H2E 電腦報告

我們的報告是來自於日本卡通電影

夏日大作戰

小磯健二，十七歲，雖然個性有些懦弱又不擅交際，卻是個差一點就能成為數學奧林匹克日本代表的數學天才。在高二那年的暑假，他答應心儀的學姊夏希陪她回長野的鄉下度過四天的假期。

當天晚上，健二收到一封 2056 位數等級的神祕數字簡訊，擅長數學的他不禁入迷熬了整晚並解謎成功，然而到了隔天早上，現實世界居然完全變了樣。全世界賴以維生的網路 OZ 出了異狀，虛擬世界裡的怪物吞噬了人們在網路世界裡的分身，甚至還企圖毀滅世界！！



我們要討論的關鍵字/問題是.....

- 網路隱私/密碼
- 虛擬世界/身分
- 駭客

- 網路是如何保障我們的安全？
- 虛擬世界的犯罪應該要在現實世界處罰嗎？
- 網路駭客到底是誰？

第一部分：網路安全機制

我們會簡單的介紹幾個常用的安全系統^^

密碼安全度/加密技術的強度

- ***加密技術***的強度指的是密碼破解所需要花費的時間與資源。
- 加密技術強度的高低通常牽涉到下列的因素：
  - ✓ 演算法強度 (密碼轉換法夠不夠複雜)
  - ✓ 金鑰保護機制 (密碼轉換後怎麼保護)
  - ✓ 金鑰的長度 (密碼本身多長)

嘿嘿~ 簡單介紹幾種鎖密方法~~

簡單的加密 ^^

- 取代(substitution)
  取代指的是明文中的每一個元素都被對應到另一個元素。
- 置換(transposition)
  置換是將明文中的元素重新排列。
- 相乘(Product)
  以取代與置換為基礎構成的複雜組合，以達到更複雜的相乘效果。

你看得懂我在寫甚麼嗎？

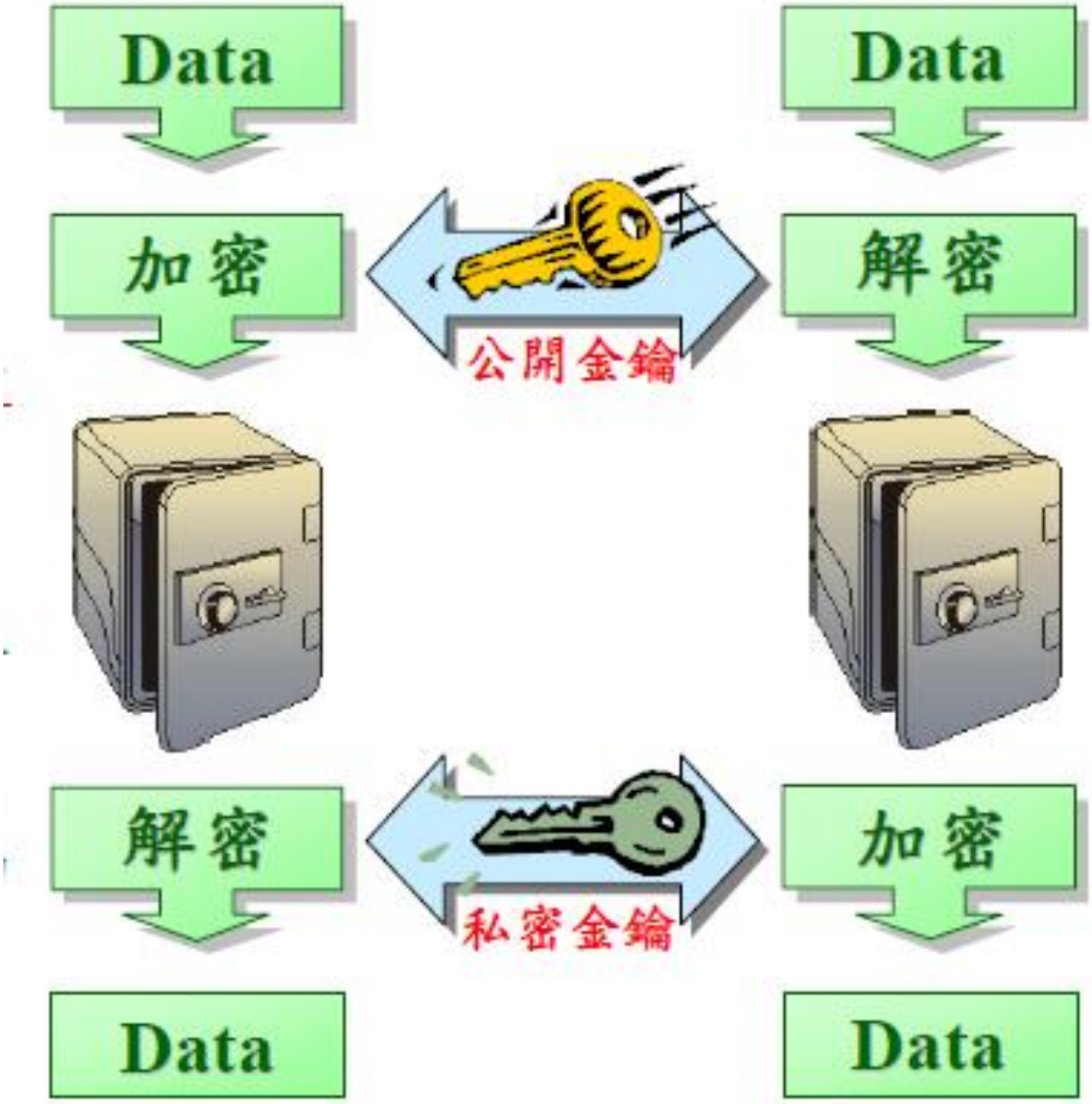
- YLIMAF
- ERA
- EW
- WE
- ARE
- FAMILY

對稱性/非對稱性密碼

- 密碼系統可以分成兩種
- 對稱性：就是把密碼經過F(x)=x+3這個函數加密。
- 如果設(A、B、……Z) = (1、2、……26)，經過F(x)→F(A)=1+3=4，而4就是D
  這樣子 “GEORGE” 就會變成 “JHRUJH”
- 除非對方知道F(x)=x+3這個函數，否則就沒人知道你在說甚麼了。

非對稱性密碼(公開鑰匙加密法)

- 非對稱密碼複雜很多@@”…..我們也沒有完全弄懂。但是看起來好像是：
- **信件內容→利用public key加密→密文→傳送密文→用private key解密→信件內容**
- 而private key是不能公開的私密鑰匙
- 所以人們就用大家都知道的public key加密檔案，可是要如何解開密碼要靠只有對方擁有的private key才能閱讀內容。


Data
Data
加密
解密
公開金鑰
解密
加密
私密金鑰
Data
Data

這怎麼有可能呢？嘿嘿~ 數學是無所不能的

- 簡單來講，非對稱性密碼的原理是用到了同餘的概念：
- 同餘<Modulo> 也就是相同的餘數。
  簡稱<mod>
- x=y<mod n>　n=除數
- Ex: 9=21<mod 2>
  也就是說 9 和21除以2會有相同的餘數 “1”
- 用這個概念設立public/private key就對了！*(實際上怎麼作~ 我們都看不懂了@@”)*

所以他們各有甚麼優缺點呢？

對稱性

- 優點：
  - 較快速
  - 如果使用足夠大的金鑰，將難以破解。
- 缺點：
  - 需要有一個安全性機制將金鑰安全性的分送至交易的雙方。
  - 提供私密性(Confidential)的安全性能力，無法提供不可否認的能力 (???)

非對稱性

- 優點：
  - 公開鑰匙可以公開分送
  - 提供私密性、驗證與不可否認性等服務
- 缺點：
  - 效率較差

	對稱式加密法	非對稱式加密法
其它名稱	秘密金鑰加密法	公開金鑰加密法
加解密的key是否相同	相同	不同
key可否公開	不可公開	公開鑰匙可以公開 私有鑰匙不可公開
key保管問題	如果與N個人交換訊息， 需保管好N把加解密鑰匙	無論與多少人交換訊息， 只需保管自己的私密鑰匙
加解密速度	快	慢
應用	常用於加密長度較長的資料， 例：email	常用於加密長度較短的資料， 數位簽章

第二部分：虛擬世界

我們每個人多多少少都活在這個根本不存在的世界中……

它跟現實世界有甚麼連結呢？

虛擬世界-現代人新議題

- 在虛擬世界裡的行為舉止，應該負多少實體世界的法律責任？對大部份人來說，答案也許是「零」，然而當線上社群從事真實財務交易、吸引更多參與者之際，有些法律專家認為，或許是到了將實體世界法律學延伸到虛擬王國的時候了。

- 有些研究估計，全球大約有一億人進駐線上社群。美國舊金山林登實驗室所創造的「第二人生」（Second Life）擁有100萬名活躍的玩家，他們能在個人電腦上即時體驗，以數位角色（亦即「虛擬化身」）漫步在城堡、荒島和其他奇妙的3D幻境當中，還可以透過虛擬化身與數千位線上參與者相遇、交談，甚至在沙發上擁抱，來場虛擬性愛。

- 在網路上再結一次婚，算是外遇嗎？事實是：有不少對夫妻已經因相關問題分道揚鑣了。
- 目前正在撰寫《虛擬法律》（Virtual Law）的美國路特格大學法律教授拉斯托卡（Greg Lastowka）表示，在過失離婚法庭裡，這種主張是相當合法的。但他將之當成類似「我先生一天到晚打高爾夫球，沒時間陪我」之類的抱怨，是僅次於通姦的離婚理由。

啊不就虛擬的~有必要那麼認真嗎？

- 平均每週花20小時待在虛擬世界的玩家，往往比立法者更看重虛擬事務。中國一位遊戲玩家邱誠偉在「傳奇3」（Legend of Mir 3）裡贏到一把「屠龍刀」，後來被朋友借走，在網路上以人民幣7000多元賣掉。邱誠偉報警後，卻被告知沒有法律可保障虛擬寶物的所有權，於是邱誠偉殺了那個小偷。
- 拉斯托卡說：「***如果虛擬犯罪會造成一人死亡、另一人在牢裡度過餘生，那我們最好認真看待這件事。***」

所以網路上偷東西會怎樣？

- 為了解決這些類似問題，刑法在民國九十二年六月，增訂了「***妨害電腦使用罪***」專章，
- 其中第三百五十八條規定：「*無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑*」
- 第三百五十九條規定：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑」。至此，關於線上遊戲的犯罪，總算有法可罰。

案例

- 以本案例所涉及之「公然侮辱罪」而言，網際網路是一個開放的環境，只要電腦處於連線狀態，任何人皆可連上網站，瀏覽其上的網頁內容，沒有任何時間或地點的限制。因此，顯係一種不特定人或多數人皆可共見共聞之狀態，符合刑法上公然侮辱罪「公然」的要件。
- 故只要行為人在網路上之侮辱行為，足以使受害人之名譽受損，即符合該罪之要件

- 陸建民與 程曉 君是中部某私立大學教育系三年甲班的同班同學，也是該班相戀已久有名的「班對」，過去幾年來，兩人在學校中不論是上課還是參加活動，總是出雙入對，形影不離，讓班上同學們好生羨慕。
- 陸建民同時也是該校學生社團「攝影社」的社長，平日課餘之暇，便會帶著心愛的女友，到各地名勝出遊攝影，拍下許多美麗的照片，程曉君當然便是他攝影作品中最美麗的模特兒。

- 不料，這學期的某一天，陸建民在偶然的情況下，竟然發現程曉 君背著他與在碩士班就讀的學長暗中交往，兩人因而爆發激烈的口角，雙方大吵一架後，陸建民無法容忍他的女友竟然暗中「劈腿」，因此憤而與程曉君分手。
- 與程曉君分手之後，陸建民過著生不如死的日子，每天渾渾噩噩，但卻經常看到 程曉 君與那位學長在校園中攜手漫步，甜甜蜜蜜有說有笑的樣子，讓他實在無法釋懷。一天晚上，他利用照片編輯軟體，將某色情網站上的 AV 女優全裸照片，移除頭部的面容，移花接木在過去他幫 程曉 君所拍攝的風景人像照片上，並將合成後的裸體照片，上網貼圖在著名的「有名小站」網站上的「自拍裸照」貼圖區中。

由於在該網站上註冊的會員有數萬人之多，而其「自拍裸照」貼圖區，更是許多該系男同學經常上網瀏覽的網頁，大家發現該網頁中竟然有程曉 君的自拍裸照，紛紛競相走告，全班同學更是不分男女對此議論不已， 程曉 君發現後感到非常羞辱與難堪，對於陸建民的行為非常憤怒，決定向陸建民提出法律告訴。

觸犯法條

- 為保護個人名譽之安全，禁止任何人從事公然侮辱他人名譽之行為，刑法第三百零九條第一項規定：「公然侮辱人者，處拘役或三百元以下罰金。」。

第三部分：網路駭客

常聽到這個名詞，但是，他們到底是誰？

駭客的由來？

- 在西元1970年代左右，當時網路並不發達，以美國為主要地區的電腦玩家們，常常利用電話線路互相連線通訊。但是在幅員廣大的美國，玩家之間或許相隔甚遠，為了節省鉅額的長途電話費用，所以有人發明了一種***模擬長途電話訊號的儀器***，可以「騙」過電話公司的長途撥接控制系統，這種儀器暱稱為「藍盒子」（BlueBox）。之後，***凡是使用藍盒子或是其他技術玩弄電話系統的人，開始有了「Phreak」的綽號，中文就稱之為「飛客」。***
「飛客」是「駭客」的前身，許多網路入侵、破解密碼的知識技巧，都是早期「飛客」的經驗累積。

現代駭客

- 駭客，它是英文hacker的中譯，而hacker又是由「hacking」這個意思演變而來，***hacking的意思是「利用高度技術做出不符合常理所能判斷之結果」***，因此駭客的行為，常常是有別於常人的行動邏輯，凡是從事此類行為的人，就叫做hacker。時至科技發達的今日，網路與通信系統的發達，提供了許多技術高超的專家們一展身手的機會，所以網路成為駭客聚集的樂園。

駭客……他們到底是甚麼樣的人？

- 駭客(Hacker)是一群對作業系統非常有興趣且專精的人，大部份的人是程式設計者，因此對作業系統與程式設計都相當地清楚
- **大多數的駭客不會故意毀壞他人主機中的資料**。駭客入侵電腦的目的，*只為證實防護安全上的漏洞確實存在。*且在入侵之後，會寄出一封E-mail給該網站擁有最高權限的管理者，告知管理者該漏洞的所在，並說明原因為何且教導如何解決，有時會直接給予修正檔進行修正
- 這些駭客是網站管理者的貴人，而不是個會破壞他人電腦的怪客(Cracker)。

可是駭客不一定都是好人。

- 許多駭客會***藉由網際網路***的方式進入您的主機，然後駭客可以做到很多事情，例如竊取您的個人資料、上傳下載檔案、刪除檔案、執行程式、開關CD-ROM、遠端關掉您的主機等等，
- 您可能不會受到什麼影響，但是您也可能因此而導致重大的損失。***惡意而技術高超的駭客甚至能破壞社會金融秩序，危害國家安全***，在網際網路的重要性及廣泛性日益增加之後，防止駭客的入侵勢必成為現今最受矚目的要務之一。

知己知彼-駭客是如何入侵的呢？

1. ***目標鎖定，資源搜尋***(駭客比較在意的是：組織坐落的地址，網域名稱等等)
2. ***主機掃描***(避開你的防火牆)
3. ***windows資源列舉***(對目標NT主機建立一個空連線，透過這個方式來得到目標的主機名稱，網路卡編號，群組，帳號等資訊。如果進一步的猜出你的NT系統管理員密碼，它更可以遠端連上你的主機，擁有一切的權限，這對系統的危害相當的大。)

4. 入侵系統 以下介紹幾種形式

- **密碼破解**
- **特洛伊木馬**(攻擊手法主要是騙取被害人執行特定的程式(不外乎是偷拐哄騙)來植入木馬程式，再透過clinet端的程式來竊取對方主機的資源。)
- **Sniffer(監聽器)監聽** (監聽器的出現來自於網管人員對於網路流量的管理監控需求，因此需要一套軟體來記錄LAN裡面傳遞的封包資訊，流量等紀錄。但被有心人士拿來當作竊取資訊的手法。)
- **DoS/DDoS攻擊**(駭客會使用大量的封包或是特異畸形的封包來癱瘓目標主機上的服務，結果輕則使目標主機服務停止，重則讓主機當機。)
- **Buffer Overflow(緩衝區溢位)攻擊**(這好像是最高級的攻擊手法~ 有看沒有懂~ 所以以下省略)

所以可以如何預防不肖份子？

- ***勿隨意下載***免費使用及試用軟體，或開啟不明電子郵件
- 使用MSN等即時通訊，***避免點選不明網址***
- 使用隨身碟前，將電腦的系統自動執行功能關閉
- 預防隨身碟病毒（含系統自動執行功能關閉說明）
- 電腦不使用時最好關機並***切斷網路電源***
- ***裝設防毒軟體***，定期掃毒並更新病毒碼
- 一旦被植入木馬程式，須掃毒移除
- 遇到「xxx.dll」先確定是否中毒！如何確定？使用***線上掃毒或用防毒掃掃***

資料來源

- *avp.toko.edu.tw/docs/class/3/密碼學原理與技術.pdf*
- 科學人雜誌網站 http://sa.ylib.com/news/newsshow.asp?FDocNo=1423
- 2004.06.16 Hinet 新聞網專家開講 http://old.npf.org.tw/PUBLICATION/CL/093/CL-C-093-087.htm
- **大學校園網站法律案例教材** *www.ntnu.edu.tw/dsa/newdsa/02/download/right/04/04_4.doc*
- *書名：對不起駭到你*
- *奇摩知識+*