



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 (ESAM) 理事長、中央警察大學資訊管理學系專任教授 — 王旭正

網路的興起，改變了人們溝通的方式，不再有面對面的必要性，不再有「一日不見，如隔三秋」之吟頌，也不再有傳統生活作息一天「二十四小時」的不可分割性。

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。

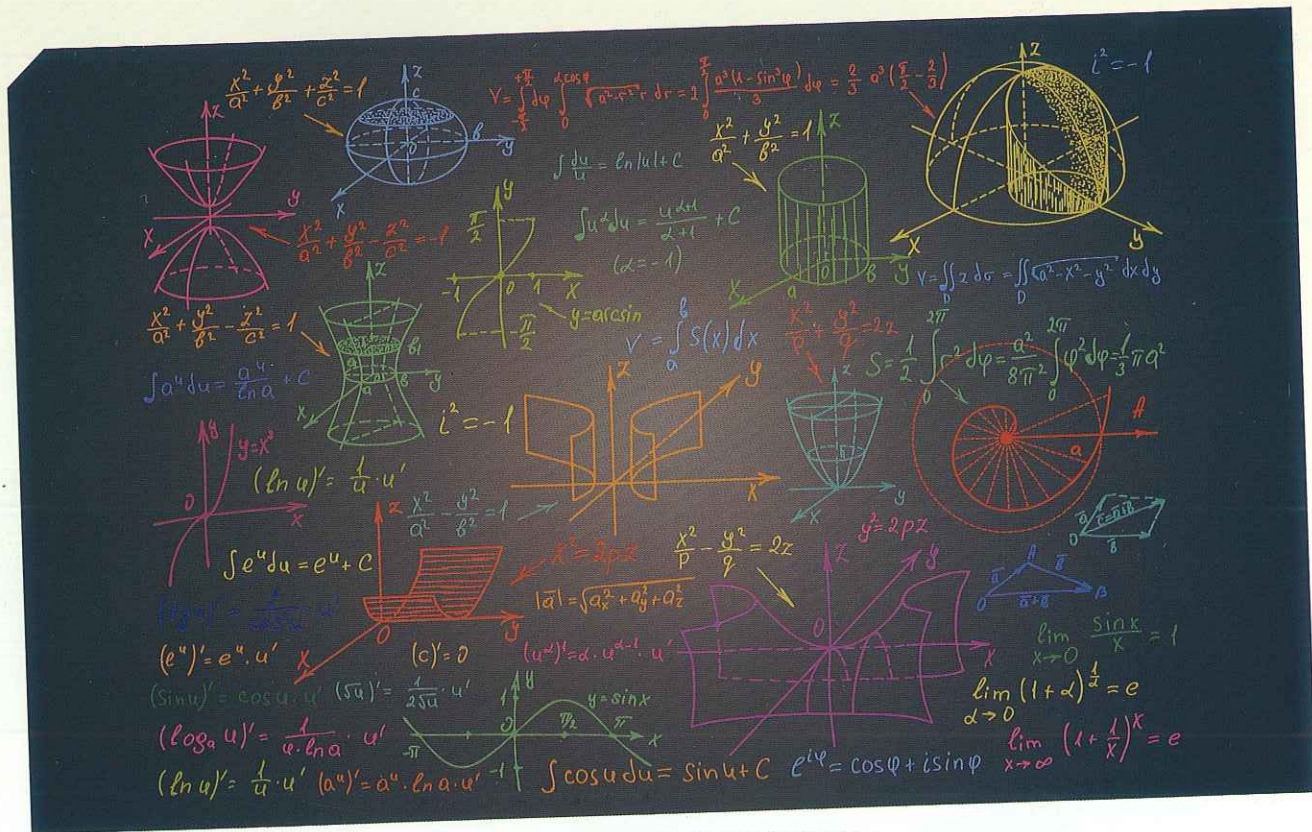
「快」5G

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，「 $a^{\phi(n)} \bmod n = 1$ 」，其中 $\phi(n)$ 為歐拉函數，數學家歐拉找出規律，給了這樣的含意： $\phi(n)$ = 「小於 n 且與 n 互質的所有正整數個數」（例如 $\phi(7)$ 為小於 7 且與 7 互質的數為 {1, 2, 3, 4, 5, 6}，個數共有 6 個； $\phi(12)$ 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

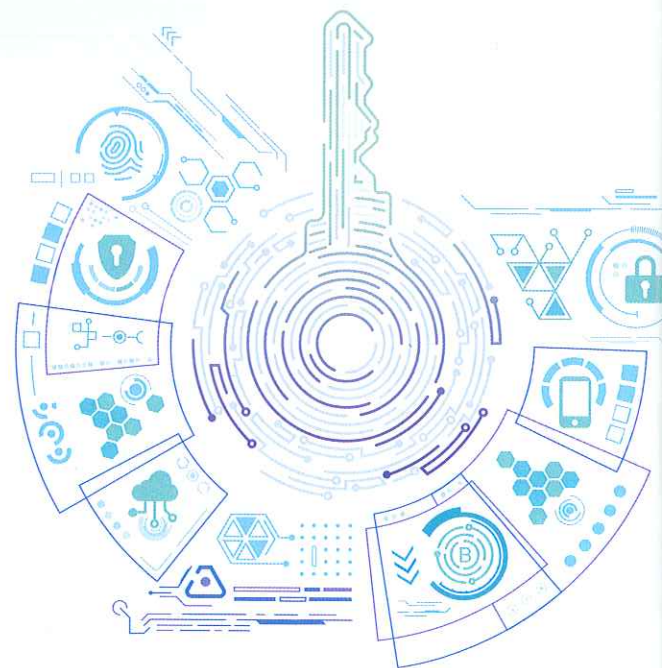
的「祕密 key」對訊息做加密得到「驗證碼」。當老孫傳送訊息給老牛時，「驗證碼」也將一併送出。接收方的老牛即以小猴的「公開 key」來解密「驗證碼」，再比對傳送訊息與解密「驗證碼」運算的結果，得為辨識真假訊息的依據。在公開金鑰系統下，若非老孫的小猴公開 key，是無法對網路所傳遞的「驗證碼」做正確解密運算，以得到吻合的比對結果。因為唯有同源（即代表老孫分身的

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 increase 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。

② 訊息真實性判讀



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」。

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，此因畏懼公事外洩。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。