深耕密碼學　帶領同學加解密

陳君明 老師

小檔案

系　　所　理學院數學系

專　　長　密碼學、計算代數

教授科目　密碼學導論、應用代數、橢圓曲線密碼學、金融科技導論、微積分

學　　歷　國立臺灣大學數學系學士
國立臺灣大學數學系碩士
美國普渡大學數學系博士

現　　職　國立臺灣大學數學系兼任助理教授

榮譽紀事　國立臺灣大學教學傑出教師

採訪撰稿／簡鈺璇
攝影／楊文卿

密碼學的魅力在於它與生活息息相關。只要打開電腦、收發信件、登入社群網站、線上刷卡，就有一堆密碼系統在跑，進行加解密。

「你們知道Snowden如何揭祕嗎？」陳君明常用時事吸引學生。他的「密碼學導論」貼近時下最夯的資訊產業，且橫跨電機、資工和數學領域。正因為題材新、延伸廣，課程迅速竄紅，近三百人的教室座無虛席。

逃避聯考　保送進數學系

從小陳君明就對資訊科技感興趣。國小時，宏碁電腦公司推出最早的個人電腦「小教授二號」，也開啟他對資訊科技的探索。從此他開始買書研究，學寫簡單的程式。「講這個就洩漏我的年紀了！」他笑著說。

陳君明高中是以電機、資訊工程為大學的前二志願，當時陳君明的成績名列前茅，拚聯考勝券在握。他還記得，建中高三時，全班模擬考成績貼在布告欄，可以看到第一名的三民主義只考六十分，但其他科目全都八、九十分。「那就是我。數學、物理和化學比別人好很多，但我不想浪費時間背三民主義。」陳君明說。

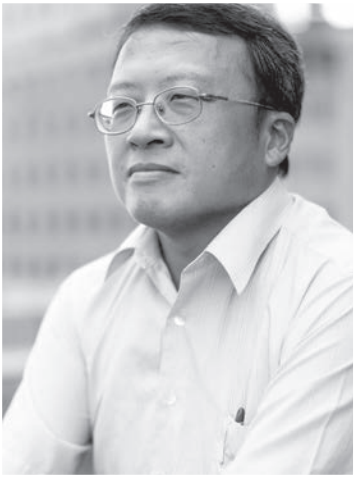
他心知自己對背誦的科目完全不在行，加上反叛性格，總認為當時聯考制度不對勁。他解釋：「三民主義和數物化國英五科一樣，滿分都是一百分；但三民主義只上一年，且應用有限；而數學是從國小就學習了，比重居然一樣，這不合理！」因為不想參加聯考和背誦三民主義，他選擇保送進臺大數學系。

■ 陳君明為了避免背誦三民主義，索性不考聯考。（楊文卿／攝影）

確定保送之後，陳君明的暑假提早開始。「當同學們還在努力拚大學聯考時，我已經在建中附近的撞球場，以『碰撞實驗』檢視能量守恆與動量守恆了。」他幽默地說。對陳君明而言，打撞球就是在做物理實驗。

數學系非常難讀，各類數學理論、推導相當抽象，在系館與同學們討論課業到深夜的景象，至今仍讓陳君明記憶猶新。「我們這屆的必修課高等微積分，全班五十八人，包含重修生，被當掉人數剛好一半——二十九人。」他說。因為還「撐得下去」，所以他繼續讀碩士班，主攻代數數論。

代數數論為純數學領域，跟日常生活脫節。陳君明表示，當時每個碩士生都有各自鑽研的主題，差異很大，同學間很難相互討論。就讀研究所時，美國有人完整證明著名的費馬最後定理，在當時的數學界造成一陣轟動。這是三百多年來，首次有人發表公認正確的證明。陳君明



■ 陳君明喜歡交朋友，認為自己不適合待在純數學領域。（楊文卿／攝影）

記得，當時指導老師問他，「有沒有興趣閱讀證明？」他心想這解法與代數數論有關，便欣然接受，隔天厚厚的兩百頁論文就躺在桌上。陳君明笑說：「證明的第一頁，我就看不懂！所以就讀不下去了，反正世界上有天才看得懂。」

他將純數學理論喻為藝術品。陳君明說，人們不會去問畢卡索的畫有何用途，那是藝術；「數學也是一樣的，是真理、是人類智慧的結晶。」陳君明認為，因為數學可能無法與日常生活沾上邊，作為純數學家是要耐得住孤獨。陳君明發現這樣的日子與自己的個性不符，所以便在博士班轉換領域，到美國普渡大學鑽研密碼學，將抽象代數與應用領域結合。

赴美讀密碼學　返台後創業

密碼學的魅力就在於它與生活息息相關。「只要打開電腦、收發信件、登入社群網站、線上刷卡，就有一堆密碼系統在跑，進行加解密。」陳君明說。小到個人日常的娛樂，大至國防機密保護、商業資訊傳遞，都需要仰賴它；再如近年銀行界前仆後繼投入的金融科技區塊鏈，核心技術正是來自密碼學。

另外，密碼學還需要密切的跨界合作。他指出，數學領域的人才設計演算法，分析密碼系統的安全性，以及思考如何破解演算法；演算法一旦確定後，就需要資工專家撰寫程式應用；如果需要如悠遊卡、金融卡的內置晶片等硬體實作，就是電機系所的專業。他笑著表示，密碼研究如同矛與盾的攻防，除了破解密碼外，還須鞏固自身的系統。

■ 陳君明熱愛講故事、分享知識給學生。（簡鈺璇／攝影）

取得普渡大學數學博士後，陳君明並未留在美國教書，他引用電機系教授李琳山所講的一句話：「回家是不需要理由的！」作為他的答案。陳君明表示，從抵達美國的第一天直到離開的前一天，都想回臺灣。雖然與洋人朋友們相處愉快，但總覺得自己不屬於那個環境。

陳君明回國後，在美國博士班指導教授莫宗堅的鼓勵下，與朋友合夥開設以密碼嵌入式系統為基礎的資訊安全公司；並於二〇〇三年開始在數學系兼課教授密碼學、微積分等課程，至今未申請專任教職。

他表示自己喜歡接觸社會，希望研究的東西能夠實際運用，這也是他的成就感來源。他自認不適合留在學校發表論文，而是能經常在外界談合作。提及在數學系兼任授課，陳

君明認為這是產業趨勢。如果能將最新的知識與學生交流，協助學生未來能有不同的就業選擇，甚至持續深耕密碼學領域，都很不錯。

陳君明認為自己是完美主義者，「對在意的事情一定要做到最好！因此做出來的東西品質不錯，但同時也花費不少時間。」陳君明提到自己最欣賞的是四十年前發明「RSA密碼系統」（RSA cryptosystem）的密碼學家希米爾（Adi Shamir），至今希米爾仍非常活躍，一直有創新的點子出現，也帶領不少後輩。像這樣不以過去成就而滿足的精神，最令陳君明佩服。

教書如交友　同理心待學生

密碼學課程並不輕鬆，曾有電機系的書卷獎同學對他說，這門課內容精實程度不輸電機系的必修課。平時面對兩百多人上課，陳君明只有一個原則：「同理心」。他表示自己當學生時，討厭老師做什麼事，自己當了老師時絕對不會做。所以，在陳君明的課堂上絕不點名，也絕不用單一考試定生死。老師也絕不遲到，以免浪費同學時間。

備課時，陳君明會思考如何讓學生理解原理，先從簡單的範例著手，再看抽象的公式，並講解演算法原理。每年他都會研讀學術論文與科技報導，補充新知，讓課程與世界接軌，上課前則會充分備課。他強調，無論上過幾次同樣內容的課，「為了確保不會臨場解不出題目，掛在黑板上，準備絕對要非常充分。」

陳君明說，他考試的考題很多，學生讀多少就拿幾分。絕不會有學生看到考卷，發現考的沒讀、讀的沒考，而怒拍桌子的情況。

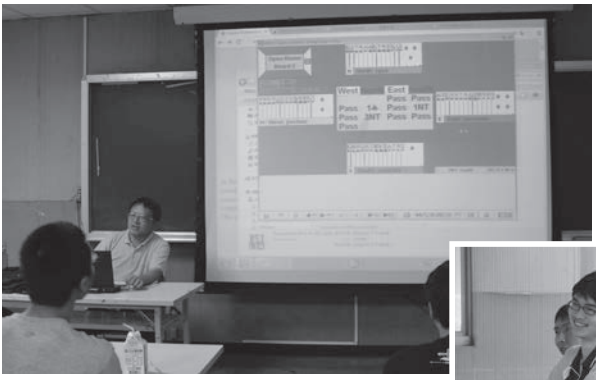
他對待學生如朋友，兩年前到舊金山開會，陳君明順便拜訪在美國攻讀博士的學生。學生看到他訝異地說：「老師你現在穿的衣服，是不是在微積分課堂上也穿過？」他想這件衣服確實很久了，七年前應該在，沒料到同學還記得。而現在他的橋牌夥伴，不僅是公司同事也曾是他學生，他與學生間真是零距離。

他也常鼓勵學生勇敢提問。「我當學生時常質疑老師，所以我也對學生說我講的不一定是對的，若有意見可以提出，讓真理越辯越明！」他表示，教學相長，和學生討論的過程中，自己也有明顯收穫。

■ 學生常在課後，向陳君明請教。（簡鈺璇／攝影）

熱愛打橋牌　鬥智兼學處世態度

在工作之餘，陳君明的主要興趣是橋牌和高爾夫球。今年（二〇一六）他將代表台灣參加世界



■ 陳君明將精彩牌局攤出來，與學生討論叫牌過程。（簡鈺璇／攝影）

■ 學生專注聽陳君明講解實戰牌局。（簡鈺璇／攝影）

盃橋牌大賽，同時也是橋藝協會理事、臺大橋藝社指導老師。陳君明高中時就加入橋藝社，他表示打橋牌時，常有機會接觸到特別的人事物。例如：他與張忠謀當過隊友、還曾與股神巴菲特、微軟創辦人比爾蓋茲參加同場比賽。

陳君明說，橋牌桌上變幻莫測，電腦無法輕易打敗人腦。他比較下棋與橋牌的差異。陳君明說，下棋是攤開來下，只須顧好自己和對手即可，但下錯一步棋就輸了。橋牌則不然，理論上的最佳判斷，不一定會得到最好結果，牽涉因素太多；換個對手、同伴或臨場狀況，結局就不一樣。」陳君明說，橋牌比起棋類，更接近真實的人生競技。

陳君明認為打橋牌除了鬥智，更能學習待人處事、團隊合作等課題。在橋藝社授課時，他常提供同學進步的管道，並激勵同學與高手過招，精進橋藝。此外，他不吝於為橋藝社尋找資源，甚至請橋

牌界資深大老鍾仁謙為社團上課，希望能朝代表臺灣青年隊出賽而努力。

數學領域廣 建議學生鋪路

「天生我才必有用，天底下一定有你擅長的事情。」這是陳君明給困在純數學領域、唸不下去的同學的建議。陳君明表示從以前到現在，學生多按考試填志願，所以對於數學不一定有熱忱，常會自我放棄。然而，他認為同學應該提前為將來打算，努力發掘興趣，找到自己做得來的事情。

他也從業界角度建議數學系，在修業規畫中加入兩三組不同選修課，一類是純數學，讓熱愛數學的同學有學術選擇；另一類則增加電腦程式設計課程，讓同學就業的路廣一些，不只擔任精算師，還有其他選擇。

至於對同學是否選擇創業的建議，陳君明認為這因人而異。「有自己想法的人比較適合！」因此他建議不愛受到拘束、看到產業前景的同學，可以考慮創業之路。

■ 陳君明建議同學提早思考，找到自己的興趣。（簡鈺璇／攝影）

■ 陳君明認為，生命有許多選擇，天生我才必有用。（楊文卿／攝影）