講題 ：Some Topics of Cryptographic Research
講者 ： 交大資科系 曾文貴教授
心得 ： 廖峻鋒(g9104@cs.nccu.edu.tw)

密碼學是用一些數學(科學)方法來保護資料，確認所有人都要經過授權才能存取資料。密碼學最早大都用軍事用途，像二次大戰時，美國的科學家就破解了德軍的 Enigma 密碼機器，造成德軍許多軍事計畫都事先被美軍識破。在當前網際網路發達的同時，密碼學被應用得更為廣泛。

現在一般有兩種類型密碼學被使用；symmetric key (對稱性的鑰匙) 和 public key (公開的鑰匙)(也叫 非對稱的鑰匙) 密碼學。相對於 symmetric key，public key 的方式因為不用考慮在網路上傳送 key，所以使用起來不但比較方便，也比較安全。不過在實作上，因為 public key 要消耗比較多的系統資源，所以也不見得能適用於各種場合。

為了平衡速度及安全性，目前大家比較傾向用二種混合的方式，也就是在二個傳送密件的端點還是採用 symmetric key 的方式，而在傳送 key 時，則以 public key 的方式來把 key 加密。不過如果沒有傳送 key 的問題的時候，還是使用 symmetric key 就夠了。以政大一個月後將上線的 Web Single Sign-On 系統來說，它會把加密後的 cookie 送到 client 端，加密 cookie 的方式便是 triple-DES(屬於 symmetric key 的 alogrithm)，因為加、解密都是在 Server 端做的，沒有傳送 key 時洩密的疑慮，所以才使用對稱 key 的方式來實作，以增進速度。

在聽過曾教授演講之前，我原本認為目前密碼學已發展到商業化的地步，這個領域的研究價值可能不高。不過聽完演講後才發現，隨著硬體速度的進步，很快地我們目前很滿意的加/解密法將不能使用，而尋找更安全，又不會損失太多運算速度的加/解密法正是目前密碼學專注的課題。就像老師說的，一旦量子電腦實用之後，我們當前的加/解密架構將一夕之間完全崩潰，這是很危險的事情。

另外，我也發現，要從高階的角度去了解 DES、RSA 的演算法還算不難，可是聽完老師的演講後才發現，真的要深入密碼學的領域，真的很不容易，很多密碼學基礎原理其實都不容易理解。不過無論如何，並不是在網路上的每一項資訊都要加密，應該先衡量必要性之後，才決定是否對資訊加密，此時做為一個密碼技術使用者的我們，應該要挑選幾個大家目前公認比較安全的加密技術來使用，隨時注意是否以前寫作的加/解密系統的核心技術目前已過時，並將過時的加解密模組更新，才能確保一個資訊系統的安全性。