



網路與公開金鑰的

奇蹟

◆ 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—電腦生命力的延伸

網路，現代科技蓬勃發展的最佳助選員，催生各式科技應用如雨後春筍般，一個個接連地冒出頭。網路將固定性的個人電腦，可攜性的手機等機器串接起來，讓這些替代人類工作的機器得以快速地交換訊息。在人的思維下，我們不斷創造「不可能」的奇蹟，而數學則是人類思維的規律性整理，不斷地觀摩、探索、實驗（若邏輯錯了再修正調整，前進下一階段）。

藉數學，科學之母的「愛」，讓人類天馬行空的思維得以實現，電腦的問世即是數學的實現之一。藉由機器的重複運算，把人類的想像，在機器、電腦的演算法中，逐一實現。

在網路世界裡，「個人」電腦讓每個人都得以迅速傳送訊息，也得以接收不同電腦使用者所分享的各式各樣資訊。亦可在網路平臺下載、讀取、吸取各形各色的知識訊息，提升生活、工作的品質。藉此，



網路將固定性的電腦和可攜性的手機等機器串連起來，讓這些機器得以快速地交換訊息。

是否可以直觀地體會到電腦搭配網路是多麼地好用，多麼地讓我們在資訊分享、新知汲取、生活需求上，以最方便、最迅速的方式成為我們資訊生活中「愛」不釋手（愛在手上、身上、永遠有一個超級無敵小的個人電腦—手機）且緊密結合生活裡食、衣、住、行、育、樂的「無所不在」。

網路—讓生命更加多彩繽紛

試想，沒有網路的连接是怎樣的情境？

- 早上起床、想要聽首 You Tube 的歌曲，可以嗎？



現今，手機搭配網路的各種功能已和人們的日常生活密不可分。

- 上班族準備出門前，想了解可搭乘的交通工具，（如公車站牌的到達資訊），在到達前 1 分鐘才悠然在站牌出現，可以嗎？
- 在公車到達前，自在無憂的在家、在早餐店裡，桌上一杯香磨咖啡，嘴上品嚐

漢堡美食；或在中式早餐店，品味濃郁豆漿、飽滿的傳統飯糰、古早味蛋餅，可以嗎？

- 到了上班處所，中午懶得外出，在辦公桌前點現今流行的“Uber Eats”、“Foodpanda”，呵呵，神奇地，不久後，熱騰騰、香噴噴的飯菜出現在面前，可以嗎？
- 炎熱的夏天，下班回家前，希望家裡的冷氣、3C 設備能自動啟動，在回家開門的那一瞬間，歡迎主人的歸來，可以嗎？

是的，這些都不是口號了，在網路「無所不可能」的通達裡，一切都是真的。沒了網路，科技就相形失色（或誇張地「瞬間消失」），成了「黑白」的人生，這似乎是可想而知的。網路在我們生活中的地位，以逆向的推想下，就能知道其不可或缺性。

有了網路安全，才有甜蜜可能

有了科技、有了電腦、有了網路，人們還需要什麼？我們開始進入主題。文明的發展，科技的催生，先求有再求好，沒



沒了網路，科技就相形失色，如今在食、衣、住、行等生活各面，網路運作無所不在。

有「安全」的加持，這檔事就永遠是沒有「保障」的缺憾。我們不會讓安全缺席的，安全裡的「祕密」與「真實」是自古以來人們最在乎的兩大存在價值。

1970年代後，網路安全的必要性已被資安專家、密碼研究者看出將成為科技趨勢的基礎，建構「安全」的網路才能成就科技帶來的「便利」與習慣的「理所當然」。「安全」的基礎觀念就是「祕密」的保護與「真實」的判斷。打破傳統的思維，如何讓保障「祕密」的“key”不再只是「隱藏」，只讓祕密的擁有者知道？如何讓相互通訊的彼此無論認識與否，皆能自然地對通訊的「祕密」做加解密？在網路的傳遞裡，藉「安全」的機制能彼此輕鬆地分享祕密，並阻擋其他「好事者」、「竊聽者」，使之望而卻步、無計可施，達到祕密通訊的目的。

科技與神話的時空交錯

「公開金鑰」系統（public key system）即是現代「網路安全」的重要基礎。《西遊記》中其實也有著「公開金鑰」的玄機，是否記得唐三藏團隊中的孫悟空（簡稱老孫）？這老孫有著許多戲法，藉著從菩提祖師那學到的「變變變」，而能在〈摘



藉由「安全」機制能在網路傳遞裡彼此分享祕密，並阻擋他人竊取，達到祕密通訊的目的。

吃仙桃〉、〈大鬧天宮〉、〈西天取經〉的故事中，從身上拔出一叢猴毛，嘴裡吹出一股氣旋，讓那叢猴毛變出千百個「小孫悟空」的小猴兒，這些小猴兒都是老孫的化身，舞刀弄劍與妖魔鬼怪廝殺，神話故事場面看得津津有味、記憶深刻。

每隻小猴都是本尊老孫的分身，傳承老孫所有功夫，得以與所有妖邪對抗。以此引申到金鑰的概念，即為當老孫本尊有一把 key，得以加解密時，老孫所變出的千百個分身小猴也都代表著老孫，所以這些小猴所持有的 key 都是來自老孫本尊，

所有 key 都能對「祕密」加密與解密。換言之，用小猴的 key 加密，也能用老孫本尊的 key 解密，如此即代表這些 key 的群體是相互有關係，能得以對「祕密」做加密與解密的處理，並自然地回復「祕密」的內涵。

藉此我們即知一個重要的概念推廣與應用，當老孫與眾分身小猴皆有 key 時，我們將傳統 key 的思維做些調整，即 key 的擁有者不再只有傳統的一把 key，而是擁有一把以上的 keys。而這些 keys 之間，是可以相互搭配來對「祕密」做處理（即加密解密運算），對應到故事中，即為本尊與

分身的同源性，藉由同一源體的本尊與分身的搭配即得以因應各式的需求與應用。例如以分身小猴的 key 對「祕密」做的任何加密處理，都得以本尊老孫的 key 作解密，以還原得到「祕密」。

依此脈絡下，若將分身小猴的 key 作為可公開的 key，讓所有欲與老孫祕密通訊者皆可用這些 keys 來對「祕密」做加密處理，傳送給老孫；收到的本尊老孫即可用老孫的 key 解密，如此一來即自然而然的以加密保護了「祕密」，卻也只有老孫本尊得以解密。此即科技與神話情境的時空交錯。



套用在金鑰的概念上，具有同源性的孫悟空（本尊）和以猴毛變出的小猴（分身），就是可以相互搭配來進行加解密運算的 keys。



圖 1 公開金鑰系統下牛魔王與孫悟空的安全祕密通訊

公開金鑰系統讓「網路安全」得以有最大的保障，使得「祕密」的傳遞，「真實」的判斷，得以在網路世界實現。所有的基本觀念傳承原始的傳統做法，key 還是對「祕密」進行「加」與「解」密的最關鍵元素。至於包裝祕密的各式方法，即是在公開金鑰系統理念下，如何來實現的下一個階段。

「公開金鑰」的玄機

回到網路公開金鑰系統下，我們再以《西遊記》的情境來做說明，以老孫與牛魔王這兩位人物的互動，可輕鬆揭開公開金鑰的運作。「公開」所指的是擁有 key

的主導者，為了順利在網路上達陣，將 key 分成 2 種型式，一部分來公開；另一部分仍是傳統的思維，即 key 本來是被主事者所祕密擁有，不得為任何其他人所知曉，如此才是安全保護的核心價值。

既然 key 公開了，那麼不就所有安全也都「公開」了嗎？這是一般人的誤解所在。公開系統的「公開」二字，僅限於主事者 key 的擁有與管理，為了在科技網路下依然能對「祕密」做安全保護，因此將「部分」的 key 做公開，此即「公開」二字命名來由。

依圖 1 所示說明：孫悟空與牛魔王（以下用「老牛」來稱呼）的互動裡，老牛欲

跟老孫作祕密通訊，那麼老牛會告訴老孫派個分身小猴來，小猴所持有的 key 可在網路裡公開被知，小猴亦可公開為老孫的分身。老牛看到分身小猴後，能用小猴的 key（公開的 key）將「祕密」做包裝加密，讓分身小猴將加密的包裝帶回，亦即由網路傳送給本尊的老孫。老孫輕鬆地看到加密的包裝，順手用老孫自己的 key 即可將包裝裡的「祕密」解密。因為老孫與小猴的 keys 是來自同源，小猴是老孫變出來的，當然老孫的 key 可輕鬆地解密。

這套戲法，依此「祕密」的傳遞方式，網路上的牛魔王也將是如此炮製，先有一些相互有關係的 key（內容值當然是不同的），且有自己的祕密 key，並公開一部

分的 key 於網路，使所有人皆知此公開的 key，若想跟老牛祕密通訊，即可用老牛的公開 key 做加密後的黑盒子包裝，而後傳送給老牛，老牛當然也輕鬆地用個人祕密持有的 key 得以將已加密的黑盒子包裝做解密。

談了公開的系統，神話故事裡的《西遊記》竟也搬上現代網路的檯面。那麼如何包裝神話故事的「古」事？如何不再只是「故事」？「前人種樹後人乘涼」，德國的高斯（Gauss）為資安的密碼技術奠下基礎；法國的費瑪（Fermat）閱讀書頁記事的神奇小定理， $a^{p-1} \bmod p = 1$ ，其中 p 為質數，為公開金鑰系統的現代網路的安全性，揭開運用的序幕。



社團法人台灣 E 化資安
分析管理協會 (ESAM)



中央警察大學資訊密碼暨建構
實驗室 (ICCL)

