斯基 (Marian Adam Rejewski，1905年8月16日－1980年2月13日)、傑爾茲·羅佐基 （Jerzy Witold Różycki，1909年7月24日－1942年1月9日）和亨里克·佐加爾斯基 （Henryk Zygalski，1906年－1978年），史稱『波蘭三傑』。



圖、破解 Enigma 密碼的三位波蘭數學家

『波蘭三傑』並非只是玩玩數學而已，他們還設計出了幫助密碼分析工作的機器，最早開發的是一台稱為「記轉器」的儀器，後來又開發了名為「炸彈」的Enigma密碼分析儀器——「Bomba」。「炸彈」最初由六台以Enigma為基礎改裝

的機器輔以其他一些設備組成，能夠通過暴力搜索的方法機械驗證出Enigma上所有轉子的組合，在兩個小時內找出密鑰。後來英國設計建造的「Bombes」和美國設計建造的「Bombs」其實都是在「Bomba」的基礎上研製而成的。

『波蘭三傑』透過他們的理論研究與裝置，在 1933年1月到1939年9月期間，破譯了將近十萬條來自德方的消息，令波蘭掌握了大量德國的機密情報。

1938年9月，德國軍隊對Enigma進行了修改，導致破譯的難度大大增加。此時德國進攻波蘭的意圖越來越明顯，而波蘭在人力、物力方面資源不足，為了在波蘭遭到入侵後盟國能夠繼續對德國Enigma密碼進行研究和破譯，波蘭在1939年7月25日在華沙召開的一次會議上將雷耶夫斯基等人在破譯Enigma密碼上取得突破的細節告知英國和法國的情報機構。

1939年9月1日德軍入侵波蘭後，他們帶著機器一同逃往羅馬尼亞，而後穿越南斯拉夫和義大利的邊界到達法國巴黎。在那裡他們成立了 Z 小組，在法國維希的 PC Bruno 情報站繼續進行破譯 Enigma 和改進 「炸彈」的工作達兩年之久。這期間，他們破譯了九千餘條德軍情報，直接或間接導致了德軍在南斯拉夫、

希臘和蘇聯的慘敗，有力地支持了盟軍在北非開闢戰場的作戰計劃。

1942年1月9日，羅佐基在從阿爾及利亞乘Lamoriciere號輪船返回法國，途中輪船在Balearic島附近撞上水下不明物體（礁石或水雷），魯日茨基和另外兩名密碼分析專家連同船上兩百餘名乘客一同遇難，英年早逝，只活了 33 歲。

而在德國入侵法國後，Z小組的處境越來越危險，他們決定逃離。1942年11月9日，也就是盟軍登陸北非的次日，雷耶夫斯基和佐加爾斯基開始繼續流亡。1943年1月29日，他們在庇里牛斯山脈試圖穿越法國-西班牙邊境時被西班牙安全警察逮捕，投入難民營，難民營的生活令雷耶夫斯基患上了風濕病。在那裡他們始終沒有向其他人透露真實身份。同年5月，他們被釋放，前往直布羅陀，隨後乘船到達英國。英國方面知道他們在破譯Enigma領域作出的巨大貢獻，卻有意將他們排除在外，他們只是從事德軍另外一種密碼SS碼的分析工作。

二戰結束後，1946年，雷耶夫斯基返回波蘭與妻子和兩個孩子團聚。回國後他在波茲南大學擔任行政工作（一說波蘭的一家工廠），並且對他自己在戰前和戰時所作的工作保持沉默。1967年退休。1980年於華沙去世，安葬在波蘭的

Powazki公墓，享年75歲。

而佐加爾斯基則是留在英國，並在巴特爾西(Battersea)技術學院任教，1978 於普利茅茨去世，享年 72 歲。

2000年7月17日，波蘭政府向雷耶夫斯基、魯日茨基和佐加爾斯基追授波蘭最高勳章。2001年4月21日，雷耶夫斯基、魯日茨基和佐加爾斯基紀念基金在波蘭華沙設立，基金會在華沙和倫敦設置了紀念波蘭數學家的銘牌。

雜誌訊息

讀者訂閱

程式人雜誌是一個結合「開放原始碼與公益捐款活動」的雜誌，簡稱「開放公益雜誌」。開放公益雜誌本著「讀書做善事、寫書做公益」的精神，我們非常歡迎程式人認養專欄、或者捐出您的網誌，如果您願意成為本雜誌的專欄作家，請加入 程式人雜誌社團 一同共襄盛舉。

我們透過發行這本雜誌，希望讓大家可以讀到想讀的書，學到想學的技術，同時也讓寫作的朋友的作品能產生良好價值 － 那就是讓讀者根據雜誌的價值捐款給慈善團體。 讀雜誌做公益也不需要有壓力，您不需要每讀一本就急著去捐款，您可以讀了十本再捐，或者使用固定的月捐款方式，當成是雜誌訂閱費，或者是季捐款、一年捐一次等都 OK！甚至是單純當個讀者我們也都很歡迎！

本雜誌每期參考價：NT 50 元，如果您喜歡本雜誌，請將書款捐贈公益團體。

例如可捐贈給「羅慧夫顱顏基金會 彰化銀行(009) 帳號：5234-01-41778-800」。(若匯款要加註可用「程式人雜誌」五個字)

投稿須知

給專欄寫作者： 做公益不需要有壓力。如果您願意撰寫專欄，您可以輕鬆的寫，如果當月的稿件出不來，我們會安排其他稿件上場。

給網誌捐贈者： 如果您沒時間寫專欄或投稿，沒關係，只要將您的網誌以 [創作共用的「姓名標示、非商業性、相同方式分享」授權] 並通知我們，我們會自動從中選取需要的文章進行編輯，放入適當的雜誌當中出刊。

給文章投稿者： 程式人雜誌非常歡迎您加入作者的行列，如果您想撰寫任何文章或投稿，請用 markdown 或 LibreOffice 編輯好您的稿件，並於每個月 25 日前投稿到程式人雜誌社團 的檔案區，我們會盡可能將稿件編入隔月1號出版程式人雜誌當中，也歡迎您到社團中與我們一同討論。

如果您要投稿給程式人雜誌，我們最希望的格式是採用 markdown 的格式撰寫，然後將所有檔按壓縮為 zip 上傳到社團檔案區給我們， 如您想學習 markdown 的撰寫出版方式，可以參考 [看影片學 markdown 編輯出版流程] 一文。

如果您無法採用 markdown 的方式撰寫，也可以直接給我們您的稿件，像是 MS. Word 的 doc 檔或 LibreOffice 的 odt 檔都可以，我們 會將這些稿件改寫為 markdown 之後編入雜誌當中。

參與編輯

您也可以擔任程式人雜誌的編輯，甚至創造一個全新的公益雜誌，我們誠摯的邀請您加入「開放公益出版」的行列，如果您想擔任編輯或創造新雜誌，也歡迎到 程式人雜誌社團 來與我們討論相關事宜。

公益資訊

公益團體	聯絡資訊	服務對象	捐款帳號
財團法人羅慧夫顱顏基金會	http://www.nncf.org/ lynn@nncf.org 02-27190408分機232	顱顏患者 (如唇顎裂、小耳症或其他罕見顱顏缺陷）	銀行：009彰化銀行民生分行 帳號：5234-01-41778-800
社團法人台灣省兒童少年成長協會	http://www.cyga.org/ cyga99@gmail.com 04-23058005	單親、隔代教養.弱勢及一般家庭之兒童青少年	銀行：新光銀行 戶名：台灣省兒童少年成長協會 帳號：103-0912-10-000212-0