Module 7：電子郵件安全

學習目的

1. 網際網路的發展改變了人類的生活方式與行為模式，利用電子郵件交換訊息已是多數人生活方式之一，對於企業與客戶進行溝通時，利用大量電子郵件更是不可或缺的方式。由於電子商務的發展，借由網路傳送廣告，有低成本、高效率的特質，網路廣告成為多數商家或是網路使用者的最愛。
2. 然而廣告信不外乎是販賣盜版光碟、色情光碟、直銷事業等等。這些不請自來的郵件甚至可能夾帶有病毒入侵使用者電腦，或是利用Mail client軟體本身缺陷，散播大量病毒、植入後門程式等。

3. 本模組共有四個小節包括

(1)電子郵件弱點

(2) PGP

(3) S/MIME

(4)垃圾郵件防治

(5)專案實作，共須三個鐘點。

Module 7：電子郵件安全

- Module 7-1：電子郵件弱點(*)
- Module 7-2：PGP(*)
- Module 7-3：S/MIME(**)
- Module 7-4：垃圾郵件防治(*)
- Module 7-5：專案實作(*)

* 初級(basic):基礎性教材內容
**中級(moderate):教師依據學生的吸收情況，選擇性介紹本節的內容
***高級(advanced):適用於深入研究的內容

Module 7：電子郵件安全

- 目的
  - 本課程模組將介紹廣告商如何利用各種方式收集、濫發垃圾郵件
  - 進一步將探討一些郵件安全編碼(包含PGP與S/MIME)以及郵件炸彈等相關議題。
  - 同時也提供幾個防治措施，讓學生能有效的對付垃圾郵件
  - 最後則提出建議，希望政府及ISP業者能雙管齊下，有效遏止濫發垃圾郵件的情形

Module 7-1：電子郵件弱點(*)

電子郵件弱點

- 電子郵件發展歷史
  - 電子郵件翻譯自英文的email或e-mail
  - 早在網際網路流行以前，電子郵件就已經存在了
  - 現在已經演變成為一個更加複雜並豐富得多的系統
  - 網際網路擴展了其應用的範圍
  - 使用在支援TCP/IP協定或具有SMTP和POP的網路

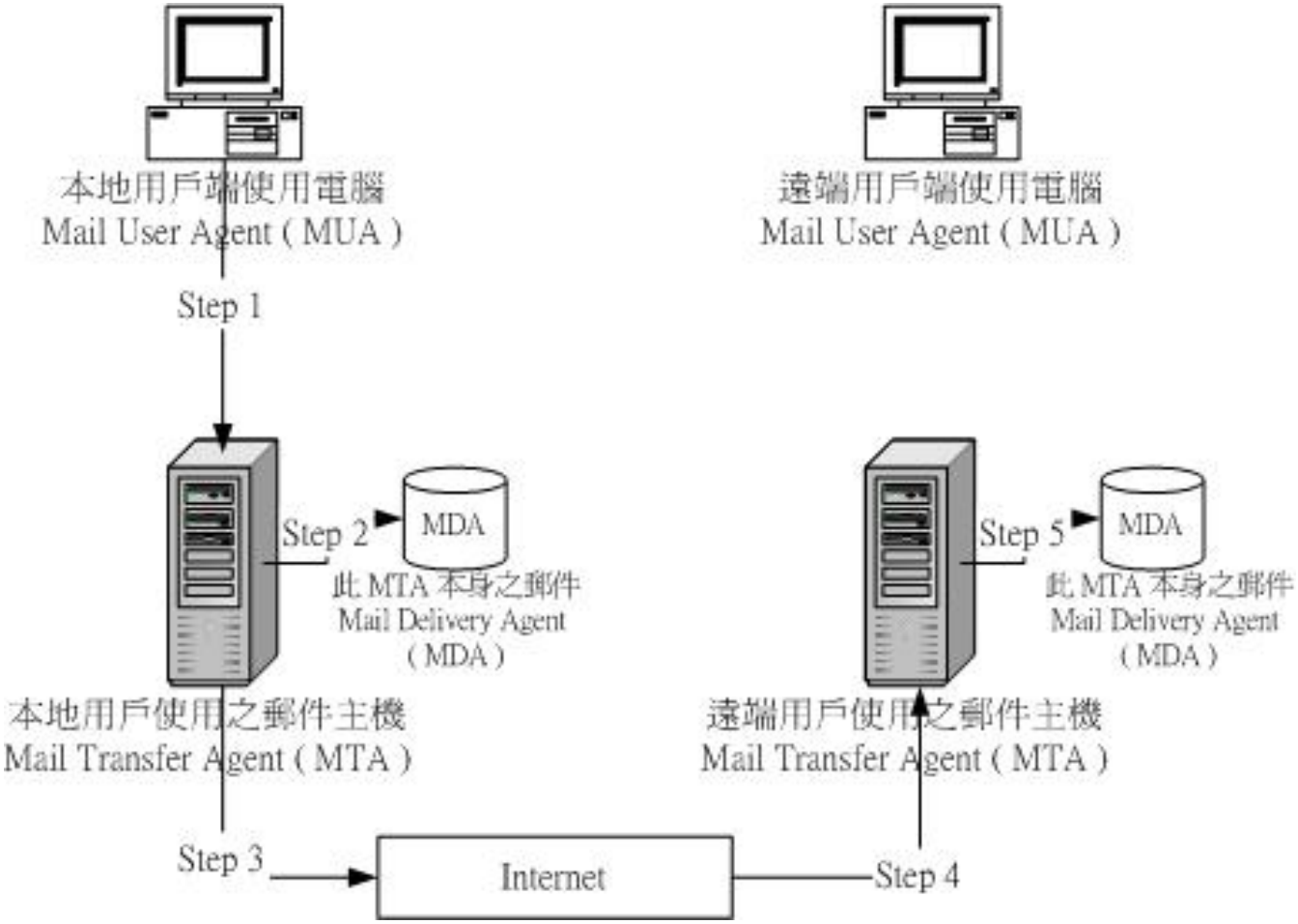
電子郵件的誕生

- 電子郵件的發明人雷.湯姆林森(Ray Tomlinson) 研製出一套新程式，改善以往傳遞資訊的缺點：
  - 可輕易透過電腦網路發送和接收資訊
  - 為了易識別的電子郵箱位址，決定採用@符號，符號前面加用戶名，後面加用戶郵箱所在的地址

電子郵件的30年發展歷程

- 電子郵件是在70年代發明的，它卻是在80年才得以興起
  - 70年代的沉寂主要是網路人口太少，網路的速度太慢
  - 80年代中期，電子郵件開始在電腦迷以及大學生中廣泛傳播開來
  - 90年代中期，全球上網人數激增，電子郵件被廣為使用

電子郵件的傳送



電子郵件以郵件主機寄送信件示意圖

電子郵件的傳送（續）

- MUA (Mail User Agent)：MUA 就是『郵件使用者代理人』
  - 例子：Windows 裡面的 OutLook Express，Netscape 裡面的 mail 功能與 KDE 裡面的 Kmail 都是 MUA

電子郵件的傳送（續）

- MTA (Mail Transfer Agent)： MTA 就是郵件伺服器，『郵件傳送代理人』的意思。主要功能有：
  - 收受外部主機寄來的信件
  - 幫使用者傳送 (寄出) 信件
  - 讓使用者自己的信可以收回去

電子郵件的傳送（續）

- MDA (Mail Delivery Agent)
  - 將 MTA 所收受的信件，依照信件的流向 (送到哪裡去) 來將該信件放置到本機帳戶下的郵件檔案中 (Mailbox) !
  - 如果信件的流向是到本機當中時，這個郵件代理人的功能還具有郵件分析 (filtering) 與其他相關的功能。

電子郵件的傳送（續）

- Mailbox
  - 『郵件信箱』就是在主機上面的一個目錄下某個人『專用』的信件收受檔案。
  - 以 UNIX 來說，系統管理員 root ，有個信箱在 /var/spool/mail/root 。
  - 當 MTA 收到 root 的信時，就會將該封信件存到 /var/spool/mail/root 這個檔案中。

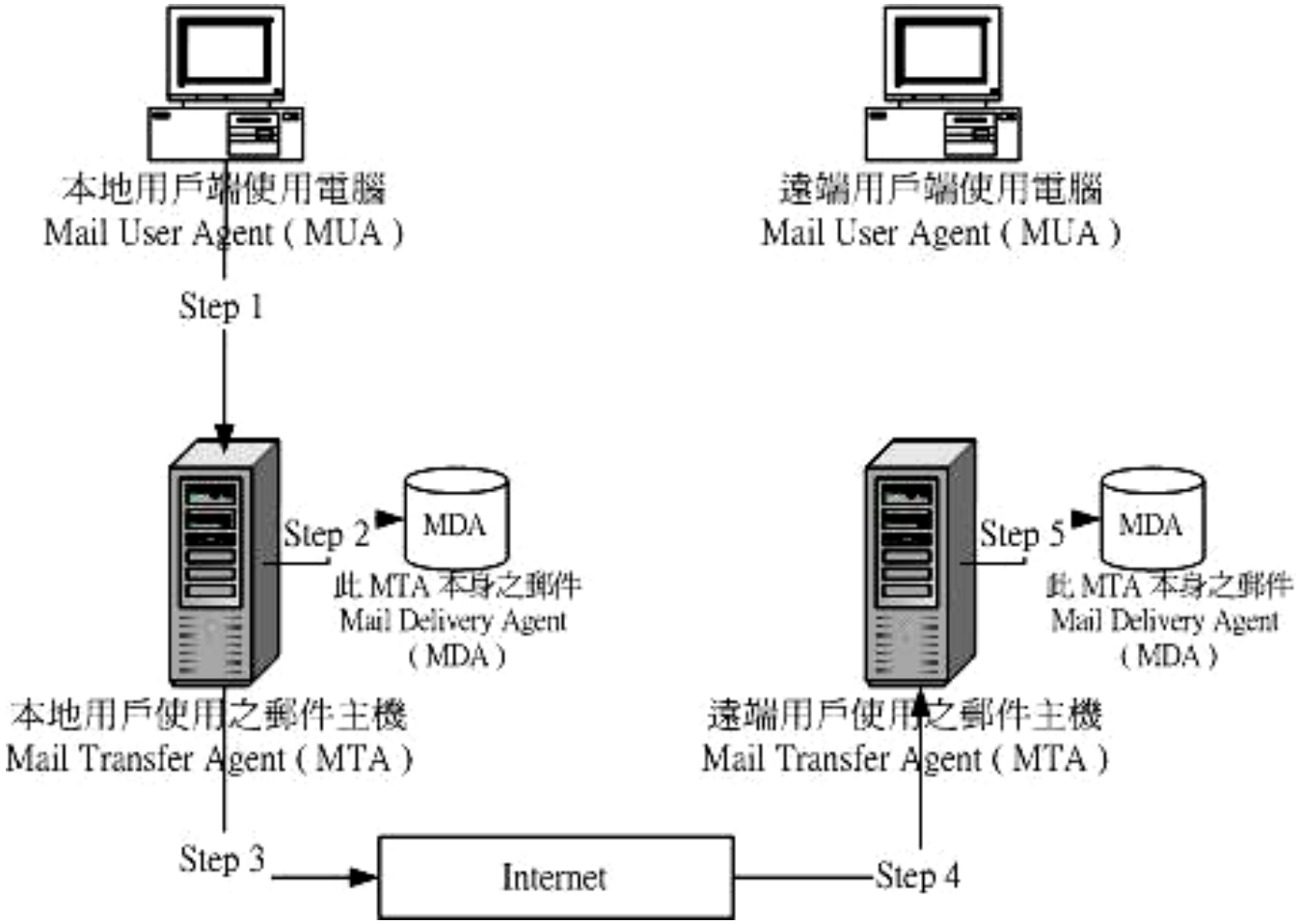
使用的協定-SMTP

- 郵件主機使用 SMTP (Simple Mail Transfer Protocol) 這個協定，port number 為 25 。
- 寄信時，MUA 主動連接 smtp 協定 (port 25) 而送出去。
- 郵件主機 MTA 在轉遞的時，也是經下一部 MTA 的 smtp 協定 (port 25)來將信送出去。

使用的協定-POP3

- 收信是 MUA 經由 POP (Post Office Protocol) 協定來連接 MTA 的使用者 Mailbox
- 目前常用的 POP 協定為 POP3 (Post Office Protocol version 3 ，port number 為 110)
- MUA 經由 MTA 的 port 110 將信件由 MTA 的 mailbox 收到本地端的 MUA 上

如何將信寄出去

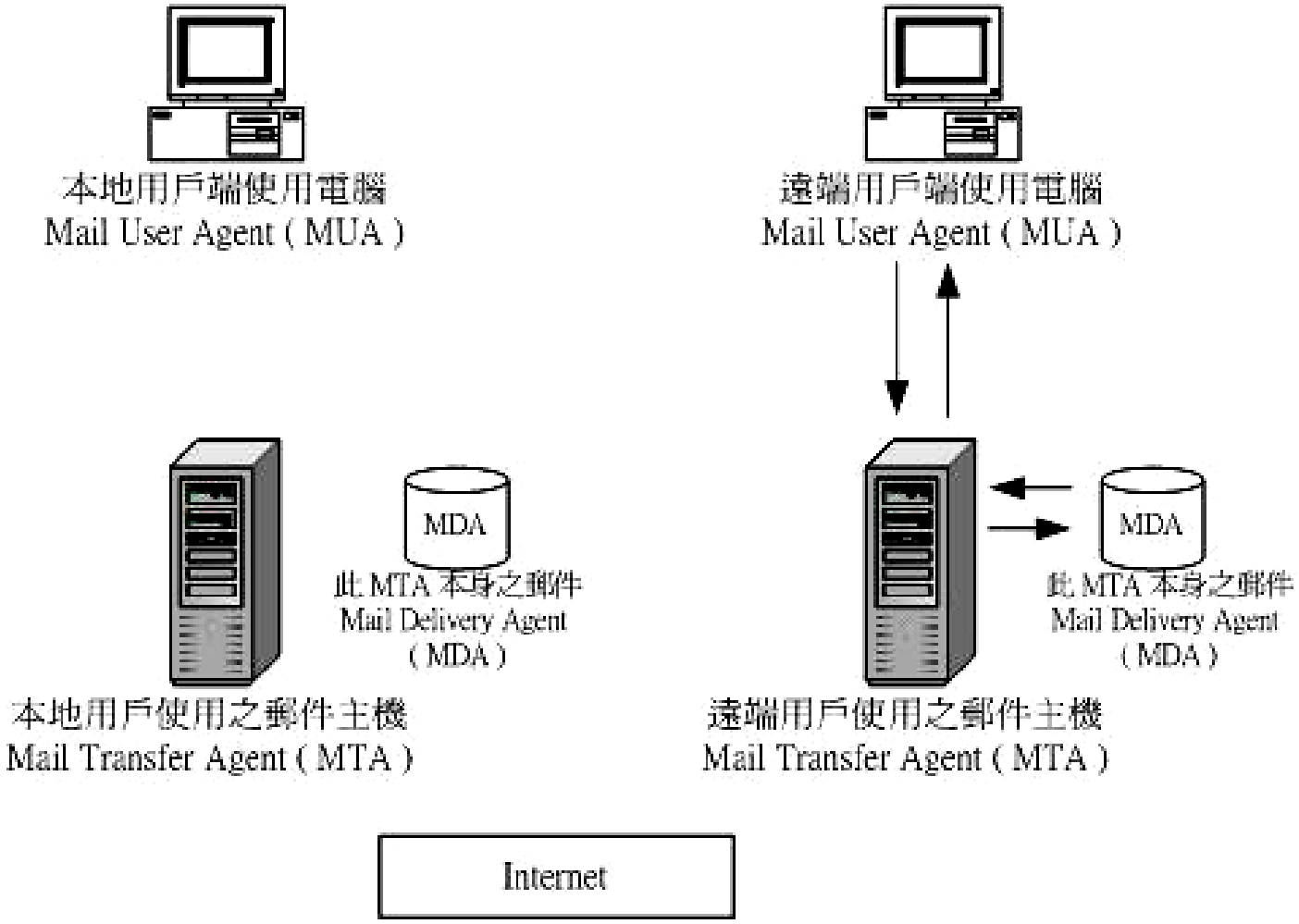


電子郵件以郵件主機寄送信件示意圖

如何將信寄出去

- Step 1： 使用者利用 MUA 寄信到 MTA 上
- Step 2：MTA 收到自己的信件，交由 MDA 發送到該帳號的 MailBox
- Step 3 ：MTA 將信再轉送出去
- Step 4 ：遠端 MTA 收受本地的 MTA 所發出的郵件
- Step 5 ：信件會存放在遠端的 MTA 上面

收信的動作



用戶端收受郵件主機的電子郵件示意圖

收信的動作（續）

- 遠端用戶使用的電腦直接連接到MTA。
- MTA 透過 MDA 檢查信件。
- 同時，根據 MUA 的不同設定， MTA 會選擇將該 mailbox 清除掉，或者繼續保留。

垃圾郵件的來源

- 在網際網路開始時就有垃圾郵件。
- 垃圾郵件也被稱作是“未經收信人許可的商業郵件”(UCT)或“未經收信人許可的大量郵件”(UBE)。

電子郵件的安全

- 你知道你的電子郵件只比你從牙買加郵寄的風景明信片稍微安全一點嗎？
- 即使確信並非人人能輕易攔截並且讀你的電子郵件時，這個危險仍然存在的
- 你或許透過網際網路傳送許多祕密和合法敏感檔案，其中的危險會立即使你感到害怕

電子郵件的安全

- 電子郵件的弱點
  - BEWARE THE SNIFFER（注意監聽者）
  - KEYS TO THE CODE（關鍵）

電子郵件的安全

- BEWARE THE SNIFFER（注意監聽者）
  - 電子郵件最常被侵害的是電子竊聽（electronic eavesdropping），或者是被稱為網路監聽（sniffing）
  - 不要認為你的密碼非常的長而且有非常複雜的保護
  - 那和電子郵件的傳送和儲存模式是有關的
  - 當郵件檔案從你的組織的磁碟或者ISP 的電腦中被搬移到獨立的磁碟保存

電子郵件的安全

- KEYS TO THE CODE（關鍵）
  - 防止電子郵件未被授權的讀取最常用的方法是使用軟體加密
  - 任何沒有解碼器（decoder）或者鑰匙（key）的人無法讀取它
  - 今日的電腦是非常快速，它可以在幾乎沒有被察覺的狀況下作出編碼的動作

電子郵件的安全（續）

- KEYS TO THE CODE（關鍵）
  - 有兩個主要的商業加密標準：PGP 和S/MIME
  - PGP是最廣泛接受的工具
  - 讀取PGP 加密的訊息，需要兩把鑰匙
    - 私鑰
    - 公鑰

Module 7-2：PGP(*)

如何利用PGP 安全傳送的例證

- 只能讓瑪莉看到訊息
  - 鮑伯要用瑪莉的公鑰加密
- 身份真實性的問題
  - 鮑伯則用他的私鑰加密
  - 瑪莉用鮑伯的公鑰打開電子郵件
- 機密性和真實性
  - 使用“double lock”：鮑伯使用他的私鑰和瑪莉的公鑰加密他的訊息
- PGP 可提供給非商業性用戶免費使用 http://www.pgpi.org 可下載和得到更多的訊息

PGP的優勢/缺點

- PGP的優勢：
  - 使用者接受率在S/MIME之上
  - 幾乎沒有相容性的問題
  - 可以被外掛進最受歡迎的電子郵件軟體
- PGP的缺點：
  - 沒有任何方法可以確認PGP鑰匙不會被冒用
  - 使用數位認證來確認使用者的身份將提高成本

我為什麼要撰寫 PGP

- PGP 之父—菲爾・齊麥曼 (Phil Zimmermann) —「我為什麼要撰寫 PGP (Why I Wrote PGP) 」
  - 保護隱私乃是天經地義的事，就和憲法一樣的重要
  - 為什麼不通通只用明信片寄所有的信件呢？
  - 如果政府想要侵犯非數位化的隱私，得花去大量的金錢和代價來擷取
  - 越來越多的私人通訊是透過數位途徑傳遞
  - 1991 年參議院第 266 號法案

我為什麼要撰寫 PGP（續）

- 在 94 年版的法案中，最大的警訊是：白宮的新加密政策方案。
  - 它的核心是一個由政府製造的加密裝置，稱為 Clipper 晶片
  - 平凡老百姓和基層單位沒有辦法取得軍事等級公鑰密碼科技

我為什麼要撰寫 PGP（續）

- PGP 讓人們能夠掌握自己的隱私權
- PGP 能夠提供獨立電腦上的資訊保護功能：
  - 資料加密
  - 虛擬的私人網路系統

我為什麼要撰寫 PGP（續）

- PGP可以做這些事
  - 在任何軟體中進行加密/簽署以及解密/驗證
  - 打造以及管理金鑰
  - 建立自動解密壓縮檔 (self-decrypting archives, SDAs)
  - 永久的銷毀檔案、資料夾，並釋放出磁碟空間
  - 保密網路傳輸

PGP密碼法導論

- 密碼法基礎
  - 凱撒大帝傳送信息給他的將軍時
  - 信息中每一個字母 A 通通換成了字母 D
  - 每一個字母 B 都換成字母 E
  - 所有的字母都如此類推。
  - 只有知道這個「上移三」規則的人，才能夠看懂他的信息。

加密和解密

- 利用某種方法隱藏起來則稱為加密
- 變成一堆無法讀取的亂碼，稱為密文
- 只要不是訊息真正的接收者，就無法取得隱藏在其後的資訊
- 把密文轉換回原來純文字的過程稱做解密

甚麼是密碼學？

- 密碼術囊括了密碼法和密碼分析
  - 密碼法是利用數學方法來對資料加密和解密的科學
  - 密碼分析則是分析和破壞保密通訊的科學

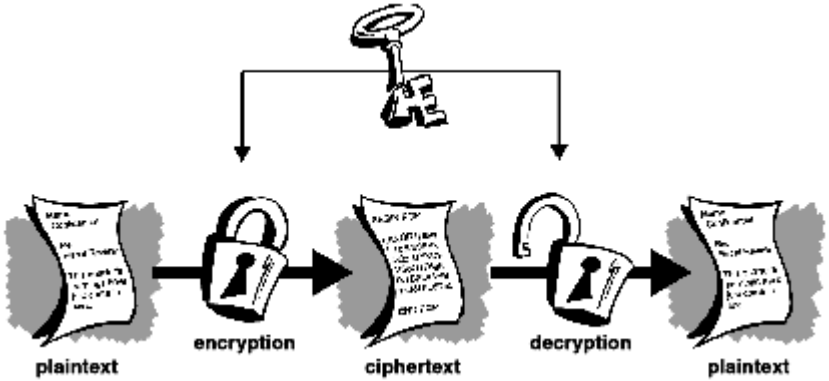
強密碼法

- 密碼法的強度端看將其還原回純文字訊息所會耗去的時間和資源而定
- 強密碼法所產生的密文若沒有適當的解碼工具來處理，將會非常難破解

密碼法如何運作？

- 密碼演算法，或稱為密碼本，是用來處理加密和解密的數學函式
- 一個密碼演算法必須和一副金鑰 — 一個文字、數字、或詞組 — 一起將純文字加密
- PGP 就是一個密碼系統
  - 密碼演算法，加上金鑰及協定，構成一個密碼系統

傳統密碼法



- 傳統密碼法又稱為密鑰加密法或對稱式金鑰加密法
- 在這種密碼法當中，用來加密和解密的是同一把金鑰
- 資料加密標準法 (Data Encryption Standard, DES) 就是一種被聯邦政府廣泛使用的傳統密碼系統

凱撒的密碼本

- 一個傳統密碼法的簡單例子是取代法密碼本。也就是透過取代法密碼本把一部份的資訊取代成另一些
- 在凱撒大帝密碼本的例子裡，密碼演算法就是「字母偏移」，而金鑰則是「字母偏移的距離」

凱撒的密碼本（續）

- 「SECRET」用凱撒的方法加密，金鑰的數值是 3 的話
  - 原先的字母系統應該是 ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - 每個字母都挪動 3 個位置後，得到 DEFGHIJKLMNOPQRSTUVWXYZABC
  - 也就是 D ＝ A 、 E ＝ B 、 F ＝ C ，依此類推
- 原先的純文字「SECRET」被加密成「VHFUHW」。要讓別人能夠解讀密文，需要告訴他們所用的金鑰數值是 3 。

金鑰管理和傳統加密

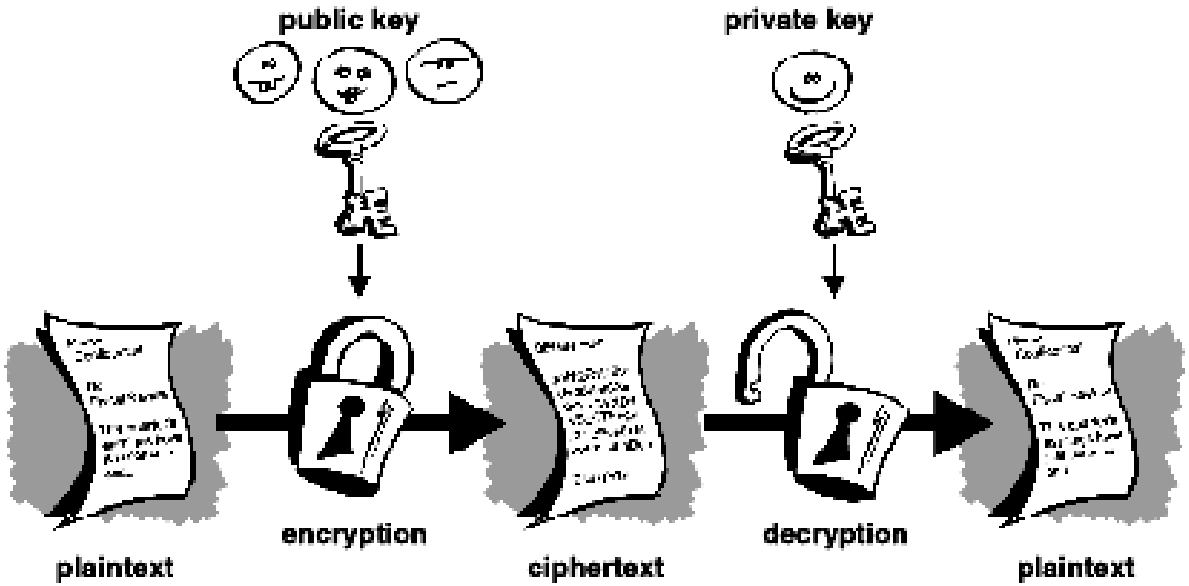
- 傳統加密有個好處：它非常的快
- 傳統加密要保密地傳遞金鑰太過困難了
- 保密溝通的遞送者和收件者必須事先對金鑰取得共識
- 如果他們身處不同的地理位置，那更必須重視任何保密溝通媒介的安全，以避免秘密金鑰被公開

公開金鑰密碼法

- 金鑰傳遞的問題被公開金鑰密碼法解決
- 公開金鑰密碼法是一種非對稱性的結構，它使用了一對金鑰來進行加密
- 公鑰可發表到世界各處，同時保密你的私鑰
- 任何取得你的公鑰複製的人都可以加密出只有你才能閱讀的資訊

公開金鑰密碼法（續）

- 在運算上要從公鑰追溯出私鑰是不可能的



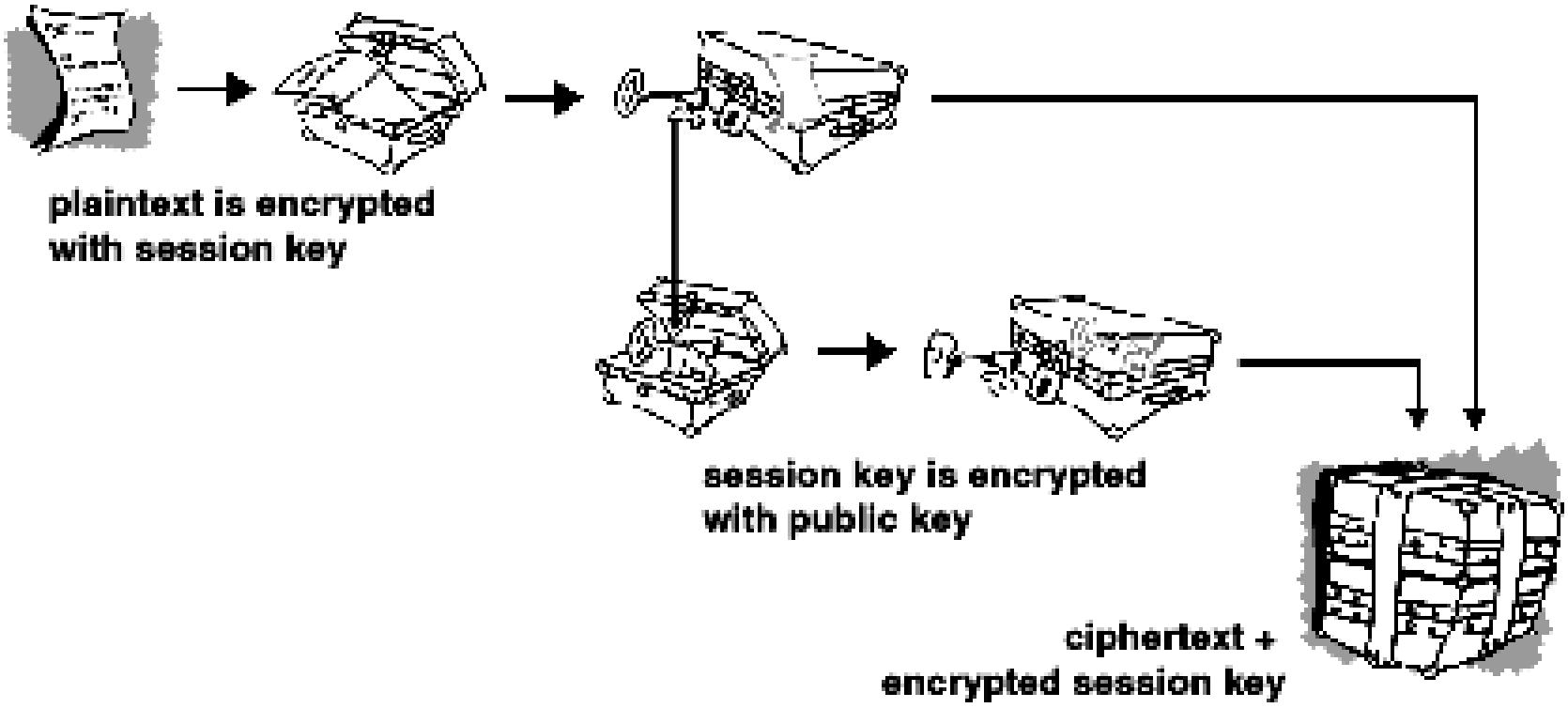
公開金鑰密碼法（續）

- 公開金鑰加密法最主要的優點是它允許沒有事先安排保密管道人們仍然可以保密地交換訊息
- 公開金鑰密碼系統
  - Elgamal，以它的發明者 Taher Elgamal 的名字所命名
  - RSA ，以它的發明者 Ron Rivest 、 Adi Shamir 、 Leonard Adleman 的名字所命名
  - Diffie-Hellman（以它的發明者的名字所命名）
  - 還有 DSA，也就是數位簽章演算法，由 David Kravitz 所發明

PGP 如何運作

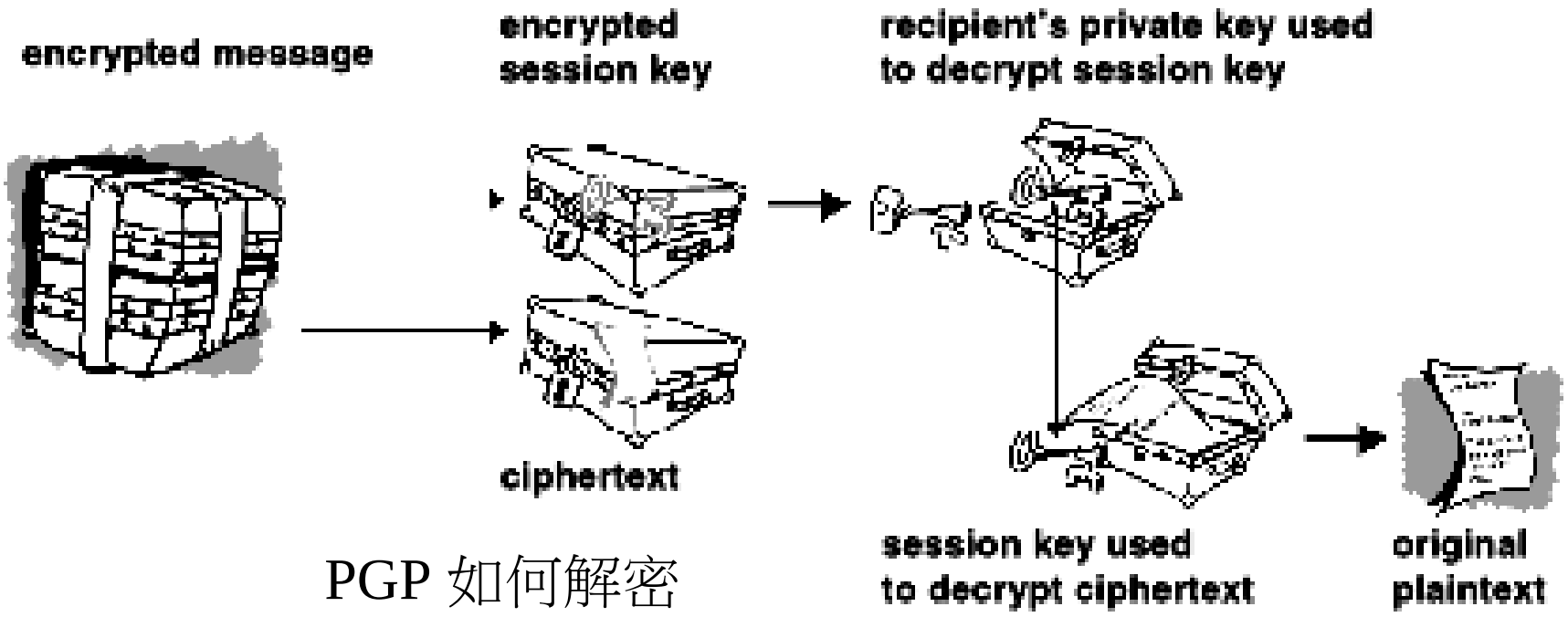
- PGP 結合傳統密碼法和公開金鑰密碼法的特色
  - 當使用者使用 PGP 來對純文字加密的時候， PGP 首先會壓縮這段純文字
  - 然後產生一個階段金鑰
  - 以非常秘密而快速的傳統加密演算法來加密純文字，而產生出密文
  - 當資料加密完成後，這把階段金鑰接著就會開始以收信者的公鑰被加密
  - 這個被公鑰加密過的階段金鑰將會與密文一併交付給收信者

PGP 如何運作（續）



PGP 如何加密

PGP 如何運作（續）



PGP 如何解密

解密的過程就是反向運作了。
收信者的 PGP 會利用他的私鑰來還原那把暫時的階段金鑰，
然後 PGP 再利用這把階段金鑰來將傳統加密過的密文解密。

PGP 如何運作（續）

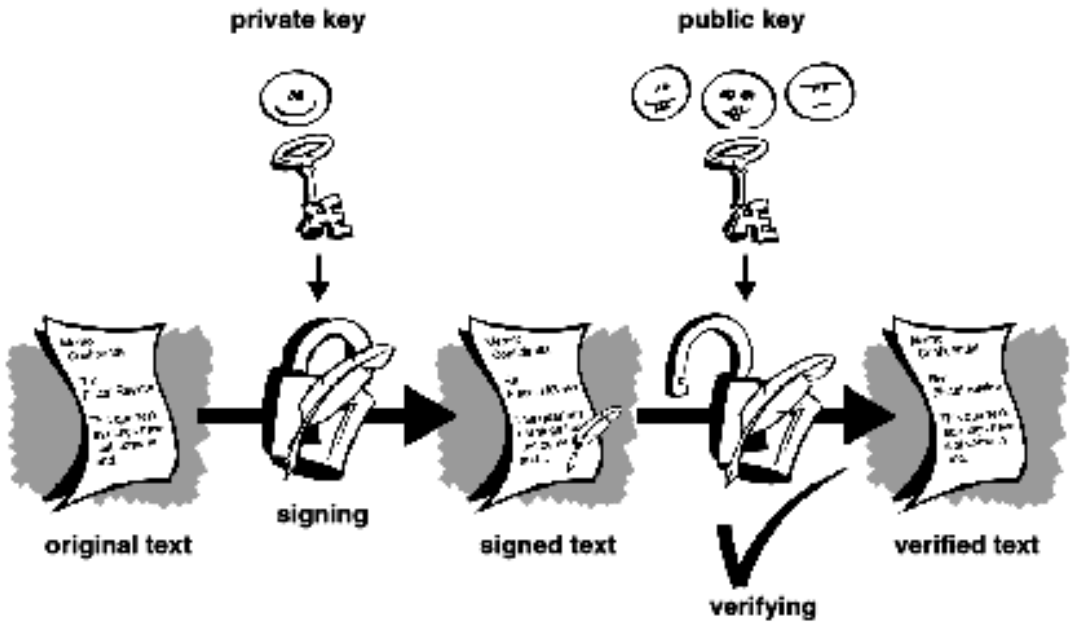
- PGP結合匯聚公開金鑰加密法的便利和傳統加密法的迅速兩種加密方法。
  - 傳統加密法大約比公鑰加密法要快上 1,000 倍
  - 公鑰加密法則解決了金鑰傳遞和資料傳輸的課題
  - 雙管齊下，效率和金鑰傳遞兩者同時改善了，而且不會有任何安全上的犧牲。

金鑰

- 金鑰是用來和密碼演算法產生特定密文的數值。
- 金鑰的大小可以用位元組來計算
- 金鑰會以加密過的形式儲存下來
  - PGP 將金鑰儲存在硬碟上的兩個檔案裡：一個用來儲存公鑰，另一個儲存私鑰。這些檔案被稱作金鑰鑰匙圈。

數位簽章

- 公開金鑰密碼法的一個主要好處是它提供了一種數位簽章的方法。
  - 不可否認性的證明和資料完整性

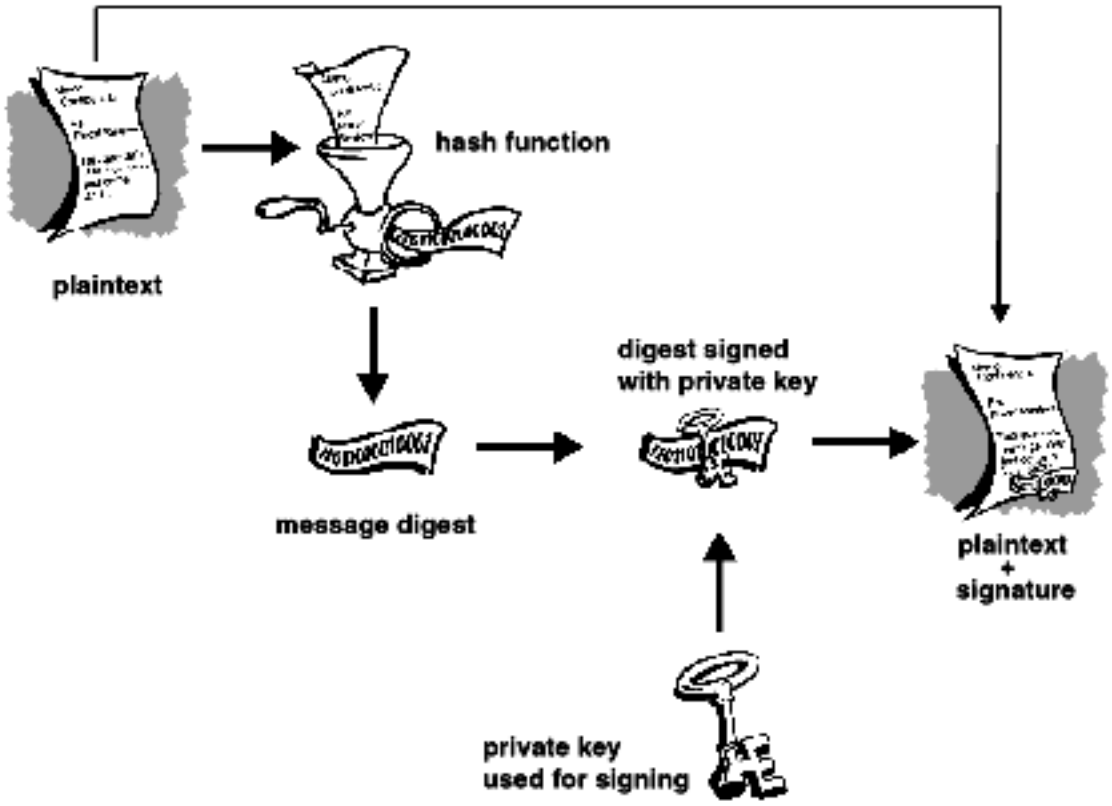


簡單的數位簽章

雜湊函式

- PGP 對使用者簽署的純文字使用密碼法上的雜湊函式
- PGP 使用摘要和私鑰以產生「簽章」
  - PGP 把簽章和純文字一起傳遞。當收件者收到訊息後，利用 PGP 重新計算摘要並驗證簽章
  - 任何在簽署過的文件上所動的細小手腳，都會導致數位簽章驗證的結果失敗

雜湊函式（續）

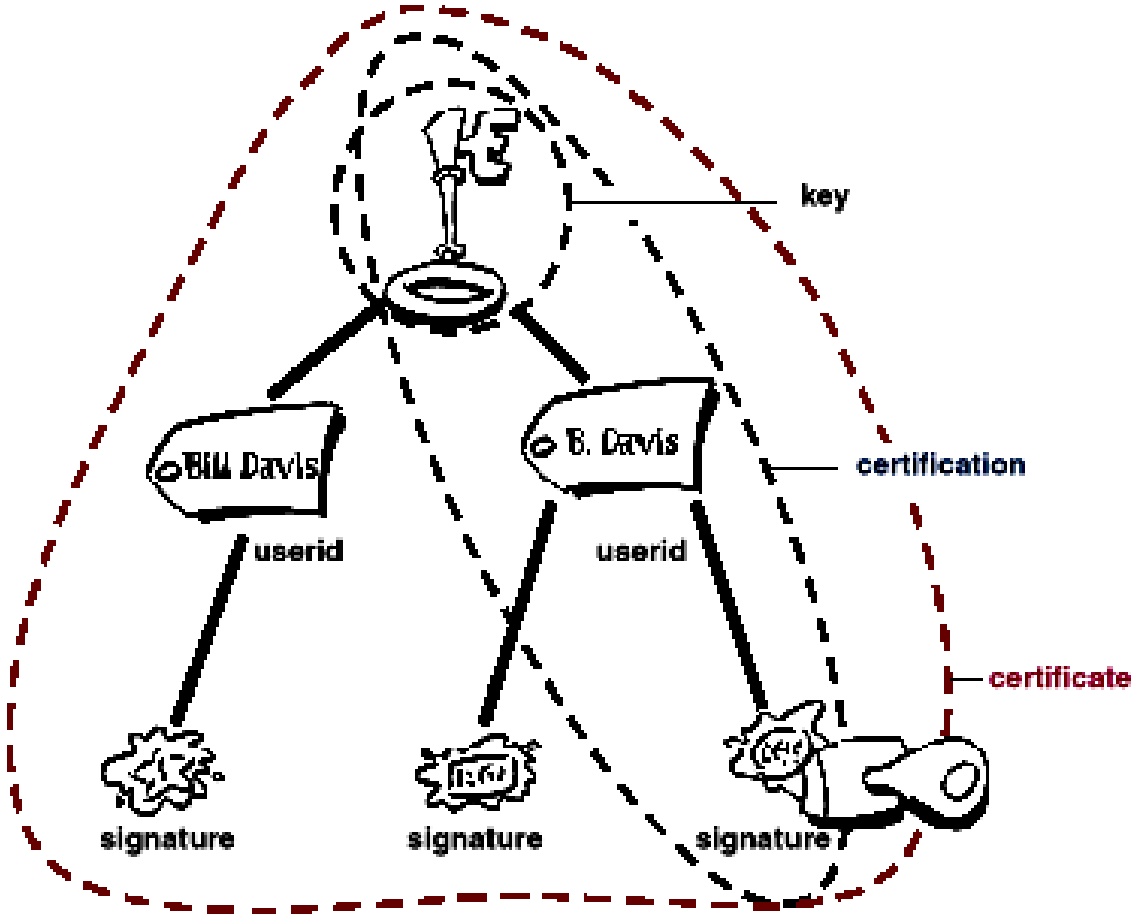


保密數位簽章

數位憑證

- 數位憑證，或稱憑證，確認某把公鑰是不是真的屬於某個人的工作。
- 一個數位憑證由三件事情組成
  - 一把公鑰
  - 憑證資訊。（使用者的「身份」資訊，像是名字、使用者 ID 之類的。）
  - 一個以上的數位簽章

數位憑證



PGP 憑證解剖圖

憑證散佈

- 憑證用於有需要和他人交換公鑰的時候
- 要散佈憑證必須要架設起一套能夠提供足夠的安全、儲存、交換機制的系統
- 透過提供儲存功能的憑證伺服器，或者提供更多額外金鑰管理功能的公鑰基礎建設 (Public Key Infrastructures，PKIs)

憑證伺服器

- 也被稱金鑰伺服器，是一個允許使用者提交和收回數位憑證的資料庫
- 憑證伺服器通常會提供一些管理功能讓公司行號能夠維護它們的保密政策 — 例如只允許合規定的金鑰被儲存

公鑰基礎建設

- PKI 包含了憑證伺服器所具備的儲存能力，另外又提供了憑證管理能力（發行、撤銷、儲存、收回、以及信任憑證的能力）
- PKI 的主要特色被稱之為憑證中心(Certification Authority，CA) 是由一個人類實體 — 一個個人、團體、部門、公司、或任何協會 — 認可了並發行它們所有電腦使用者的憑證

憑證格式

- 數位憑證基本上是把辨識資訊和公鑰以及由信任的第三者用以證明其授權的簽署打包蒐集起來。它可以有許多不同的格式
- PGP 能夠理解兩種不同的憑證格式：
  - PGP 憑證
  - X.509 憑證

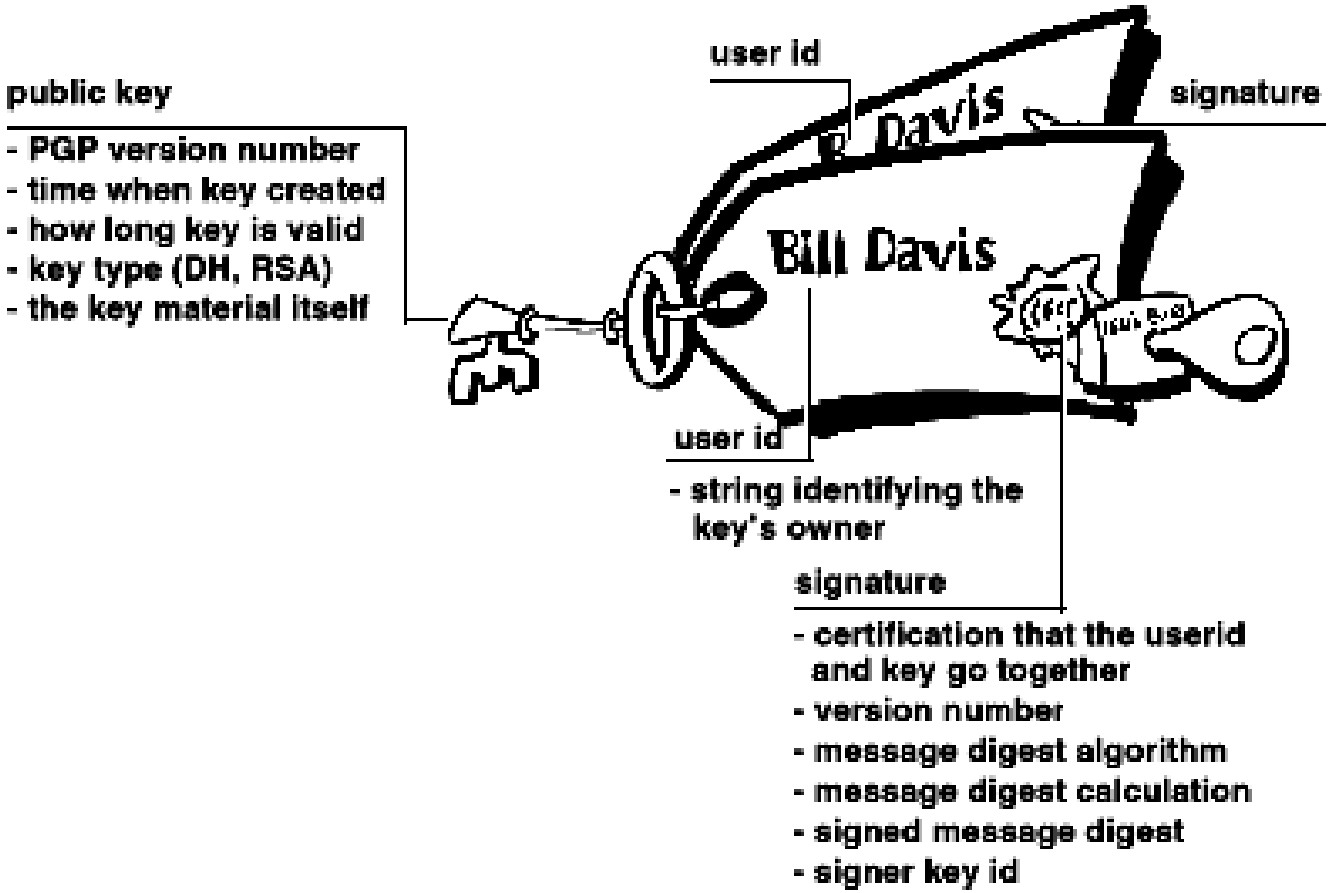
憑證格式（續）

- 一份 PGP 憑證包括（但不限於）下列的資訊：
  - PGP 版本號碼
  - 憑證持有者的公鑰
  - 憑證持有者的資訊
  - 憑證持有者的數位簽章
  - 憑證有效期限
  - 這把金鑰偏好的非對稱性加密演算法

憑證格式（續）

- PGP 憑證可以想成是一把貼上一大堆標籤的公鑰
- 在這些「標籤」上可以找到足以辨識金鑰持有者的資訊，以及金鑰持有者的簽署，用以聲明這些資訊和金鑰是一併送出的

憑證格式（續）


user id
public key
- PGP version number
- time when key created
- how long key is valid
- key type (DH, RSA)
- the key material itself
signature
Bill Davis
user id
- string identifying the key's owner
signature
- certification that the userid and key go together
- version number
- message digest algorithm
- message digest calculation
- signed message digest
- signer key id

PGP 憑證

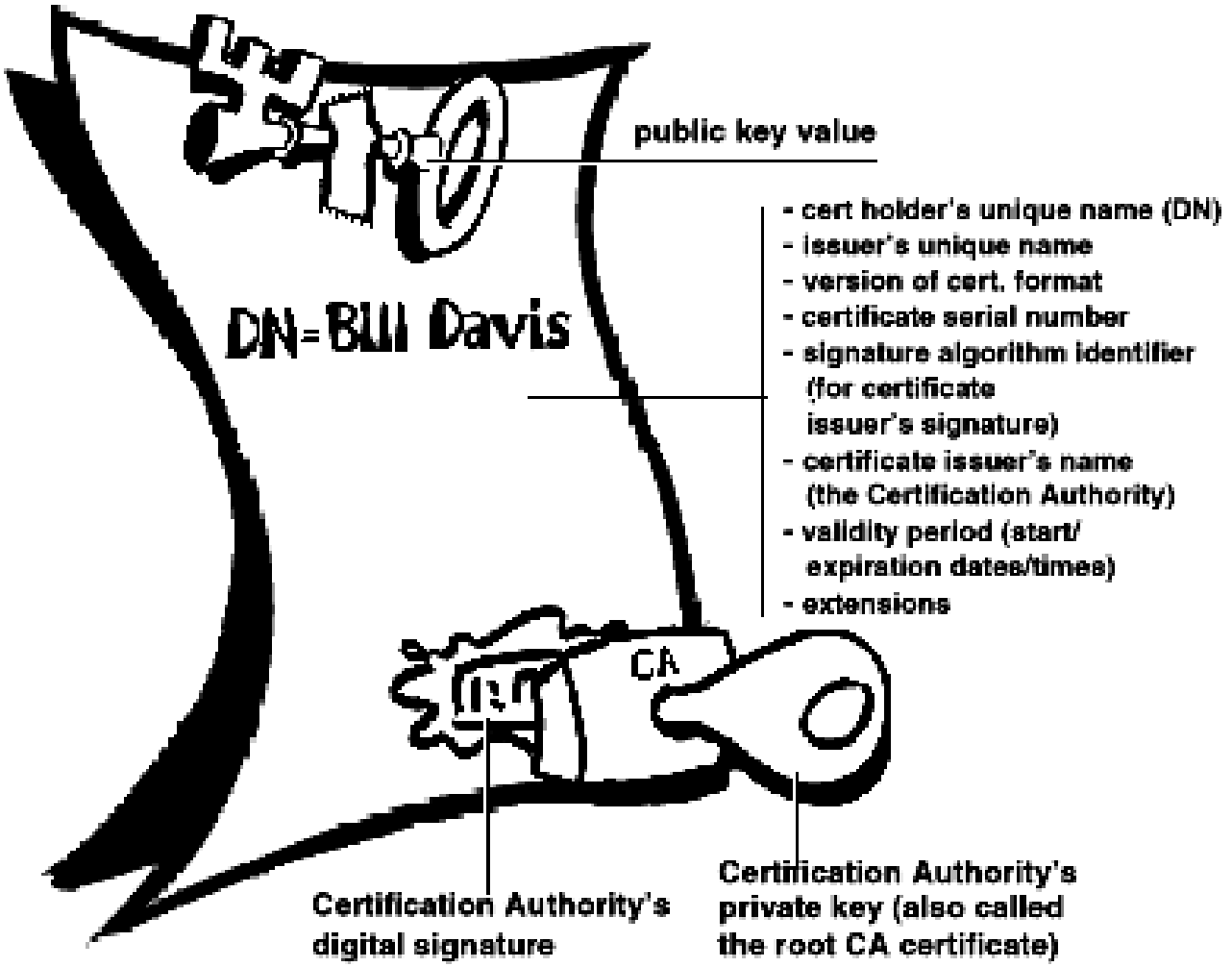
憑證格式（續）

- X.509 憑證包括了使用者或設備資訊的標準格式範疇和相對應的公鑰
  - X.509 版本號碼
  - 憑證持有者的公鑰
  - 憑證的序號 — 建立憑證的實體（程式或個人）需要提供一個獨一無二的序號
  - 憑證持有者獨一無二的鑑定碼
  - 憑證的有效期限
  - 憑證發行者獨一無二的名字
  - 發行者的數位簽章
  - 簽章演算法鑑定碼

憑證格式（續）

- 在 X.509 憑證和 PGP 憑證間有許多差異，其中較顯著的列出如下：
  - 你可以建立你自己的 PGP 憑證；但是 X.509 憑證卻只能經過申請的手續，由憑證中心發行
  - X.509 憑證自然地只能接受金鑰持有者使用單一名字
  - X.509 憑證只能接受單一一個數位簽章來證明金鑰的有效性

憑證格式（續）


public key value
- cert holder's unique name (DN)
- issuer's unique name
- version of cert. format
- certificate serial number
- signature algorithm identifier (for certificate issuer's signature)
- certificate issuer's name (the Certification Authority)
- validity period (start/ expiration dates/times)
- extensions
DN=Bill Davis
CA
Certification Authority's digital signature
Certification Authority's private key (also called the root CA certificate)

Module 7-3：S/MIME(**)

S/MIME的簡介

- S/MIME是美國RSA公司所提出的Secure E-Mail標準
- RSA公司有提供S/MAIL的library來support，其重要成分有：
  - Messaging Encryption Servises
  - Key and Certificate Databases
  - User Interface Manager
  - Certificate Handling Servises

S/MIME的簡介（續）

- S/MIME在網際網路上
  - 被包含在Netscape Navigator 和 Microsoft Internet Explorer 的瀏覽器套件內
  - 也能夠外掛進大部份的電子郵件套件內

例外因素

- S/MIME很容易設定和使用—但有兩個主要的例外因素
  - S/MIME的鑰匙使用shorter code，駭客更容易破解它
  - S/MIME不倚賴公鑰；相反的它使用第三方數位認證。共包含了用戶的名字、電子郵件位址和公鑰

購買數位認證

- 最主要兩種認證 VeriSign（digitalid.verisign.com）及HiTRUST網際威信股份有限公司（http://www.hitrust.com.tw）
- 有一些關於VeriSign的細節：
  - 等級1的數位認證要花費9.95 美元。VeriSign也為非商業性的用戶提供一次免費6個月使用
  - 等級2的數位認證要花費19.95 美元
  - 等級3的數位認證要花費大約300 美元到1000 美元
  - 相關認證清單，可到www.pki-page.org查詢

不利條件

- 不利條件
  - 便宜的認證提供使用人的身分保證太少。這表示只有高費用的等級才能得到最佳的認證
  - 電子郵件發信人和收件人雙方必須要有數位認證
  - 不同於PGP 產生的公鑰，數位認證會過期，因此使用人必須不斷的更新和額外的付費。（PGP也能使用數位認證；然而，這不是必備的）

S/MIME如何工作的實例

- 送件人—鮑伯—使用私鑰加密給瑪莉的訊息
  - 他使用數位認證”簽章”。如果有機密性的需求，這個訊息也會包含瑪莉的數位認證
  - 當收到時，瑪莉比對包含在訊息中的數位認證和自己的數位認證檔案
  - 如果鮑伯送的訊息內包括他和瑪莉的數位認證，可以保證這個訊息的機密性和真實性是沒有問題的

功能性

- S/MIME(安全/多用途網際郵件擴充協定)訂定一個安全收發MIME資料的標準
- S/MIME提供
  - 收發電子郵件時加密、解密的安全服務
  - 用於任何傳輸MIME資料的環境，如HTTP
  - S/MIME用於自動資訊傳輸代理

S/MIME V3和OpenPGP的比較

- OpenPGP 規範
  - 『非常好的隱密』(Pretty Good Privacy, PGP) 由 Phil Zimmermann 教授獨立發展
  - RFC 1991, PGP Message Exchange Formats
  - RFC 2015, MIME Security with Pretty Good Privacy
  - RFC 2440, OpenPGP Message Format
  - RFC 3156, MIME Security with Pretty Good Privacy
- S/MIME 規範
  - Secure/MIME 由 RSA Data Security Inc. 發行
  - RFC 2311, S/MIME Version 2 Message Specification
  - RFC 2312, S/MIME Version 2 Certification Handling
  - RFC 2313, PKCS #1: RSA Encryption Version 1.5
  - RFC 2314, PKCS #10: Certification Request Syntax Version 1.5
  - RFC 2315, PKCS #7: Cryptographic Message Syntax Version 1.5
  - RFC 2268, Description of the RC2 Encryption Algorithm

S/MIME V3和OpenPGP的比較（續）

制定規範	S/MIME v3	OpenPGP
訊息格式		Binary, based on PGP
憑證格式	Binary, based on X.509v3	Binary, based on PGP
秘密鑰匙系統	Triple DES	Triple DES
簽章演算法		ELGamal DSS
雜湊演算法		SHA-1
MIME 簽署封裝	multipart/signed 或 CMS	multipart/signed
MIME 加密封裝	application/pkcs7-mime	multipart/encrypted

MIME 郵件標準 (一)

- RFC 822 封裝格式
  - 標頭 (Header)
  - 主體 (Body)

From: 志明 <bob@cc.cma.edu.tw>

To:春嬌 <alice@pchome.com.tw>

Subject: See you tomorrow

Date: Fri. 26 Dec 2003 10:12:37 – 0400

Please come to meet me at tomorrow.

<LF>&<CR>

MIME 郵件標準 (二)

- MIME 封裝格式
- MIME 標頭列
  - MIME-Version
  - Content-Type
  - Content-Transfer-Encoding
  - Content-ID
  - Content-Description
- MIME 內文型態
  - Text
  - Multipart
    - Multipart/Mixed
    - Multipart/Parallel
    - Multipart/Alternative
    - Multipart/Digest
  - Message
    - Message/rfc822
    - Message/partial
    - Message/external-body
    - Application/Octet-stream
  - Image
    - Image/Jpeg
    - Image/Gif
  - Audio
  - Video
  - Application
    - Application/Octet-stream
  - Application/PostScript
- MIME 內容轉換編碼
  - 7 bit
  - 8 bit
  - binary
  - quoted-printable
  - base64
  - x-token

MIME 郵件標準 (三)

- 範例：Multipart/mixed

```
From: Nathaniel Borenstein
To: Ned Freed
Date: Sun, 21 Mar 1993 23:56:48 -0800 (PST)
Subject: Sample message
MIME-Version: 1.0
Content-type: multipart/mixed; boundary="simple boundary“
     This is the preamble.  It is to be ignored, though it
    is a handy place for composition agents to include an
     explanatory note to non-MIME conformant readers.
--simple boundary
     This is implicitly typed plain US-ASCII text.
    It does NOT end with a linebreak.
--simple boundary
Content-type: text/plain; charset=us-ascii
     This is explicitly typed plain US-ASCII text.
     It DOES end with a linebreak.
--simple boundary—
     This is the epilogue.  It is also to be ignored.
```

S/MIME 安全郵件 (一)

- S/MIME 安全郵件 (Secure/Multipurpose Internet Mail Extension)
  - 訊息摘要：SHA-1, MD5
  - 數位簽章：RSA 演算法
  - 訊息加密：RC2/40 或 Triple DES 密碼系統
  - 會議鑰匙加密： ElGamal 演算法

- 安全郵件型態 (1)
  - Multipart/Signed 型態
    - **MIME 型態名稱：Multipart/Signed**
    - **參數：boundary, protocol, micalog**

```
Content-Type: multipart/signed; protocol="TYPE/STYPE";
        micalg="MICALG"; boundary="Signed Boundary“
--Signed Boundary
Content-Type: text/plain; charset="us-ascii“
   This is some text to be signed although it could be
   any type of data, labeled accordingly, of course.
--Signed Boundary
Content-Type: TYPE/STYPE
  CONTROL INFORMATION for protocol "TYPE/STYPE" would be here
--Signed Boundary--
```

S/MIME 安全郵件 (二)

- 安全郵件型態 (2)
  - Application/pkcs-7-mime
    - 信件包裝成 **CMS (Cryptographic Message Syntax)**
    - 數位信封格式
    - **PCKS #7 安全套件**

```
EnvelopedData ::= SEQUENCE {
    version Version,
    recipientInfos RecipientInfos,
    encryptedContentInfo EncryptedContentInfo }
RecipientInfos ::= SET OF RecipientInfo
EncryptedContentInfo ::= SEQUENCE {
    contentType ContentType,
    contentEncryptionAlgorithm
    ContentEncryptionAlgorithmIdentifier,
    encryptedContent
      [0] IMPLICIT EncryptedContent OPTIONAL }
EncryptedContent ::= OCTET STRING
```

S/MIME 安全郵件 (三)

- 僅信封包裝格式
  - 包裝成『數位信封』
  - 可加密或明文封送

```
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
        name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m
    rfvbnj756tbBghyHhHUujhJhjH77n8HHGT9HG4VQpfyF467GhIGfHfYT6
    7n8HHGghyHhHUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H
    f8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
    0GhIGfHfQbnj756YT64V
```

S/MIME 安全郵件 (四)

- 僅簽署郵件
  - 採用 Application 型態
  - 採用 Multipart 型態

```
Content-Type: multipart/signed;
        protocol="application/pkcs7-signature"; micalg=sha1; boundary=boundary42
--boundary42Content-Type: text/plain
      This is a clear-signed message.
--boundary42
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s
      ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
      4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbn
      n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
      7GhIGfHfYT64VQbnj756
-boundary42--
```

- 簽署並加密郵件
  - 利用 signed-only 與 encrypted-only 交替處理
  - 一般皆先簽署再加密

Module 7-4：垃圾郵件防治(*)

Spam

- 開始流行是在1994年4月，當時有兩位美國律師Canter與Siegel為了代辦美國綠卡抽籤事宜，突發奇想找了一位程式人員寫了一小段程式，將他們所提供的服務大量散發至新聞群組(USENET)的每個版上，之後便開始有人將這類信件稱為Spam，而Spam也自此逐漸成了「垃圾郵件」的代名詞

- 近來世界各國立法禁止SPAM已逐漸成為潮流，例如美國聯邦與各州皆陸續完成立法禁止SPAM，並可能設立「do not spam」（謝絕廣告）名單讓民眾註冊

SPAM垃圾郵件的定義

- SPAM
  - 指未經電子郵件收信者同意而大量寄發的電子郵件，也有人將它翻譯為「大量郵件」
  - 通常是以商品廣告為內容，收信者最常收到的又以色情、藥品、強身或美容，發財夢等一類的廣告居多
  - 由於大量寄發收件者不想要的資訊，除了佔去整體電子郵件的大半流量之外，也常常大量塞爆使用者的電子信箱，並以各種欺騙手段混淆收件者判斷，甚至郵件內容讓人產生厭惡，更甚者，綁架使用者的電子郵件信箱或身份，因此普遍讓電子郵件使用者造成困擾

區別

- SPAM和大量方式寄送的商業廣告電子郵件
  - 兩者的差別在於有無經過收件者的同意。
    - 一般正派的行銷業者在寄發廣告郵件時是以「加入型」（opt-in）名單為基礎，也就是每個電子郵件地址都是經由收件者事先同意加入收信名單；同時也會有「退出」（opt-out）的機制，讓使用者可以自由選擇不想收到廣告郵件
    - SPAM則是未經收件者opt-in，也就是不具收件者同意的基礎

垃圾郵件防治策略簡述

- 網路的發展永遠都是雙刃劍，它給人們帶來了無限溝通的同時也帶來永無止境的安全問題。
  - 病毒成為了可以被控制的“殺手”，於是我們隨之進入了後病毒時代
  - 新的殺手—“垃圾郵件”，它的出現使得全球網路中40%的流量都在被它佔用，每一秒中世界都在因它而流失著大量的財富

垃圾郵件溯源

- 只要是符合下述四條之一的電子郵件都可被稱為垃圾郵件
  - 收件人事先沒有提出要求或者同意接收的廣告、電子刊物、各種形式的宣傳品等宣傳性的電子郵件
  - 收件人無法拒收的電子郵件
  - 隱藏發件人身份、地址、標題等資訊的電子郵件
  - 含有虛假的資訊源、發件人、路由等資訊的電子郵件
- 而在上述四條的定義中，符合第一條定義的垃圾郵件就佔了80%以上

垃圾郵件危害

- 垃圾郵件嚴重影響用戶的工作與生活
- 嚴重影響網路的正常運行
- 垃圾郵件攜帶病毒感染網路

垃圾郵件防治

- 儘量避免使用郵箱的“自動回復”功能
- 不要訂閱一些不太了解的網站郵件列表
- 申請兩個以上的個人郵箱
- 使用專業的工具

垃圾郵件的防治技術

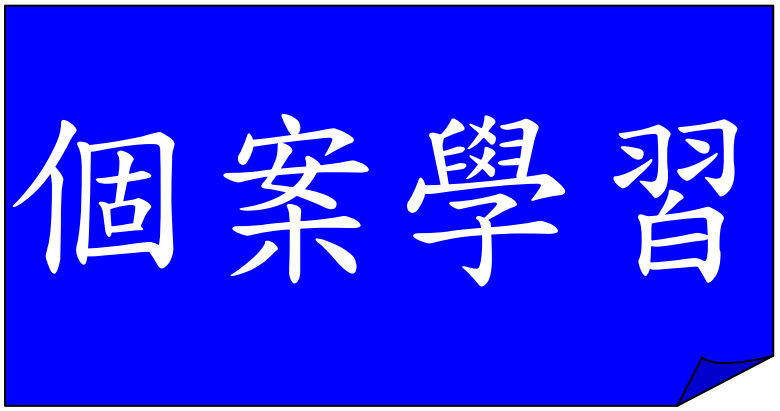
- 最多人使用的防治技術是“內容過濾”技術
  - 通過對郵件內容進行關鍵字過濾和對發信地址進行正確性分析來分辨是否為垃圾郵件
  - 但垃圾郵件程式
    - 將真實的發信地址隱藏起來而用一個正常的發信地址代替
    - 標題也會利用社會工程學的技術儘量避開敏感字眼，使得採用“內容過濾”技術的反垃圾郵件軟體無法真正過濾垃圾郵件

垃圾郵件的防治技術（續）

- 為了對付新型垃圾郵件，於是又出現了“智慧過濾”的反垃圾郵件技術
  - 採用智慧過濾的學習方法，使垃圾郵件過濾系統可以自動學會並適應垃圾郵件的變化手段，並進行智慧過濾
  - 據美聯社消息，近日，微軟公司就創建了一個團隊來專門研究這種“智慧過濾”技術。這一技術將會是目前乃至將來一段時間內主流的方法

成功大學垃圾郵件防治與成效

- 減少內部連線單位散發垃圾郵件機制
- 過濾外來垃圾郵件機制
- 執行結果
- 誤判處理機制
- 未來執行目標



減少內部連線單位散發垃圾郵件機制

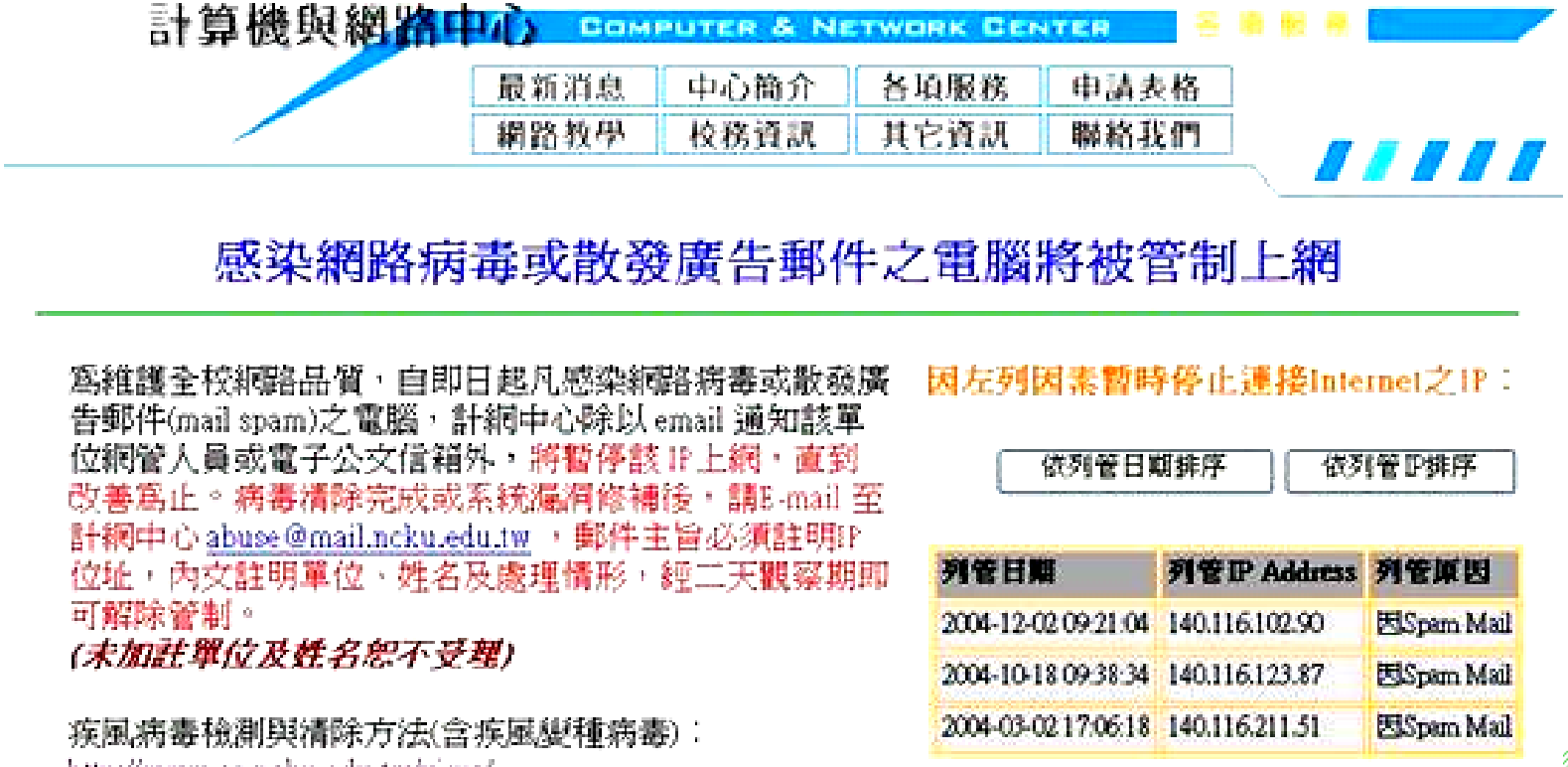
- 一、處理流程：
  - 本中心設有abuse@ncku.edu.tw及security@ncku.edu.tw二個專用e-mail信箱，一但接獲教育部或其他單位之抱怨信或檢舉信，立即透過e-mail通知該主機所屬單位網管人員處理，並告知相關技術文件網址。較嚴重之情形另以電話直接聯絡
  - 若違規IP為學生宿舍之電腦，可透過「宿網管理系統」依IP登錄資料通知該IP使用者，並可透過該系統停用違規IP

減少內部連線單位散發垃圾郵件機制（續）

- 二、防制措施：
  - 對於嚴重影響網路品質之主機，除立即通知管理單位或使用者外，並於網路設備管制該主機上網，直到管理者或使用者回應改善才解除限制
  - 為防止本校校園內之mail server被利用來寄發廣告信，本中心定期使用自動掃描程式主動檢測出本校網域內open relay之mail server，並請該主機管理單位修改設定，期使mail spam降至最低

減少內部連線單位散發垃圾郵件機制（續）

- 因中毒或mail spam被管制者將公告於中心網頁直到解除管制：

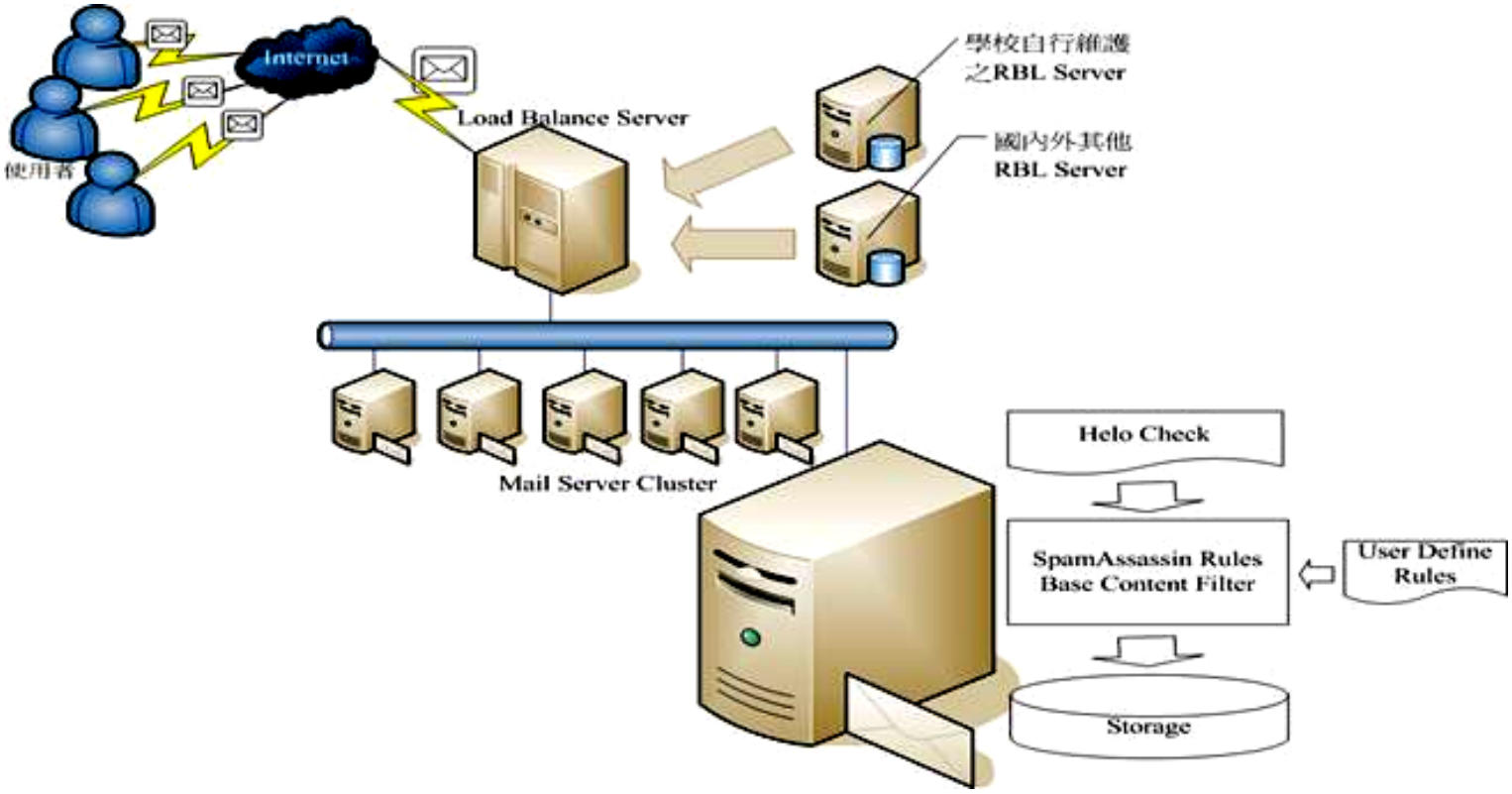


過濾外來垃圾郵件機制

- 一、目的
  - 根據校內郵件伺服器分析，垃圾郵件佔總郵件60%以上，且有不斷增加的趨勢，造成處理人力、媒體儲存空間處理效能與網路頻寬資源浪費，本校教職員工生已有處理垃圾郵件之需求。
- 二、執行方式
  - 國外已有許多組織建立DNS Block Lists (DNSRBLs)可供利用，並可有效查證垃圾郵件來源是否正確。
  - 國內ISP之使用者發信，正常來說應透過ISP之MailServer，若自行架站發信，實屬可疑。
- 目前根據以上兩點執行以下工作：
  - 利用國際共用之DNS Block Lists (DNSBLs)做防堵—主要為外文
  - 拒絕接收動態IP所發送之信件
  - 以軟體對信件主題及內容過濾—主要針對中文，但目前只標示未阻檔

過濾外來垃圾郵件機制（續）

- 以下為本校垃圾郵件架構圖



過濾外來垃圾郵件機制（續）

- 由內部三台Server負責收信，執行DNSRBLs阻擋，並阻擋所有從動態IP架站發信之信件。
- 每台亦運作SpamAssasin，執行郵件內容分析工作，針對郵件結構內容給予計算權重，判定為垃圾郵件之信件在標題加上『疑似垃圾郵件』。

執行結果

- 目前每日依據DNSRBL方式阻擋之郵件到達總信件量之53%，郵件內容分析工作的程式可再判斷出4%的郵件，從動態IP阻擋6%
- 第一層經過RBL阻擋之後，使用者會接收到系統退信通知，內容說明寄建主機被列入黑名單，並提供網址給使用者查詢。若是為誤判，可以跟計網中心聯絡，我們經過調查後，會將非不正常使用之郵件主機加入白名單
- 郵件內容分析程式會分析郵件結構、來源，判別是否可能為垃圾郵件。判斷為”是”則在標題加上『疑似垃圾郵件』
- 本校郵件系統並不會擅自將使用者信件刪除

誤判處理機制

- 本校的DNSRBL Server參考將近10部國內外參考主機，自行建立本校的RBL Server。直接參考外部主機會有誤判的問題，目前本校主機採用白名單的方式加以修正，減少誤判產生的使用者困擾
- 現在郵件內容分析程式已完成可讓使用者自訂規則之介面，待全面測試完成後，即可開放讓全校師生使用，避免系統預設規則與使用者設定差距過大

未來執行目標

- 持續執行現有的DNS黑名單與動態IP阻擋工作。
- 完成使用者自訂規則之模組，讓User自行選擇過濾條件，以符合使用者個人需求
- 建立完整誤判回報機制，減少誤判

習 題

習題一

- 請畫出電子郵件收發的流程，並說明相關步驟。

習題二

- 電子郵件的弱點有那些，為什麼？

習題三

- 請說明PGP的精神。

習題四

- 請問PGP如何進行加密和解密，請以流程圖說明運作方式。

習題五

- 請簡述S/MIME功能性。

習題六

- 試比較S/MIME和 PGP不同。

習題七

- 請說明SPAM垃圾郵件的定義。

習題八

- SPAM和大量方式寄送的商業廣告電子郵件的區別在那裡？

Module 7-5:專案實作(**)

專案目的

- 建置email應用環境。
- 利用實際操作的方式讓同學了解PGP及Anti-Spam工作原理。

專案一描述：Module 7-1實作

- A公司最近一年來因兩岸商務往來頻繁，業績成長數倍，原來使用的Exchange 2000電子郵件伺服器已經不敷使用，在成本的考量下，A公司高層主管希望以最小的成本建置新的電子郵件伺服器，同時提供認證的機制，避免該伺服器被當成廣告信跳板。你是該公司的MIS人員，請以自由軟體（Free Software）為基礎實作電子郵件伺服器，該伺服器必服提供認證，避免避免該伺服器被當成廣告信跳板，並以流程圖文件，詳述運作方式。

Hint：請自行選擇熟悉的UNIX平台，並安裝可進行收發信mailserver，流程說明請參考7-10~7-20頁。

專案二描述：Module 7-2實作

- 專題實作
  - A公司最近一年來因兩岸商務往來頻繁，業績成長數倍，自從改用新的電子郵件伺服器後，電子郵件的收發更有效率。但是最近在同業間發生了幾件極機密電子郵件遭到竊聽。你是該公司的MIS人員，請以自由軟體（Free Software）為基礎實作電子郵件加密，保障極機密電子郵件不會有遭到竊聽風險，並以流程圖文件，詳述運作方式。

Hint:

- 請自行到http://www.pgpi.org/ 下載PGP軟體實作，請參考7-46~7-49 頁加解密流程圖詳述運作方式。

專案三描述：Module 7-3實作

- 專題實作
  - A公司最近一年來因兩岸商務往來頻繁，業績成長數倍，自從改用新的電子郵件伺服器後，電子郵件的收發更有效率。但是最近在同業間發生了幾件極機密電子郵件遭到竊聽。公司高層決定購買第三方認證的方式來保護公司機密，你是該公司的MIS人員，並以流程圖文件，詳述運作及申請方式。

    Hint:

    - 請自行到 https://digitalid.hitrust.com.tw/class1/index.htm 參考申請及使用方式。

專案四描述：Module 7-4實作

- 專題實作
  - A公司最近一年來因兩岸商務往來頻繁，業績成長數倍，自從改用新的電子郵件伺服器後，電子郵件的收發更有效率。但是近來該伺服器收到不請自來的廣告信件，不僅造成同仁的困擾，也佔用了不少對外連線頻寬及伺服器資源。你是該公司的MIS人員，請以自由軟體（Free Software）為基礎實作過濾廣告信方法，避免該伺服器被大量廣告信入侵，並以流程圖文件，詳述運作方式。

Hint：請參考成大個案。

參考文獻

1. http://www.soft6.com/news/detail.asp?id=11637電子郵件發展歷史
2. http://www.symantec.com/region/tw/enterprise/article/junk_mail_1.html 電子郵件的30年發展歷程
3. http://linux.vbird.org/linux_server/0380sendmail.php電子郵件的傳送
4. http://www.aicpa.org/PUBS/JOFA/jul2002/mascha.htm電子郵件的安全
5. http://www.chinaitpower.com/A/2003-11-29/63790.html 保護郵件加密兩把鎖：PGP和S/MIME
6. http://jedi.org/blog/archives/002591.html 如何利用PGP 安全傳送的例證
7. http://jedi.org/blog/archives/002592.html 我為什麼要撰寫 PGP
8. http://www.cnpaf.net/Class/RFC/053291853328757.html S/MIME版本3資訊說明書
9. http://www.ccl.itri.org.tw/express/publish/3cindex_32.htm 郵件加密　絕不外漏 S/MIME-電子郵件安全技術
10. http://taiwan.cnet.com/enterprise/glossary/term/0,2000062921,2000058056,00.htm?SPAM垃圾郵件的定義
11. http://big5.ccidnet.com：89/gate/big5/tech.ccidnet.com/art/238/20030728/56588_1.html垃圾郵件防治策略簡述
12. http://tnrc.ncku.edu.tw/93/61.htm 成功大學垃圾郵件防治與成效