# 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：** 隱形的小偷!是誰偷走我的資料?

**摘要：**現代生活中已經離不開數位科技，在享受便利的同時危機已悄然靠近，資訊攻擊使的我們不可忽視資訊安全的重要性，從國際到國內，從政府到民間，無不加強資訊保護以抵抗四面八方的威脅，在本文中將從介紹離我們最近的資訊安全應用—密碼，一直到數據傳輸時的安全保障—加密演算法，由淺入深探討密碼學。

**文章內容：**（限 500 字~1,500 字）

在早期的生活中，要保護自身的財務與資料的做法很簡單，僅需要資料放進保險箱，而竊賊必需實地走訪，接著找到保險箱，最後手動逐步破解密碼取得資料，而在現代社會中到處都充斥著數位科技的應用，帶給我們更加便利的生活，在網路上大部分每個人都會有好幾組密碼來保護各種不同的資料或作為網頁的帳號登入使用，但不同的是，網路上的駭客能夠使用各種攻擊手法取得使用者的帳號與密碼，常見手法如:社交工程、暴力破解、透過個人身分資訊去猜密碼等。


也因此密碼設定的強度，與自身對資安攻擊手法的敏感度成為了你的資料是否安全的第一道防線，接著進一步討論到資料保護的第二道防線—加密，加密演算法簡單來說就是將明文加密成密文後傳輸到對方手中，再解密回明文，早期知名的加密演算法如凱薩加密，就是一個將傳輸的內容逐個英文字母皆移動 n 格後即成為密文，例如: apple 經過 n=5 移動後為 fuunj，但是這種方式非常不牢固，因為只需要最多經過 26 次的測試，並從中找出有意義的文字即可破解此加密方式。

依據柯克霍夫原則，加解密演算法必須公開算法，並且不會因此對加解密產生威脅，評斷加解密演算法是否可靠，並非關起門來獨自運作，因為這種方式還是會很容易被人從明文與密文之間的關係找到漏洞，而是應該要公開讓各路好手去抓演算法的弱點並持續改善與優化，存活到最後的演算法必須經歷千錘百鍊才能成為一個好的演算法。

接著介紹到雜湊函數，這是一個現代普遍的演算法之一，做法為輸入長度不一的資料後，產生出固定長度的 hash 值，而這種演算法並不可逆，密文無法反推回輸入資料，且若輸入資料有一個字元的不同，則產生的 hash 值會有天差地遠的差距，相同的輸入資料則會產生相同的 hash 值，因此若需要將密文反推回去，只有逐一測試輸入資料並比對結果 hash 值是否相同這一個方式，因此若想破解 hash 值花費的大量時間與算力，使的這成為不可能的任務，也確保了雜湊函數對資料的保護性與安全性，在實務應用上可將密碼經過雜湊函數後將 hash 值儲存在資料庫中，之後的每次密碼輸入都經過雜湊函數運算後再與資料庫內的 hash 值比對。

雜湊函數還有一道保護方式，那就是在明文中加入 salt 之後再一起經過雜湊函數運算，salt 可隨機值穿插到明文中的任何位置，這樣一來即使 hash 值被破解了，得到的也只是明文與 salt 穿插的結果。

接下來要介紹的是對稱式加密，架構為明文與密文轉換僅透過同一把鑰匙運算，AES 加密標準為將不限長度的明文依照 byte 切成數個區塊，最後一個區塊空缺之處使用 padding 填補，接著每個區塊獨立和鑰匙運算，AES 可分成 CBC 與 EBC，介紹說明如下:

1. EBC: 將明文依照 byte 數切成數個區塊，並將每一個區塊獨立經過鑰匙加密後輸出，最終結果為每個區塊輸出的密文串接起來。
2. CBC: 將明文依照 byte 數切成數個區塊，並且當前區塊的明文與上一個區塊的密文經過 XOR 運算後，再交由鑰匙加密後輸出，最終結果為最後一個區塊輸出的密文。

最後要講到的是現代密碼學的主流架構—非對稱式加密，在此架構中每個用戶都會有私鑰與公鑰，顧名思義，私鑰僅限於本地端，而公鑰則開放給所有人使用，使用某人的公鑰加密過後的密文僅能透過對方私鑰解密，架構如下:

假設 A 要傳輸資料給 B

明文->B 公鑰加密->密文->從 A 傳輸到 B->B 收到密文->B 的私鑰解密->明文

如此一來便不會有初始私鑰傳輸過程被截取的風險，在著名的非對稱式加密演算法 RSA 運算方式如下:

前提: N 為兩個超大質數的乘積；e、d 為任意質數

假設 M 為明文；C 為密文

$$M^{\mathrm{e}} \bmod \mathrm{N} = \mathrm{C}$$

$$C^{d} \bmod \mathrm{N} = \mathrm{M}$$

公鑰為(N,e)；私鑰為(N,d)

在 RSA 演算法中的核心關鍵是 N，必須不能被人反推出是哪兩個質數的乘積，否則此加密方式將被輕易破解。

| 參考資料 |
| --- |
| **1.** Day 7：觀念篇 - 密碼學裡的雜湊函數是什麼？它跟加密差在哪？ - iT 邦幫忙::一起幫忙解決難題，拯救 IT 人的一天<br>**2.** AES 加解密-CBC ECB - 独孤剑—宇枫 - 博客园 |

**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