

活動 17

傳遞機密 — 資訊保密協定

活動摘要

加密技術讓我們能在擁有高度隱私的情況下和他人分享訊息。在這個活動裡提供了一個互相交流訊息但不洩露個別資訊的方法：一群學生能在不洩漏個別實際年齡的情形下，計算出他們的平均年齡。

課程銜接

數學：加總與平均

習得技能

- 計算平均
- 隨機亂數
- 協同合作

適合年齡

- 7 歲以上

所需素材

每組學生需要：

- 一些計算紙
- 一隻筆

傳遞機密



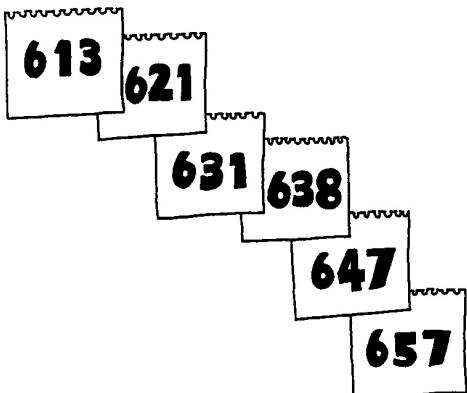
活動介紹

這個活動能在不洩漏任何人實際年齡的情形下，算出一群學生的平均年齡。另外，也可以用來找出一群學生平均拿到多少的零用錢，或是一些其他比較個人的資訊。這個方法尤其適合計算成人們相關的統計數字，因為年紀較長的人通常對收入和年齡等資料較為敏感。

一組至少要有三個人以上。

活動討論

1. 向組員說明你想要計算大家的平均年齡，但不能洩漏任何人的年齡。問問大家對這個要求有沒有什麼想法，或甚至問問大家覺得有沒有可能。



2. 找出六到十個人來。給第一個學生紙和筆，請他們在紙的最上方隨機寫下一個三位數字。以此圖的範例來說，613 是第一位學生寫下的隨機數。

3. 請第一個學生撕下第一頁，並將自己的年齡與亂數相加，寫在第二張紙上。比方說，第一個學生 8 歲，那就在第二張紙寫上 621。每個人要拿好自己的那張紙，不能讓別人看到。

4. 將便條傳給第二個人，第二人撕下第二張紙，將自己的年齡與第二張紙條上的數字相加，並將總和寫在下一張紙上。在這個範例中，第二個學生 10 歲，因此第三張紙上寫的是 631。

5. 持續照著這些流程，直到每個人都寫過，並且在手上有一張不給別人看到的紙條。

6. 將便條紙傳回給第一個學生，將紙上的數字減掉自己手上原來的數字。在範例中，便條紙總共傳給了五個人，最後的數字是 657，減掉第一個學生手上原本的數字 613，得到 44，這個數字即是所有學生的年齡總和，就可以以此算出平均值。因此，在此範例中的學生平均年齡為 8.8 歲。

7. 告訴學生們，除非兩個人刻意合作，不然只要撕毀自己的那張紙，就沒有人能知道自己的年齡。

活動變化與延伸

這個活動的進行方式也可以用來做秘密投票。做法就是每人同意則把數字加一、不同意則加零。當然，如果有人加或減了 0、1 以外的數字，這個投票就變得不公平了，雖然這種作弊方式還是有一定風險，當所有人都投同意票時，如果有人加超過 1 的數字，會讓同意票總數超過參與的人數。

這個活動在說什麼？

電腦儲存了大量的個人資訊：銀行存款餘額、個人社交網路、欠稅、駕照持有時間、信用記錄、考試結果、病歷等等。個人隱私非常重要！但某些情況下，我們仍然必須與其他人分享一些這方面的資訊。例如，當我們使用銀行卡付購物費用時，店裡需要驗證我們的存款是否足夠支付。

通常情況下，我們會提供比實際需要還要更多的資訊。舉例來說，如果我們在商店進行電子交易，他們實際上會知道我們用哪個銀行的帳戶、帳號為多少、我們的名字。此外，銀行也會知道我們在哪裡購物。銀行可以透過監測客戶在哪裡購買雜貨、每天花了多少錢購買、在什麼時間購買，藉此來建立個人資料。如果我們都使用現金付款，那當然就不會有任何個人資訊向外流出。大多數人都不太擔心個人資訊被共享，但其實有個潛在危險是這些資訊會被濫用，無論是在市場上（比方說，業者會針對某些花很多錢在購買機票的人，發送關於旅遊的廣告）、階級歧視（只針對富裕的客戶提供更好的服務）、甚至勒索（例如威脅某人要透露一些不想讓人知道的交易）。一般來說，如果人們知道自己購物方式會被監控，都會想改變這樣的購物方式。

這些隱私的損失大家似乎比較不以為意，但加密協定的存在仍然允許我們在用電子金融交易時，可以擁有跟現金交易相同的隱私水準。你可能很難相信，錢可以從銀行帳戶轉到商店帳戶，而沒有人知道錢的來源與去向。這樣做可以讓電子交易變得更合理：收付雙方都只分享到有限必要的資訊，而這件事可以透過一個聰明的協定來完成。

延伸閱讀

David Chaum 曾提出一篇經典的論文，將這些問題突顯出來，並使用了一個頗為挑釁的標題：「沒有身分識別的安全：一個讓老大哥（Big Brother）過時的交易系統」（譯註：Big Brother 是喬治·歐威爾所寫的小說「1984」中的角色。老大哥是大洋國的領袖，但沒有人實際上看過他的存在，只知道老大哥一直會盯著人民的一舉一動。）。此文頗值得一讀，裡面提供了一些關於資訊保密協定的簡單例子，包括如何使用電子現金交易而完整的保有隱私。這篇論文可以在 "Communications of the ACM"，1985 年十月號裡找到。