

活動 19

孩子的秘密 — 公開金鑰加密系統

活動摘要

加密技術對資訊安全來說是個關鍵。而現代的加密技術的關鍵，則是訊息的發送者只需要使用某些公開的資訊，就可以將一段訊息鎖住，只有特定的人才能解鎖打開。

這就如同每個人都買了一個掛鎖，在上面寫上他們的名字，然把它們全部放在相同的桌上供其他人使用。當然每個人自己都有自己鎖的鑰匙，但掛鎖是開著的，鎖上不需要任何鑰匙。如果你要寄給某人一則機密的訊息，你只需要把訊息放入一個盒子，拿鎖把它鎖起來，然後寄給收件者。即使盒子落入別人之手，因為沒有鑰匙，所以也無法打開。有了這樣的機制，大家就不需要事先溝通解鎖的密碼為何。

這個活動教大家如何在數位的世界中實現這個機制。不過在數位的世界中，我們不是直接拿起掛鎖鎖住盒子，而是去複製這個掛鎖，並使用複製後的掛鎖，把原始的掛鎖留在桌上。當然，如果我們要複製一個實際的掛鎖，我們得先把掛鎖解體，瞭解它如何運作才能複製。但是在數位的世界中，我們可以在不讓人知道鑰匙長什麼樣或掛鎖怎麼運作的情況下，直接複製掛鎖！

聽起來不可能？繼續讀下去。

課程銜接

- 技術：公開金鑰加密、密碼

習得技能

- 解決問題

適合年齡

- 11 歲以上

所需素材

把學生分成 4 組，每組再分成兩個小組。每個小組要分到一張「活動學習單：孩子的密碼地圖」（第 214 頁）。換句話說，每一組學生將需要：

- 兩張「活動學習單：孩子的密碼地圖」（第 214 頁）影本

你還需要：

- 一份「活動學習單：孩子的加密法」（第 215 頁）的（透明）投影片
- 一個在投影圖上做註記的方法



孩子的秘密

活動介紹

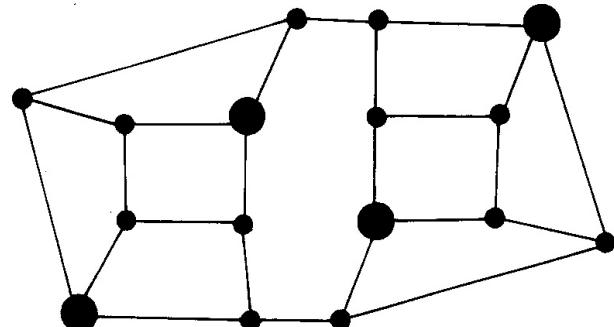
這個活動是這本書裡最具挑戰性的活動，需要十分細心與持續專注才能完成。學生們應該已經在活動 15 「旅遊小鎮」上學到何謂單向函數。如果也完成過活動 17 「傳遞機密」與活動 18 「秘魯式拋硬幣」，那這個活動應該就會比較容易上手。此外，這個活動也用了活動 1 「計算點點」與活動 5 「二十個問題」裡的概念。

Amy 正在計劃派 Bill 傳送一個秘密消息。通常情況下，我們可能會認為秘密消息是一個句子或一段話，但在接下來的練習中，Amy 只會發送一個字元 — 事實上，她只打算傳送一個代表字元的數字。雖然看起來只是個簡單的訊息，但是請記住，她可以發出一連串這樣的秘密訊息，最後組成一個句子。現實中這樣的工作會由電腦來完成，而有時即使是很小的訊息也是很重要的。在歷史上最有名的訊息之一 — 由 Paul Revere 所傳送 — 訊息裡傳達的只有兩個可能裡的其中一種¹。我們將看到如何使用 Bill 的公開金鑰來加密 Amy 的訊息。這樣即使有人攔截，也沒辦法對其進行解碼；只有 Bill 可以解碼，因為只有他有鑰匙。

我們將利用地圖來加密訊息。這裡的地圖不是指金銀島的藏寶地圖，而是像旅遊小鎮（活動 15）中的那些街道地圖：線條是指街道，而點則是指街角。每個地圖都有一個公開版本 — 就像上面例子中的掛鎖，以及一個私密版本 — 就像是例子中的鑰匙。

活動討論

在「學習活動單：孩子的加密法」裡的是 Bill 的公開地圖。這張圖不是秘密，Bill 可以放心把它放在桌上（或網頁上）給大家看，或提供給可能要發信給他的任何人。Amy 有這張圖的影本，其他人也有。而右邊的圖則是 Bill 的私密地圖。這張圖與他的公開地圖相同，只是把一些點（街角）放大。這個版本的地圖只有他有，要保密不能讓別人拿到。

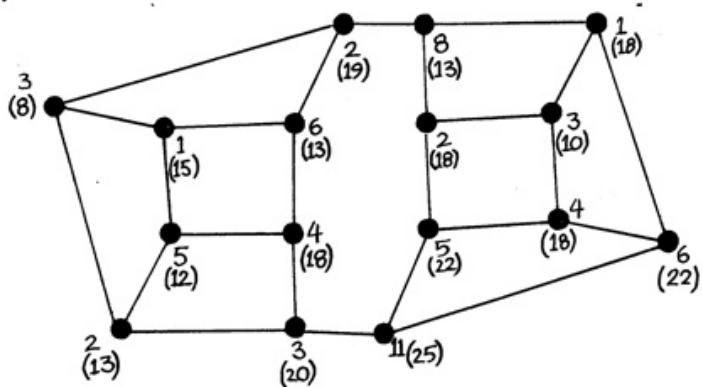


這個活動是最好作為一項課程，至少在開始時，因為它需要花費相當大的功夫。雖然並不算困難，但是一定要精確地進行，任何錯誤都會造成很多麻煩。因此，讓學生瞭解這種聽起來不可能的加密方法完全是可行的非常重要，因為他們需要這種動機來激發過程中所需的努力。

我們發現有一件事情可以高度地激發學生的興趣。告訴他們，使用這種方法，他們可以在課堂上傳遞加過密的紙條。即使被老師沒收，甚至老師們都知道這個訊息是怎麼被加密的，但他們還是無法解密。

¹ 大家可以參考維基百科上「保羅 · 列維爾」的條目。在美國獨立戰爭當時他為了盡速警告大家英軍來襲的路線，將訊息可能性降低到只有兩種：從陸上進攻或從海上進攻。

1. 把 Bill 的公開地圖顯示出來（學習活動單：孩子的加密法）。決定 Amy 要傳送哪個數字。現在，在地圖上的每個節點旁邊寫一個隨機想到的數字，但重點是所有的數字加起來要剛好等於 Amy 打算傳送的數字。我們來看看這張圖。假設 Amy 打算傳送的數字是 66，這張圖每個節點旁邊，沒有用括號括起來的數字加起來就剛好是 66。如果需要（而且學生會）的話，可以用負數沒關係。



2. 現在 Amy 必須計算發送給 Bill 的數字。如果她把地圖上沒括號的數字直接送出去給 Bill，那沒有任何意義，因為落入別人的手上時，任何人都可以把數字加起來就解開了。

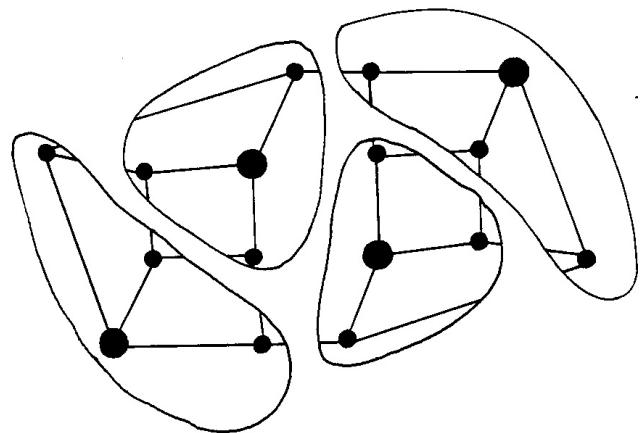
因此，我們換一個方式。選擇任何一個交點，看它和它的三個鄰居，然後把四個交點的數字都加起來。把算出來的總和寫在交點的括號中，或是使用不同顏色的筆來寫。例如，圖中最右邊的那個點，它本身數字是 6，而連接它的三個點分別是 1、4、11，四個點加起來是 22，所以就把 22 寫在括弧內。對所有在地圖中的其它交點重複此動作。

3. Amy 發送給 Bill 的地圖，只需要含括號內的數字即可。把原來寫的數字擦掉，只留下要發送的號碼，或者在一張新的地圖上重新寫上括弧內的數字。讓學生看看是否有任何方法，從這張地圖中找出原始訊息。他們會發現很困難。

4. 只有知道 Bill 的私密金鑰的人可以解出 Amy 要發送的訊息。在編過碼的地圖中，標記出在 Bill 私密地圖裡被放大的點。

要解碼訊息，Bill 只需要看剛剛標記起來的交點，並將這些點的數字加起來。在這個例子中，這些節點的數字分別為 13, 13, 22, 18，加起來剛好是 66，也就是 Amy 的原始訊息。

5. 好玩吧！這是怎麼一回事呢？實際上地圖是特別設計過的。仔細看私密地圖上被標記的點。把這些標記點與它的三個相鄰節點圈成一組，這樣會剛好把地圖分成四個不重疊的片段，如圖所示。每個片段中被標記的那個點的值，還記得怎麼算嗎？對，就是標記點與三個相鄰的點的和。換句話說，每個標記點就是那個片段中所有節點最原始的值的和。所以四個標記點相加，剛好就會是 Amy 打算送出來的原始數字。



呼！發送一個字母似乎還滿麻煩的。沒錯，加密本來就不是一件容易的事。不過看看我們的成果：使用公開金鑰，不需要傳送者或發送者之間事先講好任何隱密的事情，就可達到傳訊完全保密的情況。你可以把你的公開金鑰放在一個佈告欄，任何人都可以給你一個秘密消息，但沒有人可以解密，因為他們沒有你的私密金鑰。而在現實生活中，所有的計算都是由電腦程式來完成（通常這些計算用的程式是內建在瀏覽器裡）。所以交給電腦就好了。

完成這個活動以後，你可以讓學生們知道，他們已經成為一個非常特別的團體中的一員——團體中的每個人都曾經自己用手用腦計算公開金鑰加密的訊息！這是連電腦科學家都認為幾乎不可能完成的任務，而真的很少有人這樣做過！

那麼，這個方法容易破解嗎？Bill 手上的私密地圖就像是在旅遊小鎮（活動 15）中的一樣，其中標記放大的交點就是放置冰淇淋車為所有街道上的人服務的最佳解——沒有任何人需要走超過一個街區。我們在旅遊小鎮活動中看到，Bill 要建立自己的私密地圖很簡單：只要從標記放大的點開始往外長就可以。但是要反過來找出最佳解，找到放置最少冰淇淋車的地點就很困難。目前除了透過暴力演算法以外沒有其他更好的方法。暴力法是試著配置一台冰淇淋車，試試每種可能性；然後配置兩台冰淇淋車，看看每種可能性 … 依此類推，直到找到一個最佳解決方案。沒有人知道有沒有一個較好的演算法，可以適用於任何地圖。很多人都已經試過了！

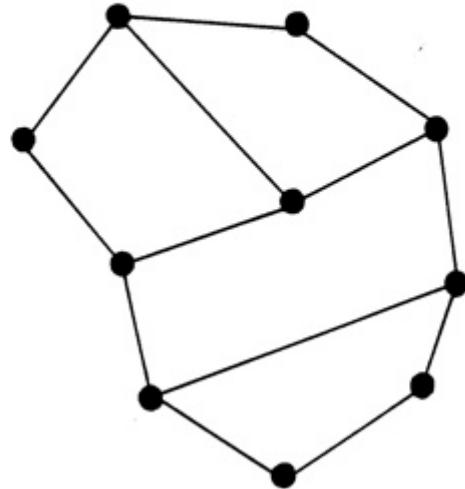
若是 Bill 一開始就用一個夠複雜的地圖（比方說，50 或 100 個交點），似乎就沒有人能夠破解密碼，即使是最聰明的數學家們努力嘗試也還是失敗。（但是有一個例外警告：請看後面的「這個活動在說什麼？」）

6. 向全班展示完這個例子之後，把學生分成四個一組。給每組裡再分成兩對，每一對學生學習活動單：孩子的密碼地圖上的公開地圖。每對要選擇一個「訊息」（任意整數），與公開金鑰對其進行編碼後，把得到的結果傳送給另一組。另一組學生可以試著進行解碼，看看有沒有辦法成功。然後給他們（或讓他們畫出）私密地圖，看看他們是否可以用私密地圖正確地解碼。

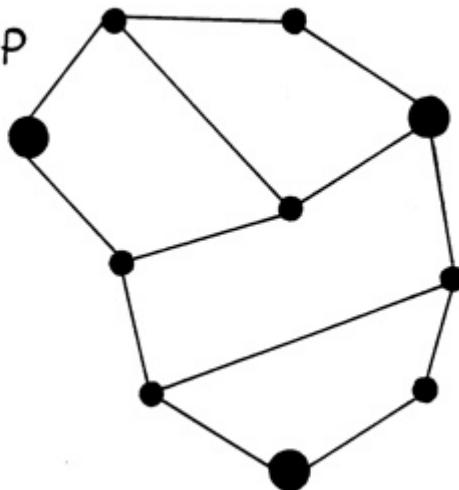
7. 現在，每一對學生可以設計自己的地圖。把私密版地圖保護起來，把公開地圖發布給另一對，或發布在教室的公布欄上。設計地圖的原理與我們在旅遊小鎮活動中所討論的相同，也可以添加額外的街道（線條）來增加複雜性。只是要注意：別把額外的街道連到任何的「特殊標記」節點。因為這樣會出現一個路口（節點）同時相鄰於二台冰淇淋車（特殊標記節點）。在旅遊小鎮問題中這倒還無所謂，但在加密時會造成嚴重的問題。因為特殊標記點就無法再分解圖成如上面私密地圖顯示的「不重疊的區塊」。這一點非常重要。

活動學習單：孩子的密碼地圖

public Map



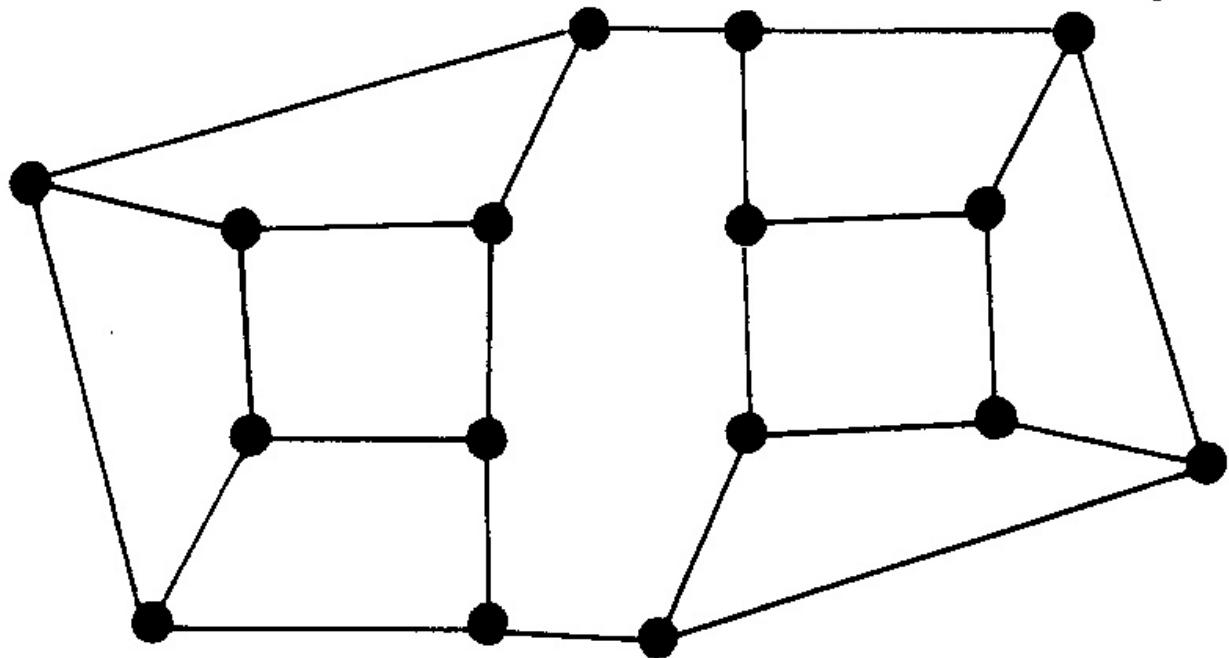
private Map



用這些地圖，照書上的方法加密與解密地圖。

學習活動單 :孩子的加密法

把這個「地圖」展示給全班看 ,並用它來示範把一個訊息加密的方法。



這個活動在說什麼？

我們能透過電腦網路傳送機密訊息，而且除了收件人外沒有人可以進行解碼，這是很重要的技術。當然，除了這個活動中所說的方法外，也有其他方式可以做到；例如發送者和收件者有一個共用的，只有這兩人知道的密碼。但是，公開金鑰加密技術裡最巧妙的地方是：Amy 可以不必先與 Bill 事先講好任何秘密方式，只要從網頁上拿到 Bill 的公開金鑰即可發送秘密訊息。

保密是密碼學的一個面向。另一個面向是驗證：當 Amy 收到 Bill 的訊息，她怎麼知道真的是 Bill 傳來的，而不是某些人冒名頂替？假設她收到的電子郵件上面寫著：「親愛的，我被困在這裡，身上沒有錢。請匯 10000 元到我的銀行帳號，帳號是 0241-45-784329。愛你，Bill」她怎麼知道這封信真的來自 Bill？一些公開金鑰密碼系統即可用於此需求。就像 Amy 用 Bill 的公開金鑰來加密自己的訊息，反過來 Bill 也可以發送出只有自己才能產生的訊息——也就是用自己的私密金鑰來加密訊息。如果 Amy 可以用 Bill 的公開金鑰來解碼，那保證這個訊息一定是來自 Bill。話說回來，任何人不都可以拿到 Bill 的公開金鑰嗎？沒錯。不過因為訊息只發送給 Amy，Bill 可以用 Amy 的公開金鑰做第二次編碼。這種雙重編碼的方式經由相同的基本方式，也就是公開金鑰與私密金鑰，可以同時提供保密和驗證識別。

現在，該是談談另一個觀點的時候了。雖然在本次活動中所展示的方法，與工業強度的公開金鑰加密系統非常相似，但它其實不是一個真正安全的方式，即使用一個相當大的地圖也一樣。

原因是，雖然目前沒有已知的方法在任意地圖上找出放置最少冰淇淋車的方式，而這個方法從這個角度來看的確是安全的；但是恰好有一個完全不同的方法可以攻擊這個系統。這個方法學校的學生不太能瞭解，至少在高中以前；但你至少應該知道有這樣的方法的存在。我們可以說，這個活動介紹的方法對學校學生來說是安全的，但對數學家則不然。如果你不是學數學的，那下一段不看沒關係。

把地圖上每個節點編號為 1、2、3、...。把每個節點原本的數字用 b_1 、 b_2 、 b_3 、... 來表示。每個節點實際傳送出去的數字用 t_1 、 t_2 、 t_3 、... 來表示。假設節點 1 與節點 2, 3, 4 相鄰。因此該節點傳送出去的數字是：

$$t_1 = b_1 + b_2 + b_3 + b_4$$

當然，每一個節點都有類似的方程式。事實上，方程式的數量和未知的 b_1 , b_2 , b_3 數量相同。竊聽者如果知道公共地圖和傳送出去的數字 t_1 , t_2 , t_3 方程式，可以用一個聯立方程式求解的程式來計算。一旦算出了原來的數字，他們的總和，也就是原始的訊息也就被算出來了。因此沒有私密地圖也可以解碼。直接使用高斯消去法，解決方程式所需的計算工作量和方程式的數量成立方比；但由於這些方程式是稀疏方程式（sparse equations，也就是大部分的係數是零），因此還有更有效率的方法。跟成指數的計算工作量相比，用私密地圖來解碼還是最好的方式。

我們希望你不會覺得被騙了！事實上，真正公開金鑰密碼系統的處理跟我們在這活動中所學到的幾乎一樣。不同的地方是，他們使用的編碼技術是筆算算不出來的。最原始的公開金鑰的方法—目前也仍是最安全的方法—是基於對大數做因數分解的難度。

舉個例子：下面這個 100 位數的數字的因數有哪些？

94123436073592629469711721362945143575289813789830825413475322119426401213015
90698634089611468911681

別浪費時間算了（我賭你也不會真的去算）！答案是：

86759222313428390812218077095850708048977

跟

108488104853637470612961399842972948409834611525790577216753

沒有其他的因數了，因為這兩個數字都是質數。找到這兩個質因數是一個相當大的工程：實際上，即使用超級電腦也要算上幾個月。

現在，在一個真正的公開金鑰加密系統，Bill 可以使用這個 100 位數的數字當他的公開金鑰，而那兩個質因數當私密金鑰。要產生這樣的金鑰並不會很難：你需要的是算出一個非常大的質數的一種方式。找到兩個夠大的質數（這不會很難做到），乘在一起，賓果！這就是你的公開金鑰。對於電腦來說，把兩個巨大的數字乘在一起並沒有什麼大不了的。把公開金鑰公布出來，沒有人會知道你的私密金鑰，除非他們有機會用超級電腦好幾個月。如果你擔心他們真的有超級電腦，那就改用 200 位的質數，他們就得多花上好幾年的時間！最主要的是，破解私密金鑰所需的成本會遠高於它要解鎖的訊息的價值。在實際應用中，建立安全通訊頻道通常會用 512 位元或更大的金鑰，相當於約 155 位數以上的數字。

其實基於質數的公開金鑰系統，目前還不保證在沒有私密金鑰的情況下就一定不能進行解碼。但這一點也並不像上述我們說的那麼簡單。目前我們並不是用兩個質數作私密金鑰，然後把它們的乘積做為公開金鑰。我們用的數字是從它們衍生而來。但效果是一樣的：你還是可以透過分解因數來破解私密金鑰。無論如何，要讓這個方法成為一個適當的加密和解密演算法，這些問題其實也不難克服。但我們不打算在這裡再細說了。這個活動已經夠困難了！

基於質數的系統有多安全？大數的因數分解問題在幾個世紀以來，已經有許多世界上最偉大的數學家們投入，而已經發現的方法也比嘗試所有可能因數的暴力法要好很多，但還沒有人找出了一個夠快（即多項式時間）的演算法。當然，也還沒有人證明這樣的演算法是不存在的。因此，其實也可以說，這個方法不只是對學校的學生來說夠安全，對數學家也一樣。但我們還是要小心！正如有一種方式不需透過解決旅遊小鎮問題就可以找出 Bill 的訊息，實際上也可能的確有不需把大數做因數分解的方法來破解。當然，許多人已經仔細檢查過這一點，目前看來結果還算好。

另一個可能發送端只有少數幾個可能的訊息，竊聽者可以利用公開金鑰把所有訊息進行加密，然後比較他們所得到的傳送端發出來的加密訊息，就可以知道實際上發送出來的是哪一條訊息。Amy 的方法避免了這個問題，因為同樣的訊息（數字）可以有很多種方式來發送，只要每個節點數字調整一下即可。在實際狀況中，加密系統也會被設計成有很多很多可能的方式，多到即使用非常快的電腦也沒辦法把原始訊息試出來。

目前還不知道是否有夠快的方法來解決質因數分解的問題；目前也還沒有人設計出來。但是，它也尚未被證明是不可能的。如果真的找到了一個快速的演算法來解決這個問題，那就麻煩了很多目前使用的加密系統就會變得不安全了。在第四部分，我們討論了 NP 完全問題，他們「要嘛就全部有解，要嘛就全部無解」：如果其中一個問題找到了有效率的演算法來解決，那麼其他的問題必然都可以找到夠快的解法。因為對這些問題找出快速的演算法已經花了那麼久的時間卻仍然沒有成功，NP 完全問題似乎是可用來設計安全密碼系統的好選擇。不過嘛，這樣的計劃有它的困難之處，因此到目前為止，密碼系統的設計者還是必須靠實際上可能比 NP 完全問題容易一點（也可能容易得多）的問題（例如質因數分解）。以上這些問題的答案都價值數百萬甚至數千萬美元，而且對國家安全也是至關重要。密碼學現在在資訊科學中已經是一門非常活躍的研究範圍了。

延伸閱讀

Harel 的 “Algorithmics” 討論了公開金鑰加密；它說明了如何使用大質數來建立一個安全的公開金鑰系統。在資訊科學領域中，密碼學的標準教科書是 Dorothy Denning 寫的 “Cryptography and data security”，不過 Bruce Schneier 的 “Applied cryptography” 這本書更偏向實務應用面。Dewdney 的 “Turing Omnibus” 介紹了另一個用公開金鑰加密的系統。