公開金鑰密碼系統的奧妙

國立中正大學 資訊工程系　張真誠

e-mail: csiccc@cs.ccu.edu.tw

丹尼爾倚靠在陽台旁，隨手把玩著掛在頸上的銀鑰匙，嘴角浮起一絲微笑，銀鑰匙是凱蒂出生時，綠野天使送給凱蒂的見面禮，鑰匙是一對的，銀鑰匙可以將寶盒鎖住，金鑰匙則可以用來打開寶盒。丹尼爾與凱蒂的戀情，在貓城非常有名，埋伏的狗仔隊常用照相機偷拍兩人通信的內容，再將信件披露在貓城的頭條新聞上，為此，兩人常心煩不已。自從他們訂婚後，凱蒂爸媽就將銀鑰匙送給丹尼爾，讓他將信件放到寶盒中，用銀鑰匙將寶盒鎖住，交給信差送信，凱蒂收到寶盒後，再用金鑰匙打開寶盒，他們便可透過寶盒秘密通信。

故事中提到的用銀鑰匙鎖上寶盒，用金鑰匙打開寶盒的概念，在密碼學上有個專有名詞，叫做「公開金鑰密碼系統」，或「非對稱式密碼系統」，所謂的非對稱式的意思就是加密的金鑰與解密的金鑰不為同一把金鑰，若加密的金鑰與解密的金鑰為同一把金鑰，則稱此種加密系統為「對稱式密碼系統」。對稱式密碼系統有個缺點，就是加密的人必須將加＼解密的鑰匙（同一把）送到解密的人手中，或者他們事先說好用哪一把鑰匙（但若他們老用同一把鑰匙，當鑰匙被偷去複製，則用此鑰匙加密的信件就無法保密了），若丹尼爾不用公開金鑰加密系統加密，而改用對稱式密碼系統加密時，他必須先將加＼解密的鑰匙送到凱蒂的手上，他有兩種作法，一種是將當初鎖上寶盒的鑰匙交給信差，請信差一起送給凱蒂，另一種是請另一位信差，秘密的將鑰匙送到凱蒂手上。不論是哪一種方式，都不算很好的方式，一個是不太安全（可以打開寶盒的鑰匙與寶盒一起傳送），一個是太浪費人力（還得找另一位信差專送鑰匙）。有鑑於此，在 1978 年時，三位麻省理工學院的教授 Rivest、Shamir 與 Adleman（RSA）首先提出了一個植基於分解因數的「公開金鑰加密法」，它是加＼解密不用同一把鑰匙，且不需傳遞鑰匙的加密系統，就簡稱為 RSA。

當人們想在網路上傳送機密信件，擔心這信件會被有心人士非法攔截偷窺，人們便可用 RSA 公開金匙加密法將信件加密，就算有心人士攔截成功，由於沒有解密的鑰匙，也就無法得知信件的內容了。

RSA 的作法是這樣的，寄信者丹尼爾先到 key directory 取得收信者凱蒂的公鑰，用公鑰將信件加密，利用網路傳送，凱蒂收到信後，用自己的密鑰解密，便可順利讀取信件內容。以一個簡單的例子說明：

信件：m = 25。
公鑰：e = 3。
加密系統，將信件 m 加密成密件 c，$c = m^e \bmod n = 25^3 \bmod 55 = 5$。（55 為加密系統的參數，為任選的兩個質數的乘積，令此兩個質數為 p 與 q，n = p*q = 5*11 = 55）
密鑰：$d = e^{-1} \bmod ((p-1)*(q-1))$
$= 3^{-1} \bmod 40 = 27$。
密件還原成信件，$m = c^d \bmod n = 5^{27} \bmod 55 = 25$。

也就是說，凱蒂在製造自己的密鑰前，要先選取兩個質數 p 與 q，與任意一整數當其公鑰 e，並利用 $d = e^{-1} \bmod ((p-1)*(q-1))$求得密鑰 d，凱蒂將密鑰 d 保存在身邊，將公鑰 e 放到 key directory，而丹尼爾想寄信給凱蒂時，便到 key directory 去找是否有凱蒂的公鑰 e，用公鑰 e 將信件加密，再加以傳送，凱蒂收到公鑰 e 所加密的信件，便可用密鑰 d 解開，好順利讀取。在傳送的途中，若有人非法攔截到丹尼爾所加密的信件，因為沒有凱蒂的密鑰 d，所以頂多只能看到亂碼，無法讀取內容。

若將故事中的角色與 RSA 的例子做一個比對，則可整理如下：

信差：網路
公鑰 e：銀鑰匙
密鑰 d：金鑰匙
非法人士：狗仔隊
被攔截的信件：用照相機所偷拍的信件

最後，談一下 RSA 方法的安全性。密鑰 $d = e^{-1} \bmod ((p-1)*(q-1))$，公鑰 e 存在 key directory 中，e 很方便取得，寄信者的加密法是 $c = m^e \bmod n$，所以 m 與 n 也是已知。但要從 n 得知 p 與 q 是非常困難的。雖然 n = p*q，但我們幾乎無法從 n 的身上利用分解因數求出 p 與 q 這兩個質數，這種計算的問題是分解因數的問題，而這分解因數的問題已歷經數百年，許多聰明的數學家，迄今仍無法想出有效的方法，可以在有限的時間內從 n 的身上算出 p 與 q。既然這麼多聰明人都解不出來，那我們就姑且先當它是很困難的問題，因而目前而言 RSA 仍然是安全的密碼系統。