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： 密碼學：MD5 的墮落還是 SHA 的崛起

摘要：在現在這種充滿各式各樣科技的時代，設備及數據顯得尤為重要，其中的角色除了大家都熟知的電子設備，程式語言等，之外還有一個也是在現代社會中扮演者關鍵的角色「密碼學」

文章內容：（限 500 字~1,500 字）

1. **什麼是密碼學？**

   密碼學包含兩個核心部分：加密和解密。加密保護訊息，讓未經授權的人無法理解內容，生成所謂的「密文」。解密則是透過特定方法，將密文轉換回可讀的「明文」。它廣泛應用於網路安全和資料傳輸。

2. **MD5 的墮落**

   MD5 是一種早期就開始使用的雜湊函數從 1992 年就已經出現，從此成為市面上最普遍的雜湊函數，它可以將輸入產生成一份 128 位元的雜湊值（不論輸入長度），然而從 1996 年開始它的問題開始逐一暴露，MD5 在當年被證實了弱點的存在，它已經可以透過彩虹表去加以破解了，並且在後來 2004 年時發現還有一個大問題存在，就是「碰撞攻擊」指的是雜湊結果的衝突，以至於不同明文可能生成相同雜湊值，例如：輸入與我所設定的密碼不相同但雜湊值相同時也能登入。

3. **SHA 的崛起**

   SHA 其實跟 MD5 很類似它們都屬於雜湊函數，而 SHA 中最早的是 SHA-0 但是因為缺陷很快就被撤回，因 1995 年發表的 SHA-1 讓 SHA 開始被廣泛使用，而在後來 2001 年時也推出新的 SHA-2，SHA-2 即使到了 2025 年的今天，也沒有出現明顯的弱點，但在 2010 年時 SHA-1 已經出現了理論上的破解方式，如果證實有辦法破解，這樣市面上只剩一種雜湊函數，剩下的一但被破解那就都來不及了，於是在 2015 年就推出了新的 SHA-3，這也成為現在常見的雜湊函數之一，而 SHA-1 最終也在 2017 年被正式宣告攻破。

4. **結論：**

   現在 MD5 的優勢只剩下了處理速度快，不過這也可以算是缺點，因為它處理的速度足夠快，就算我透過暴力破解，它也不會花上太多時間，SHA 中現在最為普遍的是 SHA-256，它會將明文透過 SHA-2 的方式轉換成 256bit 的密文，這足足是 MD5 的兩倍長，從而減少哈希碰撞的問題，並且因為長度加長的緣故運行速度相較於 MD5 就會慢上不少，但換來的就是安全性的大幅提升。

參考資料
密碼學：https://zh.wikipedia.org/zh-tw/密码学 MD5：https://zh.wikipedia.org/zh-tw/MD5 SHA：https://zh.wikipedia.org/zh-tw/SHA 家族 MD5、SHA256 比較：https://hicalvin.github.io/tech/2022/11/md5_or_sha256

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