5G與PK：不可不知的神奇密碼

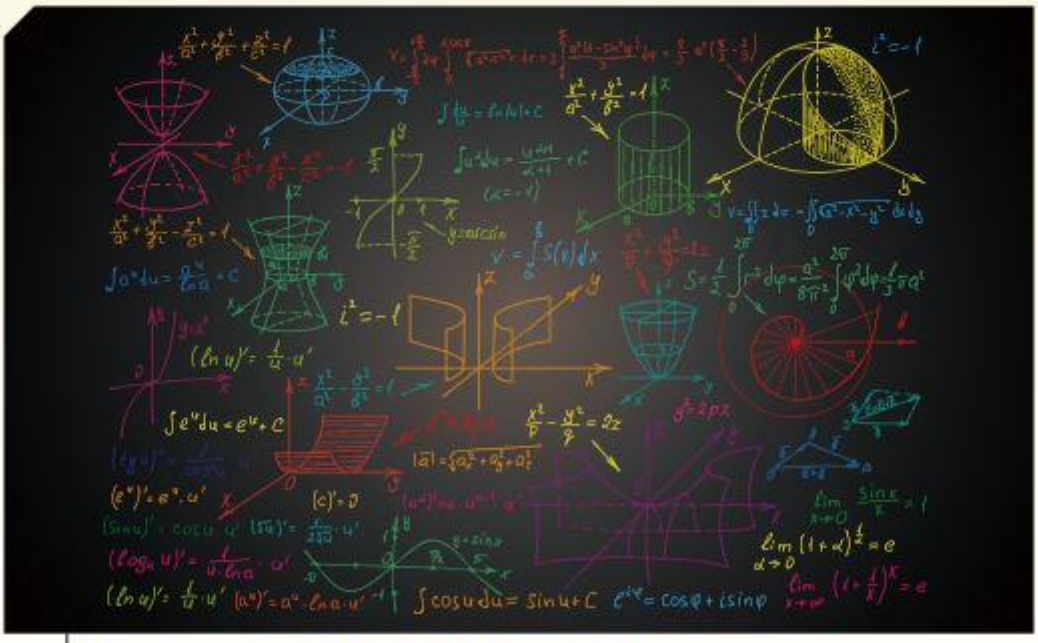
社團法人台灣E化資安分析管理協會理事長、中央警察大學資訊管理學系專任教授
／王旭正

拜科技、網路之賜，讓人們生活開始跳脫傳統的模式。相隔兩地的相思情，在網路裡，迅速縮短實際距離，讓影像的視訊互動升了溫；而時間的枷鎖藉網路的活化作用，在不知不覺中竟也神奇微妙地得以切割，以分工處理生活中的各式需求。網路媒介喚醒了人心深處的渴望—「快」與「準」，即有著 5G「快」的通訊速度、與 PK「準」的訊息正確性。

「快」5G

網路裡，訊息的傳遞讓通聯的雙方得以快速地分享資訊，1G、2G、3G、4G 通訊技術讓網路不斷地進化。近年，我們不斷聽到一個有點新又不是很新的英文詞：「5G」。其為 4G 通訊技術成熟後，下一個世代的通訊網路環境泛稱名詞。事實上，「G」世代的發展皆是建構在前一代的基礎，慢慢經營，而得以茁壯。1G 可語音通話；2G 開始數位訊息傳遞；2.5G、2.75G 的過渡時期；再到 3G 時代、3.5G、3.75G、3.9G，一直演進到現階段較為成熟的 4G。

而 5G 除了速度快、連通強，還有結合人工智慧的各式開發應用於 V2X（Vehicle to Everything）、遠距醫療系統、製造業市場等琳瑯滿目的網路應用，怎不令人心動呢！您是否也想到 1、2、3、4、5 後頭還有嗎？當然有，現在的 4G、10 年間的 5G、2030 年的 6G，再來的 7/8G 網路通訊技術的開發，那不是夢，是一代傳一代逐步建構上去的網路，得以符合人們心中的想像空間。那「安全」呢？接續前期的資安生活之旅，我們再次前進 PK（Public Key）的神奇戲法—密碼。



數學為科學之母，是記錄規律、整理順序、推演過程最重要的科學工具。

「準」PK

談了網路的「快」，是否還記得「準」？5G 通訊技術的確加快了網路的訊息傳遞速度，但還得準確地判斷訊息真實性，若一味搶快，失去了準真性，倒也可惜，是白費力氣地做虛工呀！在資安生活之旅中，我們曾說過法國的費瑪（Fermat, 1601-1665）對密碼「安全」的啟蒙，開啟了科技領域裡密碼與安全機制的新歷史。在業餘數學家費瑪的生活裡，他自行找出了許多自然界、生活中的規律。數學是科學之母，是記錄規律、整理順序、推演過程最重要的科學工具。藉由一項項的科學觀察與紀錄，費瑪的規律整理為「安全」奠定了深厚與重要的里程碑。讓我們看看「$a^{p-1} \bmod p=1$」，上一期介紹公開金鑰時留下的足跡，其中 p 為質數，此算式即為 a^{p-1} 除以 p 取餘數的結果會等於 1。舉例而言：

若讓 $a=5$、$p=11$，我們可知 $5^{11-1} \bmod 11=1$。

若讓 $a=6$、$p=11$，我們亦可立即知 $6^{11-1} \bmod 11=1$。

若讓 $a=7$、$p=11$，我們馬上可知 $7^{11-1} \bmod 11=1$。

是否覺得神奇？是的，這就是規律。

法國的業餘數學家費瑪對密碼「安全」的啟蒙，開啟了科技領域裡密碼與安全機制的新歷史。

歐拉為費瑪的規律繼續加碼，是網路公開金鑰得以實務運作的重要基礎。

一百年過後，瑞士的歐拉（Euler, 1707-1783）為費瑪的規律繼續加碼，有著新規律，「$a^{\emptyset(n)} \bmod n=1$」，其中 $\emptyset(n)$ 為歐拉函數，數學家歐拉找出規律，給了這樣的含意：$\emptyset(n)$=「小於 n 且與 n 互質的所有正整數個數」（例如 $\emptyset(7)$ 為小於 7 且與 7 互質的數為 {1, 2, 3, 4, 5, 6}，個數共有 6 個；$\emptyset(12)$ 為小於 12 且與 12 互質的數為 {1, 5, 7, 11}，個數共有 4 個），這可是網路裡經典的公開金鑰得以實務運作的重要基礎。在歐拉的此一規律下，網路的「密碼安全」得以強而有力，阻擋任何非法企圖的訊息破壞者與偽造訊息的散播者，保障網路安全訊息傳遞的正確性、值得信任的真實性。

5G 中的資安風險

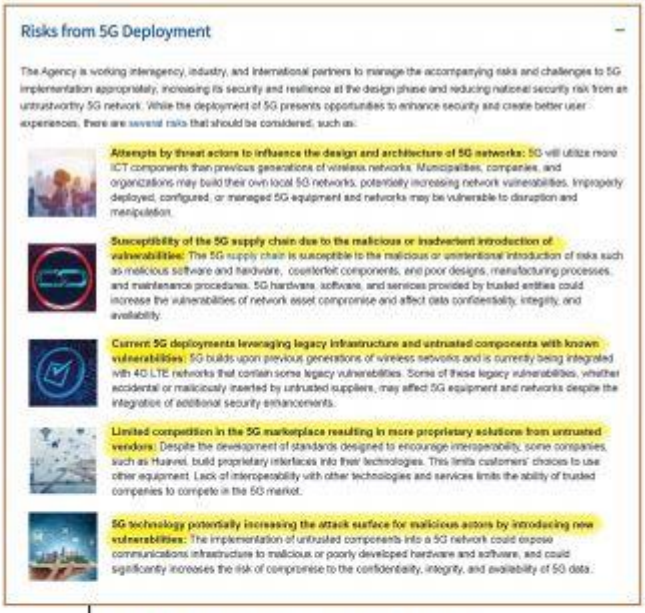
回顧我們的公開金鑰系統，「安全」有兩個目標，一者是「祕密性」、另一者是「真實性」。5G 裡所有的基礎來自前世代的通訊架構，是得以延伸而發展出來，所有 G 世代的安全問題如出一轍，卻也隨著資訊生活的普及，使得資安生活的安全意識更顯得重要。近年來網路通訊技術 5G 的推動，科技大國美國早已有所警覺並「超前部署」。根據美國負責「安全」的國土安全部與國家情報總監於 2019 年 5 月執行「保護資通技術及服務之供應鏈的行使命令」，藉此國土安全部緊接著發布「美國採用 5G 引發的風險概述」（Overview of Risks Introduced by 5G Adoption in the United States），列舉 5G 網路風險的脆弱性包含：供應鏈公司製造 5G 組件未經妥當的認證、傳承先前世代所承受的「網路安全」風險、5G 未來普及化部署實施過程安全配置、市場競爭機制不恰當、5G 技術操作標準等因素將增加 5G 執行的風險。

藉此，其中的「網路安全」，延續世代交替的密碼基礎，即 5G 系統的訊息正確性傳遞，需為通訊雙方所認可。若以密碼機制的公開金鑰系統來看此部分，也就是傳送方的訊息經網路傳遞的資訊，得被接

收方能正確的判斷訊息來源真實性。在公開金鑰系統的運作下，此一目標可以用傳送方的祕密 key 對訊息先做「驗證碼」的提供，而接收方將以傳送方的公開 key，對所接收的「驗證碼」進行檢驗，即可清楚判斷訊息來源真實性。

傳承費瑪與歐拉的密碼原理

我們再以孫悟空與牛魔王的通訊模式說明如下：老孫的「驗證碼」，是以老孫的「祕密 key」對訊息做加密得到「驗證碼」。當老孫傳送訊息給老牛時，「驗證碼」也將一併送出。接收方的老牛即以小猴的「公開 key」來解密「驗證碼」，再比對傳送訊息與解密「驗證碼」運算的結果，得為辨識真假訊息的依據。在公開金鑰系統下，若非老孫的小猴公開 key，是無法對網路所傳遞的「驗證碼」做正確解密運算，以得到吻合的比對結果。因為唯有同源（即代表老孫分身的



Risks from 5G Deployment

The Agency is working interagency, industry, and international partners to manage the accompanying risks and challenges to 5G implementation appropriately, increasing its security and resilience at the design phase and reducing national security risk from an untrustworthy 5G network. While the deployment of 5G presents opportunities to enhance security and create better user experiences, there are several risks that should be considered, such as:

Attempts by threat actors to influence the design and architecture of 5G networks: 5G will utilize more ICT components than previous generations of wireless networks. Municipalities, companies, and organizations may build their own local 5G networks, potentially increasing network vulnerabilities. Improperly deployed, configured, or managed 5G equipment and networks may be vulnerable to disruption and manipulation.

Susceptibility of the 5G supply chain due to the malicious or inadvertent introduction of vulnerabilities: The 5G supply chain is susceptible to the malicious or unintentional introduction of risks such as malicious software and hardware, counterfeit components, and poor designs, manufacturing processes, and maintenance procedures. 5G hardware, software, and services provided by trusted entities could increase the vulnerabilities of network asset compromise and affect data confidentiality, integrity, and availability.

Current 5G deployments leveraging legacy infrastructure and untrusted components with known vulnerabilities: 5G builds upon previous generations of wireless networks and is currently being integrated with 4G LTE networks that contain some legacy vulnerabilities. Some of these legacy vulnerabilities, whether accidental or maliciously inserted by untrusted suppliers, may affect 5G equipment and networks despite the integration of additional security enhancements.

Limited competition in the 5G marketplace resulting in more proprietary solutions from untrusted vendors: Despite the development of standards designed to encourage interoperability, some companies, such as Huawei, build proprietary interfaces into their technologies. This limits customers' choices to use other equipment. Lack of interoperability with other technologies and services limits the ability of trusted companies to compete in the 5G market.

5G technology potentially increasing the attack surface for malicious actors by introducing new vulnerabilities: The implementation of untrusted components into a 5G network could expose communications infrastructure to malicious or poorly developed hardware and software, and could significantly increases the risk of compromise to the confidentiality, integrity, and availability of 5G data.

美國國土安全部超前部署，列舉 5G 網路風險的脆弱性。（Source:CISA, U.S., https://www.cisa.gov/5g#risks）

在公開金鑰系統的運作下，可以用傳送方的祕密 key 對訊息做「驗證碼」的提供，而接收方將以傳送方的公開 key，對所接收的「驗證碼」進行檢驗，即可清楚判斷訊息來源真實性。

圖 1　公開金鑰驗證訊息真實性的通訊模式

小猴）的公開 key，才能與本尊老孫所採用的祕密 key 搭配，正確加解密，「還原真相」，得以做正確比對而檢驗出訊息真實性。（參考圖 1 說明）

這裡讓我們玩一個小戲法，讓老孫有著祕密 key，key 老孫 =3；公開 key，key 小猴 =7。另外再用一些數字當作訊息傳遞過程是否能判斷真實訊息的依據。

【範例】

讓訊息（數字）=「19」，老孫用祕密 key 老孫 =3 進行運算如下：$19^3 \bmod 33=28$（19 的 3 次方，再除 33，會餘 28），其中數字 33 為密碼環境中的微妙條件，戲法裡我們先賣關子，後續將陸續說明神奇卻簡單規律，得以創造強而有力密碼的安全系統。運算結果的數字「28」即是代表老孫為傳送訊息「19」過程中，所一併產生的驗證碼。老孫將一起傳送訊息「19」與檢驗用的驗證碼「28」，即傳遞{「訊息 19」，「驗證碼 28」}給老牛。老牛接著用老孫分身小猴的公開 key 小猴 =7，進行運算如下：$28^7 \bmod 33=19$。此結果將神奇地得到一個似曾相識的數字 "19"。是的，過程所傳遞的原訊息「19」與老牛運算得到的 "19"，竟是一樣的。這可不是偶然的發生，而是費瑪與歐拉這些科學先驅者所留下的智慧寶藏。

5G 基礎建設的發展需各領域技術相互依存、搭配與結合應用，加碼「安全」保障下的資安科技才能近乎「完美」。

科技不只來自人性 資安科技加持　更能深得人心

5G 通訊技術，是延續先前世代的所有基礎，我國行政院自 2019 年核定「臺灣 5G 行動計畫」，由國家通訊傳播委員會執行推動 5G 資安防護計畫。另外 2019 年開始實施的《資通安全管理法》，使得資通安全成為資訊生活裡必然得瞭解的科技基礎常識。而公開金鑰基礎建設（Public Key Infrastructure, PKI），讓 5G 承接各世代資通安全裡「網路安全」的重要技術與管理架構，得以具體實現資安科技。5G 未來十年的布置，結合我們已導入的 PKI 機制，5G — PK（5 Generation with Public Key）基礎建設利用公開金鑰系統的密碼技術、安全協定、鑑識判讀等相關資安技術，才得完善 5G 時代的「快」與「準」。科技的發展需各領域技術相互依存、搭配與結合應用，加碼「安全」保障下的資安科技才能近乎「完美」。資安生活的放心，不只廣告用語：「科技始終來自人性」；我們想說：「科技不只來自人心，以資安科技加持更是深得您我心」。

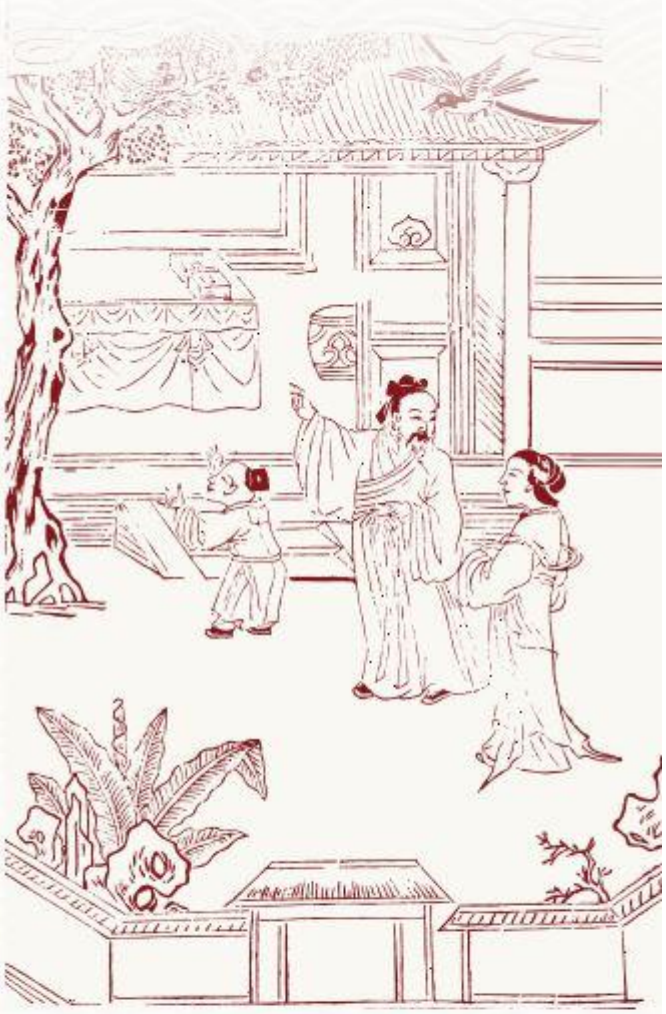
本文摘自清流雙月刊**中華民國110年3月 號P46-P52**
政風宣導電子專刊　中華民國110年4月　公務機密維護宣導

至聖之後的至慎先生-絕口不談人事、不說禁中樹

臺灣警察專科學校前校長／陳連禎

至聖之後的至慎先生

—絕口不談人事、不說禁中樹



◆ 臺灣警察專科學校前校長 — 陳連禎

居家不談人事，閒聊不涉公事，是公務員的基本素養。漢朝孔光稟性周密，典守樞機多年，時有上書，輒削稿銷毀，此固畏懼公事外洩。休假在家燕語，始終不及半句宮中政事，或問長樂宮溫室殿中樹，孔光則選擇沉默不應，答非所問。他事事至慎，故能終身無過，成為歷史保密美談。

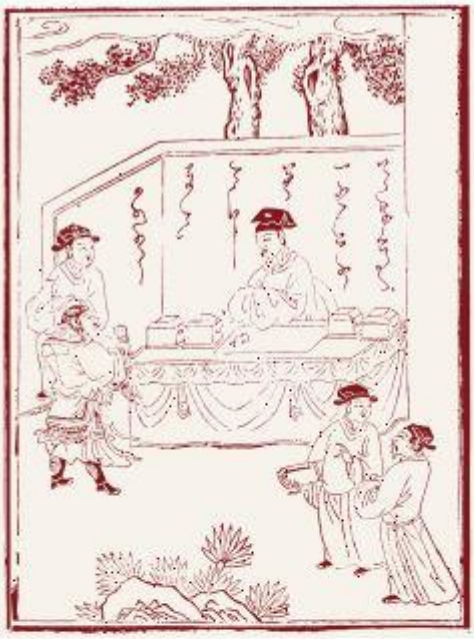
禁中—皇帝駐蹕處所及論政宮殿之統稱

自古以來，皇宮內有論政的宮殿、官署，還有帝后皇家居住的地方，後者通稱禁中；後人將警衛森嚴的宮中、府中以及皇帝駐蹕處所，都稱禁中。置身禁中人員必須絕對保密，禁止對外感言發聲，如果洩漏了禁中談話內容，就是死罪。《史記》曾記載有人洩漏始皇帝的行蹤給丞相李斯，而引發始皇帝強烈不滿，致禁中隨扈全遭殺害之史事。

國政興革都在禁中密商 置身禁中必須絕對保密

廁身禁中者必須絕對保密，否則會闖大禍。主因是為了維護最高領導者的神祕色彩，不能讓臣民窺見其真面目或知道他的底細，就可讓人心存畏懼，不敢造次。其次，為了鞏固領導中心的萬全，帝王須與人保持距離，才不會受到任何危害與驚擾，因此帝王行蹤，必須列為最高機密，以防出現危安漏洞。最後，當然是因為國政興革都在禁中密商，禁中關涉國家安全，當然要嚴防外洩，以免暴露維安破口。職是之故，不是經過精挑細選的忠誠之士不能接觸禁區。因此，凡入出禁中者，無不以口風緊、不洩密為工作倫理的最高美德。

《漢書 · 孔光傳》記載孔子十四代孫的孔光廁身禁中，於公於私都能嚴守口風，為漢史留下一道難得好風景。



孔光保密工夫到家
連禁中之樹都絕口不提

孔光品學兼優，當過議郎、僕射、尚書令等職；他嫻熟典章制度，法規命令如數家珍。孔光思慮周密、行事謹慎，未嘗有任何過失，多次受到表揚。孔光後來升為九卿的光祿勳，參贊中樞機密十餘年，遵守法度，仍不斷學習漢法的精義，很得漢元帝的信任。

孔光工作態度認真外，更有同理心，處處為人設想，因而得到上下的敬重。例如他時有建言，每次奏書核批下來，立即銷毀草稿。孔光認為個人留下底稿，恐會有外洩機會而暴露上級長官的過失，而且又有沽名釣譽而想博得忠直美名的私心之虞；這樣的心機是為人部屬的罪過。又如每逢休假，孔光經常和家人閒話家常，但是話題始終不會觸及朝廷禁中的事務。就有人好奇地探問孔光：「溫室殿上種的都是那些樹呢？」孔光保持沉默不應，立即改用其他話題支開。溫室殿是何等機敏重地，孔光連禁中之樹都絕口不提，遑論其他機敏人事政務，真是保密到家。

由於孔光是皇帝師傅的兒子，飽讀詩書，很早就服公職，難免有很多官員想接近而有所他圖；但孔光為官低調，既不結黨交遊，也沒有養賓客、培植私人勢力的習氣。歷史人物中，如孔光從政經歷如此完整，幾乎前所未見。他歷任漢家 3 代皇帝，為官前後擔任御史大夫、丞相各 2 次，又曾任大司徒、太傅、太師等要職，服公職 17 年，而身後備極哀榮。王莽陳請太后以最高規格辦理喪事，博士護駕行禮。太后派遣謁者持節視喪。公卿百官聚集弔唁

送葬。羽林孤兒四百人輓送，禮車萬餘輛送行，經過道路的居民無不舉音悲痛。

孔光居高位多年，而能善始善終，歸根究柢是他深具高度的風險意識：身為至聖先師孔子的後代，懷有強烈的責任感，不能有辱先祖家風的信念。其次是終身學習經典又嫻熟法制，與時俱進，處事嚴謹而受到上下的尊敬。再其次是為人具有同理心，上書後銷毀草稿，不留底稿的用意，除了不矜己能之外，也嚴防草稿外流而洩密。功歸長官，沒有私心，當然讓人放心。

至於為國推薦舉才，他都唯恐人知而增加人情負擔；不誇己功，更受尊重而屢受重用。最後也是最難得的是，參贊國家機要多年，都嚴守口風，即使是家居生活，人或問起宮殿上所植的樹木，隨時隨地心存危機警覺，已經成為工作習慣，斷然不肯鬆口。

吉人辭寡　最好無言

常人好奇探問，又喜愛爆料以為先知。然而吉人辭寡，最好無言，唯有懂得自律以保護自己，魔鬼就無法藏在細節裡作祟。孔子至聖，而後代子孫孔光至慎，慎處禁中事，無不憂患全身。孔光一生具有高度危機意識，已成公務員守密的典範。

唐太宗時期接任魏徵的宰相楊師道為人謹慎，從未洩漏禁中語。他常說：「年幼的時候，我讀過《漢書》，上面說孔光不言溫室之樹，我非常欽佩他的保密素養。」於公於私有高度的危機意識，絕口不談人事、不說禁中樹的保密素養，就能阻絕「黑天鵝」意外事件發生。

本文摘自清流雙月刊中華民國110年3月 號P53-P56