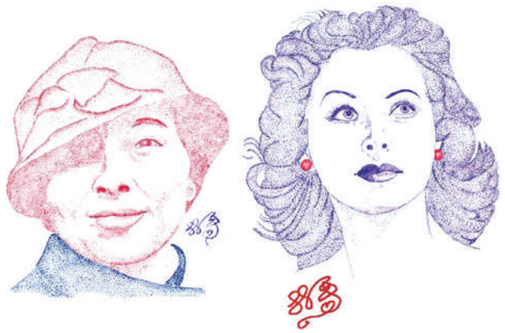
三位女性密碼專家

文／林一平 講座教授



林一平手繪之傅利曼 (左) 與拉瑪 (右)。

女性在資通訊科技的貢獻，相當顯著。全世界第一位電腦程式工程師勒芙蕾絲 (Ada Lovelace) 是女性。二次大戰時，男性上戰場，很多運用電腦計算資料的工作由女性執行。

第一次世界大戰後美國海軍密碼沙福 (Laurance Safford) 創辦了海軍密碼組織。沙福在美國海軍鼓吹解碼的重要性，在海軍的月刊《Communications Bulletin》放了猜謎遊戲，找到提供最佳解答的官兵，勸他們加入他的密碼情報單位。在他的單位有一位二十世紀初期美國最偉大的女性密碼專家 (Cryptanalyst)，名叫德里斯科爾 (Agnes Driscoll)。她於 1911 年畢業於俄亥俄州立大學，先在德州的軍校教音樂，再到一家高中擔任數學老師。1918 年她在海軍擔任文書上士 (Yeoman)。由於學歷太好，長官就教她解密碼。1921 年，赫本 (Edward Hebern) 發明全世界第一部密碼機 (Hebern cipher machine)，宣稱以此機器加密，無人可破解。然而德里斯科爾本事高強，兩三下就將赫本加密的訊息解開。德里斯科爾被尊稱為 X 夫人 (Madam X) 或海軍解碼第一夫人 (the first lady of naval cryptology) 。

美國第一位女性密碼專家是傅利曼 (Elizebeth Friedman)，她最大的貢獻是破解走私毒犯的密碼。由於她破解密碼，更抓到二次大戰日本隱藏在美國最重要的女間諜。但她最為人認知的貢獻是在莎士比亞的研究。她和先生 (William F. Friedman) 寫了一本書《The Shakespearian Ciphers Examined》，榮獲由 Folger Shakespeare Library 以及 American Shakespeare Theater and Academy 頒發的獎項。

過去一直有傳說，莎士比亞的劇本實際是別人寫的。例如馬克吐溫就曾發表長達 4 頁的文章《莎士比亞不是我們知道的莎士比亞》，羅列了所有已知事實證明歷史書介紹的莎士比亞根本不懂戲劇。於是很多人想找出莎士比亞劇本的「真正作者」。當中的一種說法認為作者是法蘭西斯培根，並懷疑劇本中可能包含培根密碼 (Bacon's cipher)。許多人曾試圖從莎士比亞的舊劇本中找出上述密碼。傅利曼夫婦證明莎士比亞劇本中沒有包含培根密碼或者其他密碼。讀者諸君如果感興趣莎士比亞劇本作者之謎，可參見卡雷爾 (J. L. Carrell) 的著作《莎士比亞的秘密》(The Shakespeare Secret)。

在二戰時期思考保密對軍事通訊的重要性，而發明秘密通訊的方法，則屬好萊塢女演員拉瑪 (Hedy Lamarr) 的故事最具傳奇性。1940 年拉瑪參加宴會。在鋼琴邊閒聊之際，看到手指在琴鍵彈跳，忽然想到可以利用跳頻發展出一個秘密通訊的方法，應用於軍事通訊系統，抵擋敵人的電波干擾 (Anti-jamming) 並且防止竊聽。1985 年高通 (Qualcomm) 在美國加州成立，以展頻技術 (Frequency Hopping) 為基礎，研發出 CDMA(Code Division Multiple Access) 系統，常提及拉瑪的貢獻。

林一平
國立陽明交通大學資工系終身講座教授暨華邦電子講座

現為國立陽明交通大學資工系終身講座教授暨華邦電子講座，曾任科技部次長，為 ACM Fellow、IEEE Fellow、AAAS Fellow 及 IET Fellow。研究興趣為物聯網、行動計算及系統模擬，發展出一套物聯網系統 IoTtalk，廣泛應用於智慧農業、智慧教育、智慧校園等領域 / 場域。興趣多元，喜好藝術、繪畫、寫作，遨遊於科技與人文間自得其樂，著有 < 閃文集 >、< 大橋驟雨 >。

Three Female Cryptanalysts

Women have played a vital role in the field of information technology. The world's first computer programmer, Ada Lovelace, was a woman. During World War II, women stepped into computer operation and programming work while men went off to war.

After World War I, a U.S. Navy cryptologist, Laurance Safford, established the Naval cryptologic organization. Safford advocated for the importance of Communications Intelligence in the U.S. Navy and recruited promising cryptanalysts by putting puzzles in the Navy's monthly Communications Bulletin. One of America's greatest female cryptanalyst in the early twentieth century, Agnes Driscoll, was in his unit. Driscoll received a Bachelor of Arts degree from Ohio State University in 1911. She began working as a music teacher at a military academy in Texas and later worked as a math teacher in a high school. In 1918, she served as a chief yeoman in the U.S. Navy. Because of her good academic qualifications, the chief in the unit taught her the skills of deciphering. In 1921, Edward Hebern built the world's first Hebern cipher machine and claimed that no one could crack the data that was encrypted by this machine. However, Driscoll was quite proficient and deciphered Hepburn's encrypted message in a jiffy. Driscoll was therefore known as Madam X or the first lady of naval cryptology.

The first female cryptanalyst in the United States was Elizebeth Friedman. Her greatest achievement was cracking the encryptions of smugglers. Moreover, owing to her assistance, the government caught the most important Japanese female spy in the United States during World War II. However, her most recognized contribution was her research in Shakespeare. She and her husband, William F. Friedman, wrote a book, The Shakespearian Ciphers Examined, which received awards from Folger Shakespeare Library and American Shakespeare Theater and Academy.

There is a popular conspiracy theory that someone other than William Shakespeare of Stratford-upon-Avon wrote the works attributed to him. For example, Mark Twain published a four-page article "Shakespeare is not the Shakespeare we know", which listed all known facts that the Shakespeare described in history books did not understand drama. Therefore, many people want to find out the "real author" of Shakespeare's works. Some sources claim that the author is Francis Bacon and suspect that the scripts may contain Bacon's cipher. Many people have tried to find the ciphers from Shakespeare's scripts. The Friedmans refuted the claims that the works of Shakespeare contain hidden ciphers that disclose Bacon's or any other candidate's secret authorship. If you are interested in the mystery of Shakespeare's works, please refer to J. L. Carrell's book, The Shakespeare Secret.

The key aspect of communications is the ability to transmit messages within the military and between allies in utter secrecy and security during World War II; however, the most legendary story regarding inventing secret communication system was of Hollywood actress Hedy Lamarr. In 1944, Lamarr attended a banquet. While chatting by the piano, she noticed the fingers bouncing on the keys. She suddenly thought that frequency hopping could be applied to a secret communication system used in military communication systems for anti-jamming and eavesdropping prevention. Qualcomm, established in California in 1985, developed a CDMA (Code Division Multiple Access) system based on frequency hopping, so Lamarr's contributions have been retroactively recognized.

Dr. Jason Yi-Bing Lin

Lifetime Chair Professor of the Department of Computer Science at National Yang Ming Chiao Tung University and Winbond Chair Professor

Dr. Lin is currently a lifetime chair professor of the Department of Computer Science at National Yang Ming Chiao Tung University and Winbond chair professor. He is an ACM Fellow, IEEE Fellow, AAAS Fellow and IET Fellow. His research interests include Internet of Things, mobile computing, and system simulation. He has developed an Internet of Things system called IoTtalk, which is widely used in smart agriculture, smart education, smart campus, and other fields. He has a variety of interests, such as art, painting, and writing, as well as voyaging through science, technology, and humanities.