2025 年【科學探究競賽-這樣教我就懂】

大專/社會組　科學文章格式

文章題目： 當鎖失去了鑰匙：量子電腦與密碼學的終局

摘要：隨著科技的高速發展，傳統超級電腦的運算速度正逐漸逼近極限。為了突破現有技術所面臨的瓶頸，人們將希望寄託於量子電腦，期待它能解決傳統運算力所無法克服的難題。然而，隨著量子技術的腳步日益逼近，現代密碼學的喪鐘也悄然敲響——我們賴以維繫資訊安全的加密體系，正面臨前所未有的挑戰。

文章內容：（限 500 字~1,500 字）

你是否有過註冊帳號時，被系統判定密碼強度太低，要求你加入特殊符號、大小寫不規則的字母與數字在密碼當中？或者是在新聞媒體上看到某間公司資料外洩了？又或者是帳號被他人給盜用的經驗？那你或多或少應該會覺得奇怪為什麼密碼會被判定強度太低、以及為什麼會被盜帳號、以及資料外洩？在繼續深入講下去之前，我們必須先認識密碼學是甚麼東西。

現今的密碼學課程，我們會將其分為兩大類，古典密碼學和現代密碼學兩種，前者多意指第二次世界大戰前，將明文轉換為密文的加密、解密演算法，多用於軍事傳輸公文來做使用，例如：古希臘斯巴達的密碼棒、凱薩密碼、二戰時期的恩尼格瑪機……；後者則多聚焦在由電腦加密的數位資料(由 0 與 1 組成的資料)，而其又可以被細分為兩大類，對稱性加密與非對稱性加密，對稱性加密你可以將其想像成傳輸方在傳輸資料時將加密文件的公鑰連同文件一並交由中間人轉交給接收方，而接收方則使用隨附的鑰匙來對檔案進行解密，而這麼做的問題是萬一這個中間人是有心人士的話，則有機率會竄改訊息，著名的例子有 AES、3DES；而非對稱性加密則是可以想像成傳輸方與接收方皆互相持有對方的公鑰以及自己的私鑰，當傳送方要傳送時，就用接收方的公鑰將訊息加密，接收方收到加密訊息後，再用自己的密鑰解開，這樣即使有心人拿到公鑰，只要沒拿到接收方的私鑰，也還是無法解密訊息，著名的例子有源於整數因數分解問題的 RSA、以及源於離散對數問題的 DSA。

那為什麼密碼會被破解？破解密碼的方式有很多種，最簡單也是最沒有效率的方式就是利用窮舉的方式進行暴力破解，還有社會工程、以及選擇性明文攻擊……方式。

這時不知道你會不會好奇量子電腦，這個和密碼學八竿子打不著的東西，為什麼會對其造成威脅，在我正式講下去之前我先介紹一下量子電腦是什麼。

量子電腦你可以把它想像成這是一台十分快速的超級電腦，他是基於量子位元，這是一種基於量子糾纏與疊加的位元，因此他既是 0 也是 1，而這種位元與傳統位元相比，傳統位元在做廣度搜尋時，一次只能跑一個資料，而量子位元則是一次就跑完一層資料。正是因為他的這個特性，才導致他在破解非對稱性加密特別的有效率。

然而，有沒有應對措施？好加在學界早就發現這個問題，目前美國 NIST 就正在開發

「量子安全加密演算法」，也就是就算有量子電腦也破解不了的新一代密碼技術。，未來我們不會因此遇到全球資安浩劫。

參考資料

1. https://www.niar.org.tw/xcscience/cont?xsmsid=0I148638629329404252&sid=0M10350591764310037O&sq=%E9%87%8F%E5%AD%90%E9%9B%BB%E8%85%A6
2. https://zh.wikipedia.org/zh-tw/%E5%AF%86%E7%A0%81%E5%AD%A6
3. https://aikawa0617.medium.com/%E5%AF%86%E7%A2%BC%E5%AD%B8-%E4%B8%80-%E5%8F%A4%E5%85%B8%E5%AF%86%E7%A2%BC%E5%AD%B8-455e43038241
4. https://pansci.asia/archives/331838

註：

1. 未使用本競賽官網提供「科學文章表單」格式投稿，**將不予審查**。
2. 字數沒按照本競賽官網規定之限 500 字~1,500 字，**將不予審查。**
   PS.摘要、參考資料與圖表說明文字不計入。
3. 建議格式如下：
   - 中文字型：微軟正黑體；英文、阿拉伯數字字型：Times New Roman
   - 字體：12pt 為原則，若有需要，圖、表及附錄內的文字、數字得略小於 12pt，不得低於 10pt
   - 字體行距，以固定行高 20 點為原則
   - 表標題的排列方式為向表上方置中、對齊該表。圖標題的排列方式為向圖下方置中、對齊該圖