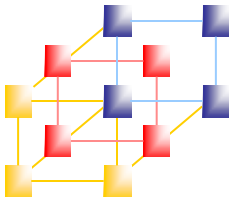
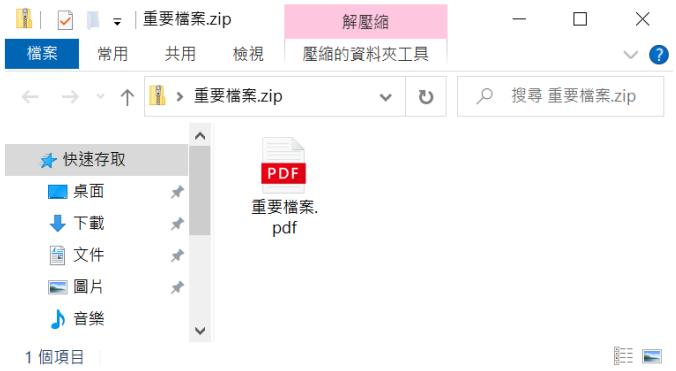


Unit 3
Electronic Mail Security

你有收過這種檔案嗎？

- 大部分掃描軟體都會掃描壓縮檔
- 但是如果壓縮檔加密碼呢？
- 1. 

2. 

我們有客戶就是這樣中標的！

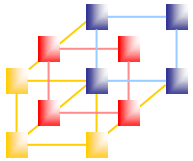
要用郵件傳送敏感檔案怎麼辦？

- 大家很愛用WinZIP加密碼
- 密碼寫在信件裡
- 日本稱為PPAP傳檔

Source: Wikipedia

感覺好安全

- 今天阿明想把金銀財寶送給阿桃
- 阿明買了個傳家名鎖保險箱
- 阿明把寶藏鎖在保險箱裡
- 把鑰匙貼在包險箱上
- 把**保險箱連同鑰匙**丟給**白貓宅急便**
- 感覺好安全、好安心！！！



安全點的做法

- 大家很愛用WinZIP加密碼
- 密碼打電話告訴對方

似乎較安全

- 今天阿明想把金銀財寶送給阿桃
- 阿明買了個傳家名鎖保險箱
- 阿明把寶藏鎖在保險箱裡
- 把保險箱丟給**白貓宅急便**
- 把鑰匙丟給**小嘴鳥**
- 似乎較安全、較安心！！！
- But... 如果白貓宅急便和小嘴鳥**共謀**呢？！
- 沒有100%的安全
- 方便、安全總打對台，真要安全，親送吧！xD

可能更安全的作法 - +

- 阿桃有一個傳家名鎖保險箱上面有投入口
- 阿桃先用白貓宅急便把保險箱寄給阿明
- 阿明把寶藏從縫丟進保險箱裡
- 請白貓宅急便把保險箱送回給阿桃
- 阿桃用自己的鑰匙打開保險箱
- 阿桃取得寶藏

→ **公開金鑰加密系統**就是如此運作的

- But… 如果白貓宅急便偷偷把保險箱掉包呢？

可能更安全的作法 - ++

- 阿桃有一個傳家名鎖保險箱上面有投入口
- **阿桃先把保險箱拿去法院公證取得防偽證明**
- 阿桃用白貓宅急便把保險箱寄給阿明
- 阿明把寶藏從縫丟進保險箱裡
- 請白貓宅急便把保險箱送回給阿桃
- 阿桃用自己的鑰匙打開保險箱
- 阿桃取得寶藏

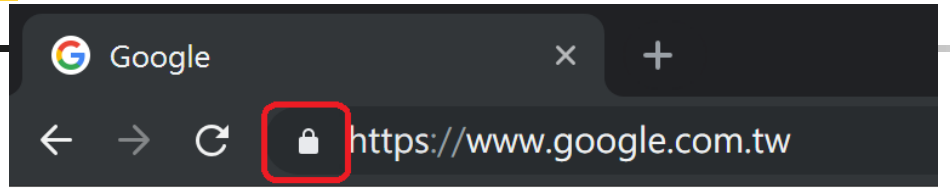
憑證

→ **PKI**就是如此運作的 Source: bilibili

- 如果白貓宅急便偷偷把保險箱掉包呢？

→憑證錯誤

複習一下說了很多次的TLS



User

Web Server

DB

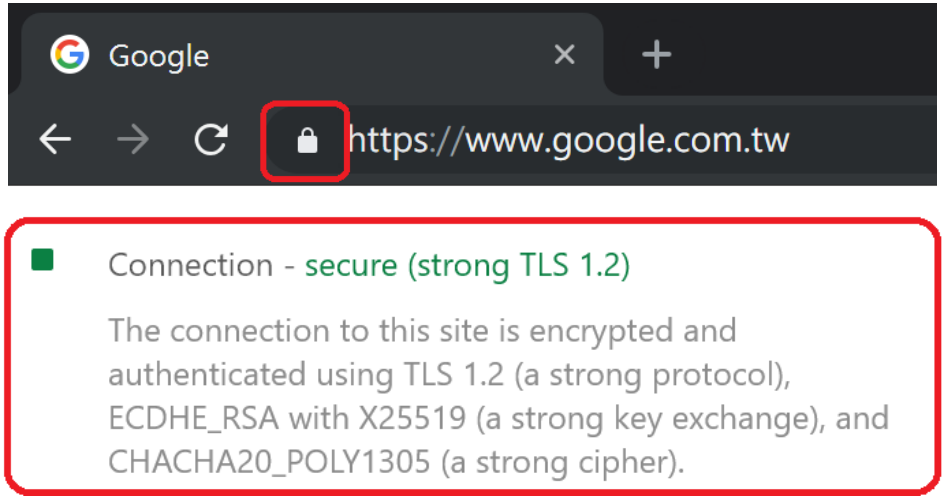
加密保護

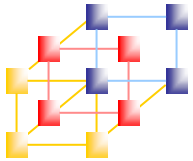
確認和我安全連線的是：

Administrator

憑證的重要性

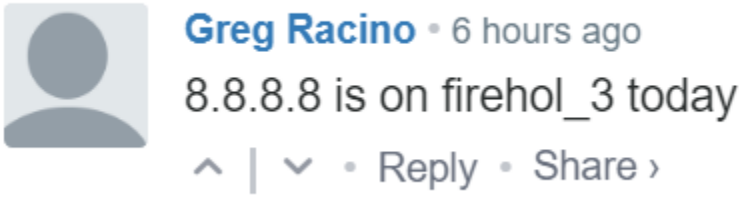
- 這就是為什麼一天到晚宣導網站鎖頭鑰是閉上的
- Transport Layer Security
  - 保障傳輸過程的安全
  - 不只出現在HTTPS上
    - SSH
    - FTPS / SFTP
    - SMTPS / POP3S / IMAPS
    - …

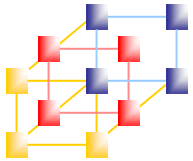




題外話 - 黑名單自動更新

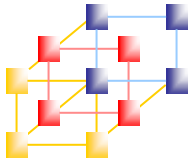
- 每天自動更新黑名單也有風險
  - http://iplists.firehol.org/?ipset=firehol_level3





社交工程實例

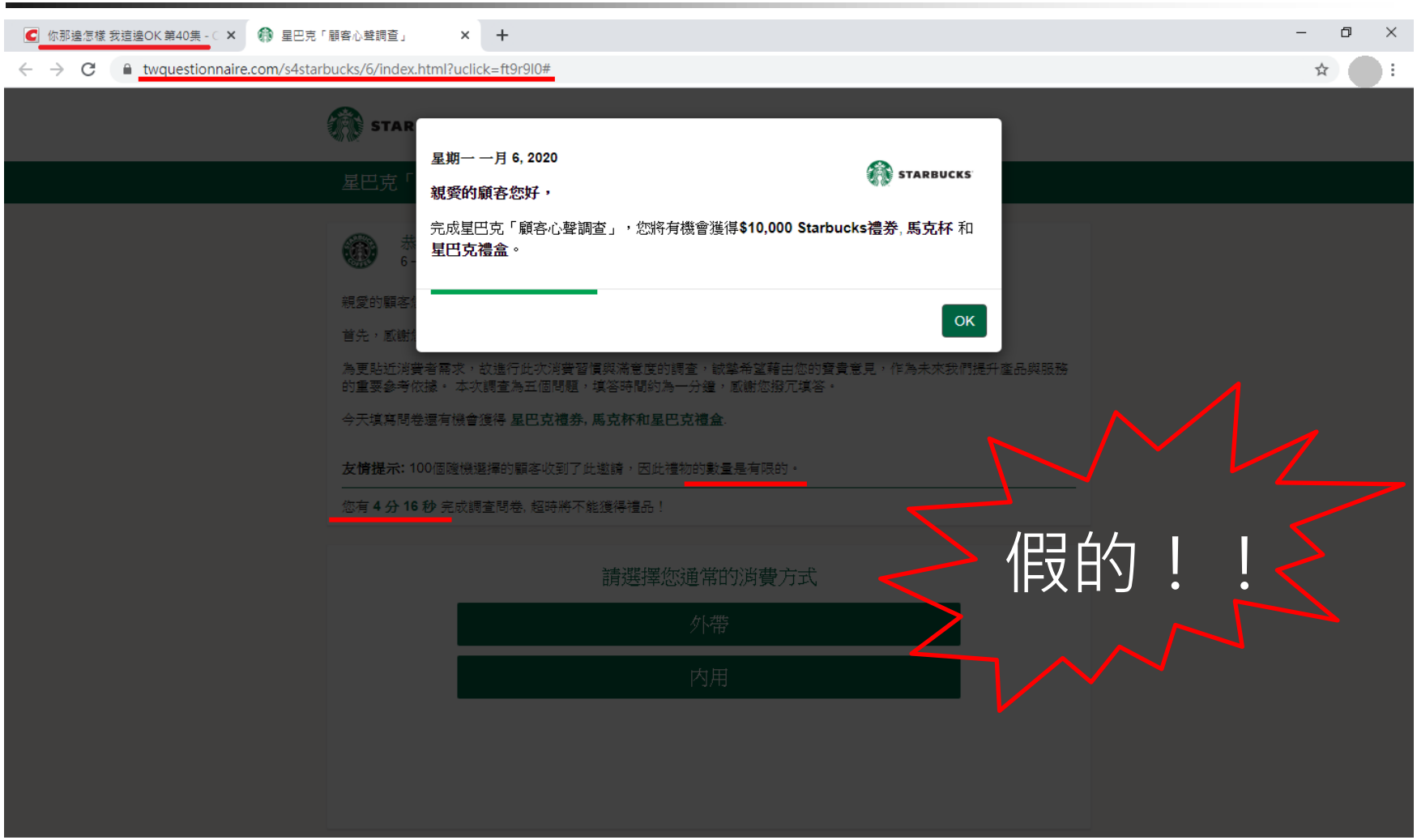
- 常用的誘惑釣魚方法
  - 年節交通疏運措施報馬仔
  - 新一年度請假攻略
  - 購物優惠與年節專案資訊
  - 團購資訊(容易集體上鉤)
  - 網銀、訂票帳號已鎖定及忘記密碼
  - 訂單確認信
  - 主管發送的交辦事項



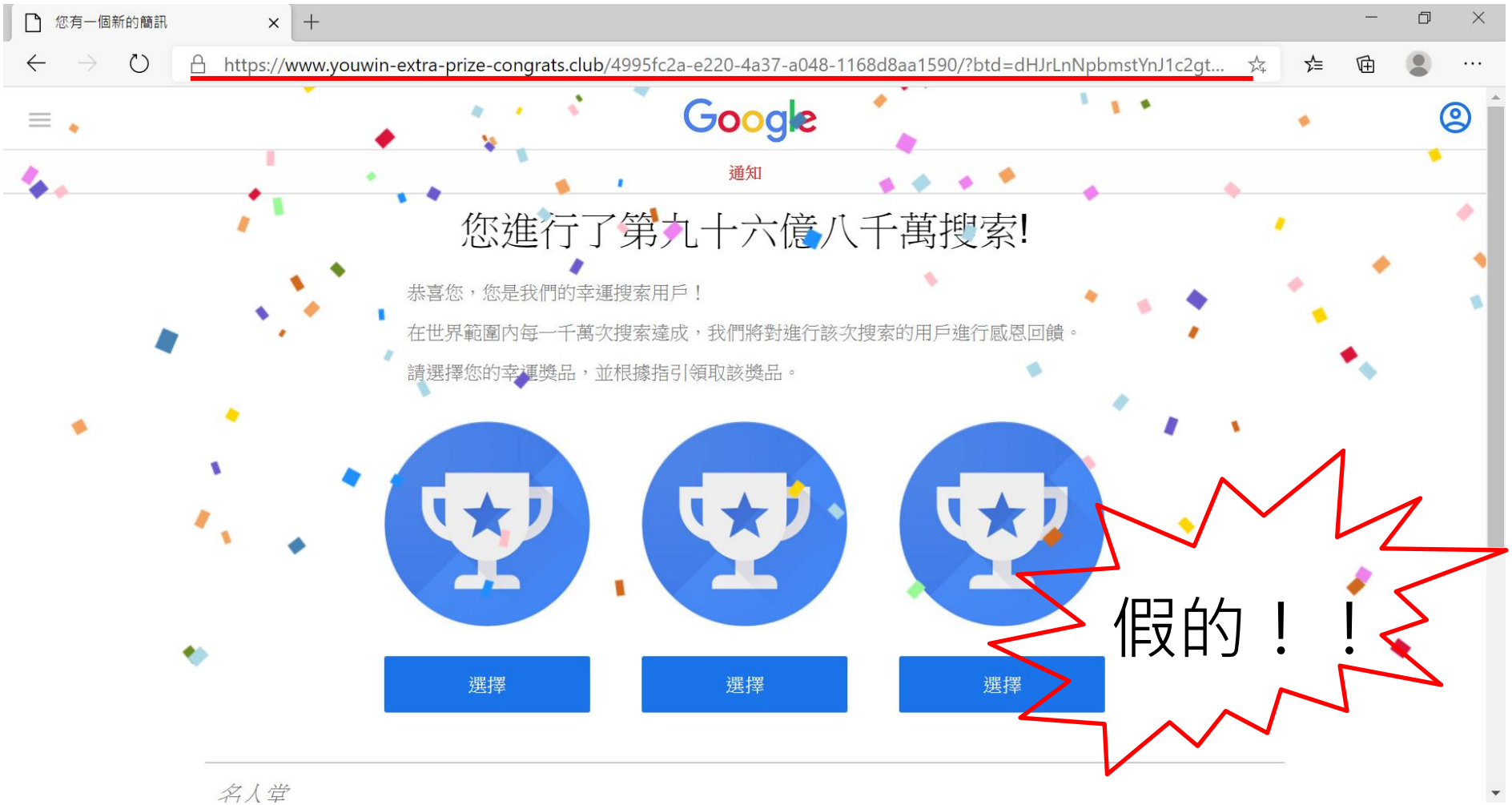
有關社交工程攻擊

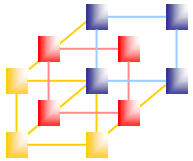
- 誰常是破口？
  - ~~3+11~~
  - 高階主管 → Powerful
  - 出納 → $$$
  - 菜鳥 → 菜渣掉滿地
- 誰常是施暴者？
  - 競爭同業
  - 吃飽撐著的駭客
  - 員工
  - 離職員工

釣魚攻擊騙個資


你那邊怎樣 我這邊OK 第40集 -
星巴克「顧客心聲調查」
twquestionnaire.com/s4starbucks/6/index.html?uclick=ft9r9l0#
星期一 一月 6, 2020
STARBUCKS
親愛的顧客您好，
完成星巴克「顧客心聲調查」，您將有機會獲得$10,000 Starbucks禮券, 馬克杯 和 星巴克禮盒。
OK
友情提示: 100個隨機選擇的顧客收到了此邀請，因此禮物的數量是有限的。
您有 4 分 16 秒 完成調查問卷, 超時將不能獲得禮品！
請選擇您通常的消費方式
外帶
內用
假的！！

釣魚攻擊騙個資


您有一個新的簡訊
https://www.youwin-extra-prize-congrats.club/4995fc2a-e220-4a37-a048-1168d8aa1590/?btd=dHJrLnNpbmstYnJ1c2gt...
Google
通知
您進行了第九十六億八千萬搜索!
恭喜您，您是我們的幸運搜索用戶！
在世界範圍內每一千萬次搜索達成，我們將對進行該次搜索的用戶進行感恩回饋。
請選擇您的幸運獎品，並根據指引領取該獎品。
選擇
選擇
選擇
假的！！
名人堂



假勒索信件

2018/11/4 (週日) 下午 03:12
asimon@asimon.idv.tw
너의 마음의 평화의 문제.
收件者 asimon@asimon.idv.tw

여보세요!

당신은 나를 알지 못할 수도 있습니다. 왜이 전자 메일을 받는지 궁금합니다. 맞습니까?
이 순간 나는 당신 계정 (asimon@asimon.idv.tw) 을 해킹했다. 내 너의 장치에 완전히 액세스 할 수 있습니다!
사실 성인 비디오 (포르노 소재) 웹 사이트에 악성 코드를 설치했는데 무엇을 알고 있었는지,이 웹 사이트를 방문하여 재미있게 지내는 것이 었습니다.
비디오 클립을 시청하는 동안 인터넷 브라우저가 RDP (원격 데스크톱)로 작동하기 시작했습니다.
그게 나에게 당신의 스크린과 웹캠에 대한 액세스를 제공하는 keylogger 를 가지고있다.
그 직후, 내 소프트웨어 프로그램은 전자 메일뿐만 아니라 메신저, 소셜 네트워크에서 전체 대화 상대를 모았습니다.

내가 뭘 한거지?
나는 이중 스크린 비디오를 만들었다. 첫 번째 부분은 시청 한 비디오 (좋고 이상한 맛)를 보여 주며 두 번째 부분은 웹캠 녹화를 보여줍니다.
정확히 무엇을해야합니까?

음, 879 달러는 우리의 작은 비밀에 대한 공정한 가격이라고 생각합니다. Bitcoin 이 지불합니다 (모르는 경우 Google 에서 "비트 코인 구매 방법"검색).
내 BTC 주소 : 1B1Vov1LTLGLcVG3ycPQhQLe81V67FZpMZ
(민감한 cAsE 이므로 복사하여 붙여 넣기하십시오)

노트 :
결제하려면 2 일이 소요됩니다.
(나는이 이메일 메시지에 특정 픽셀을 가지고 있으며,이 순간 당신은이 이메일 메시지를 읽었 음을 안다.)

BitCoins 를받지 못하면 가족, 동료 등 모든 연락처에 비디오 녹음을 보내드립니다.

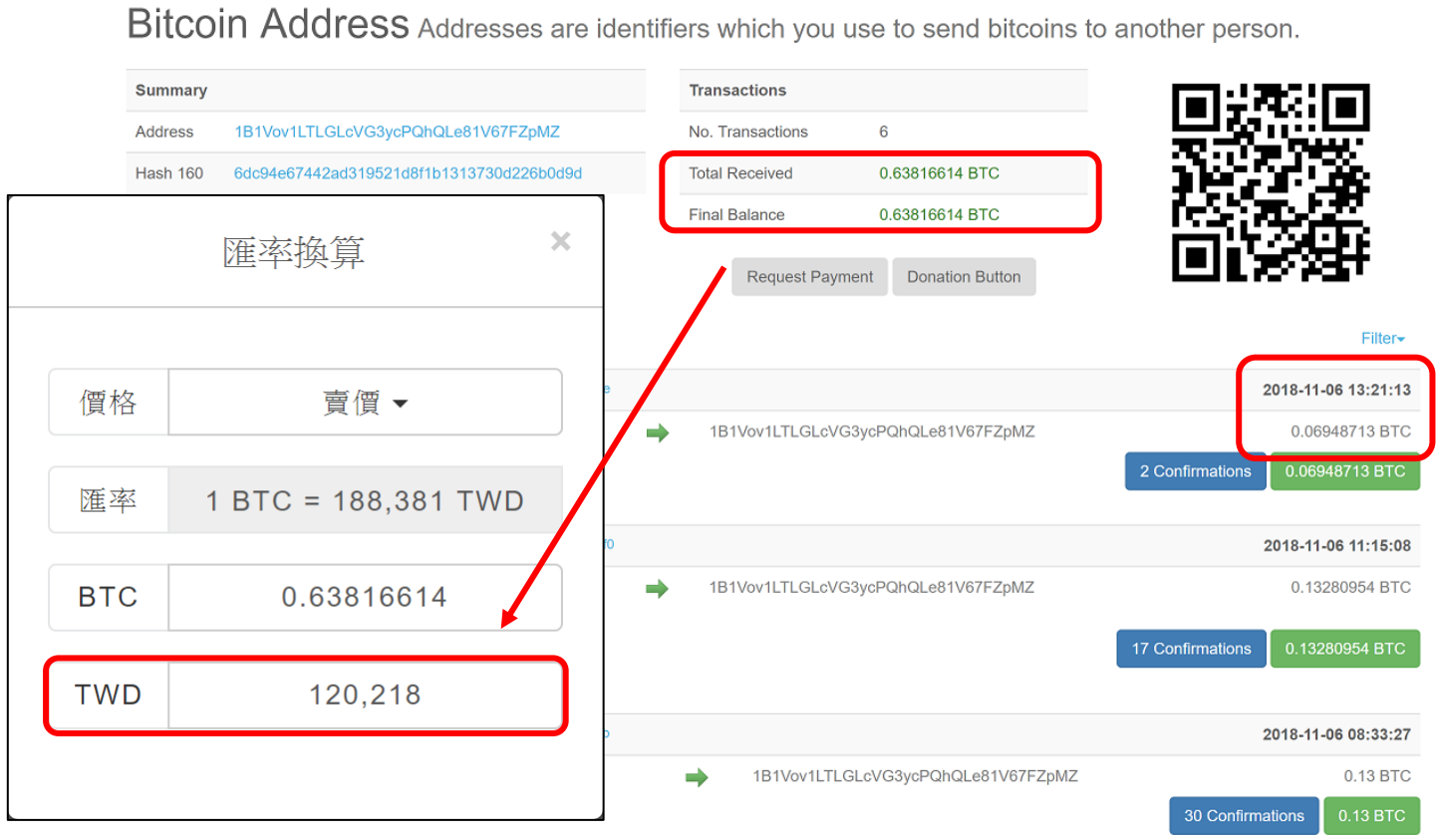
그러나 내가 돈을 받으면 즉시 비디오를 파괴 할 것입니다.

이것은 협의가 불가능한 제안이므로이 전자 메일 메시지에 응답하여 개인적인 시간을 낭비하지 마십시오.

中文版的出現指日可待... =___=

假勒索信件

- Bitcoin的特性
  - 公開 / 匿名 = 大家都可以看他騙到了多少錢 xD
  - 以最後面的韓國人為例，11/4收到信...真神奇！



假勒索信件

- Bitcoin的特性
  - 比特幣濫用回報平台 https://www.bitcoinabuse.com/

Bitcoin Abuse Database

Report history for **1B1Vov1LTLGLcVG3ycPQhQLe81V67FZpMZ**

Address found in database:

Address	*1B1Vov1LTLGLcVG3ycPQhQLe81V67FZpMZ*
Report Count	100
Latest Report	Tue, 06 Nov 18 13:26:19 +0000 (1 hour ago)

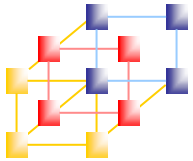
View address on blockchain.info

If you have additional information about this address, please file a report.

只能引以為戒，作為警示！

Reports:

Date	Abuse Type	Abuser	Description
Nov 6, 2018	blackmail scam	Spoofed email	I greet you! I have bad news for you. 11/08/2018 - on this day I hacked your operating system and got full access to your account yyyy@xxxxxxxx.com.br It is useless to change the password, my malware intercepts it every time. How it was: In the software of the router to which you were connected that day, there was a vulnerability. I first hacked this router and placed my malicious code on it. When you entered in the Internet, my trojan was installed on the operating system of your device. After that, I made a full dump of your disk (I have all your address book, history of viewing sites, all files, phone numbers and addresses of all your contacts). A month ago, I wanted to lock your device and ask for a small amount of money to unlock.



假勒索信件

2024/10/17

Delivery status notification.

oenytian@mailcatch.com
收件者 asimon@asimon.idv.tw

你好啊，我的变态朋友！

我就直接说重点吧。
其实我们认识有一段时间了，至少我认识你。
你可以叫我老大哥或全视之眼。
我是一名黑客，几个月前，我获得了访问您设备的权限，包括您的浏览器历史记录和网络摄像头。
我录制了一些你对着极具争议的“成人”视频撸管的视频。
你肯定不希望你的家人、同事和与你有邮件(asimon@asimon.idv.tw)往来的所有人都看到你玩弄自己的样子吧？特别是考虑到你最喜欢的“视频”类型有多变态。
我还会在色情网站上发布这些视频，它们会在互联网上广泛传播，不可能被全部删除。

我到底是怎么做到的呢？
原因很简单，你对互联网安全的无视，使我轻松地在你的硬盘上安装了特洛伊木马。
通过这一木马程序，我能够访问你设备上的所有数据，并能够远程控制你的设备。
而通过这一台感染的设备，我进而获得了访问你所有其它设备的权限。

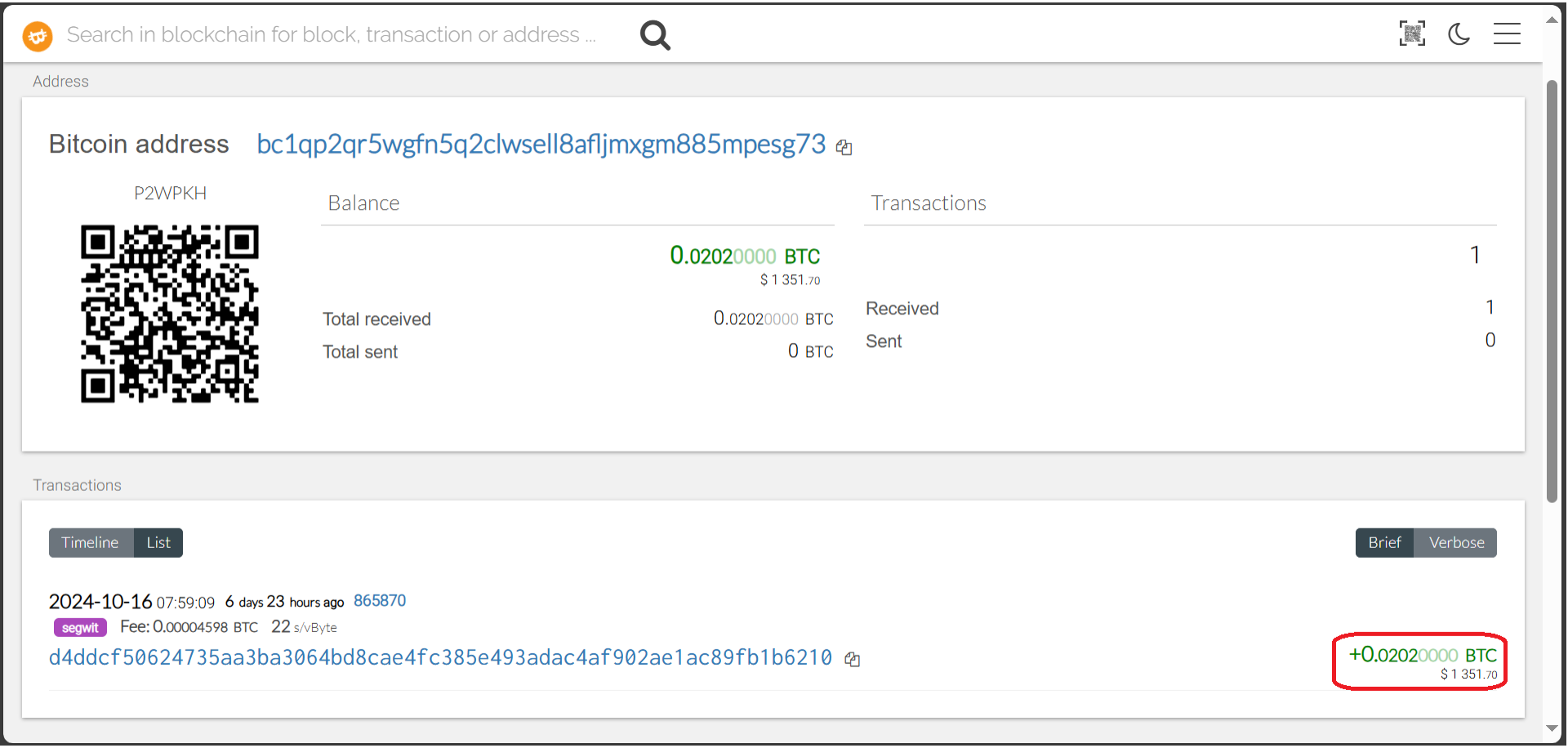
我的间谍软件是嵌入在驱动程序中的，而且每隔几个小时便会更新一次签名，因此任何杀毒软件或防火墙都无法检测到它。
现在我们来谈一笔交易吧：只要一小笔钱，就可以让你找回以前那无忧无虑的生活。

给我的比特币钱包里转 1350 美元：bc1 qp2 qr5wgfn5q2 clwsell8afljmxgm885mpesg73

一旦确认收到这笔款项，我就会删除所有对你不利的视频，并将病毒从你所有的设备中移除，然后我就会从你的生活中消失。
从你的聊天软件中的记录，可以看得出来，别人都认为你是一个正直的人。为了保住你的声誉，这点小钱并不算什么。你可以认为我是你人生路上的一个老师，教会了你应该珍惜现在所拥有的一切。

真的有人轉錢 Again

- bc1qp2qr5wgfn5q2clwsell8afljmxgm885mpesg73



假勒索信件

(σ`▽´)σ UCCU~~~

使用後

Source:Wikipedia

使用前

Source: 自由時報

比特幣的出現

與BEC詐騙結合

- Bitcoin與商業電郵詐騙結合？(未來式？！)

新聞

商業電郵詐騙猖獗，今年全臺遭詐騙金額已破兩億元

針對企業的電子郵件詐騙（BEC）案件不斷，全球企業都蒙受其害，今年危害再擴大，刑事警察局與FBI均不斷提醒企業注意。

文/ 羅正漢 | 2018-10-17 發表

讚 5.1 萬 按讚加入iThome粉絲團 讚 140 分享 G+

Source:iThome

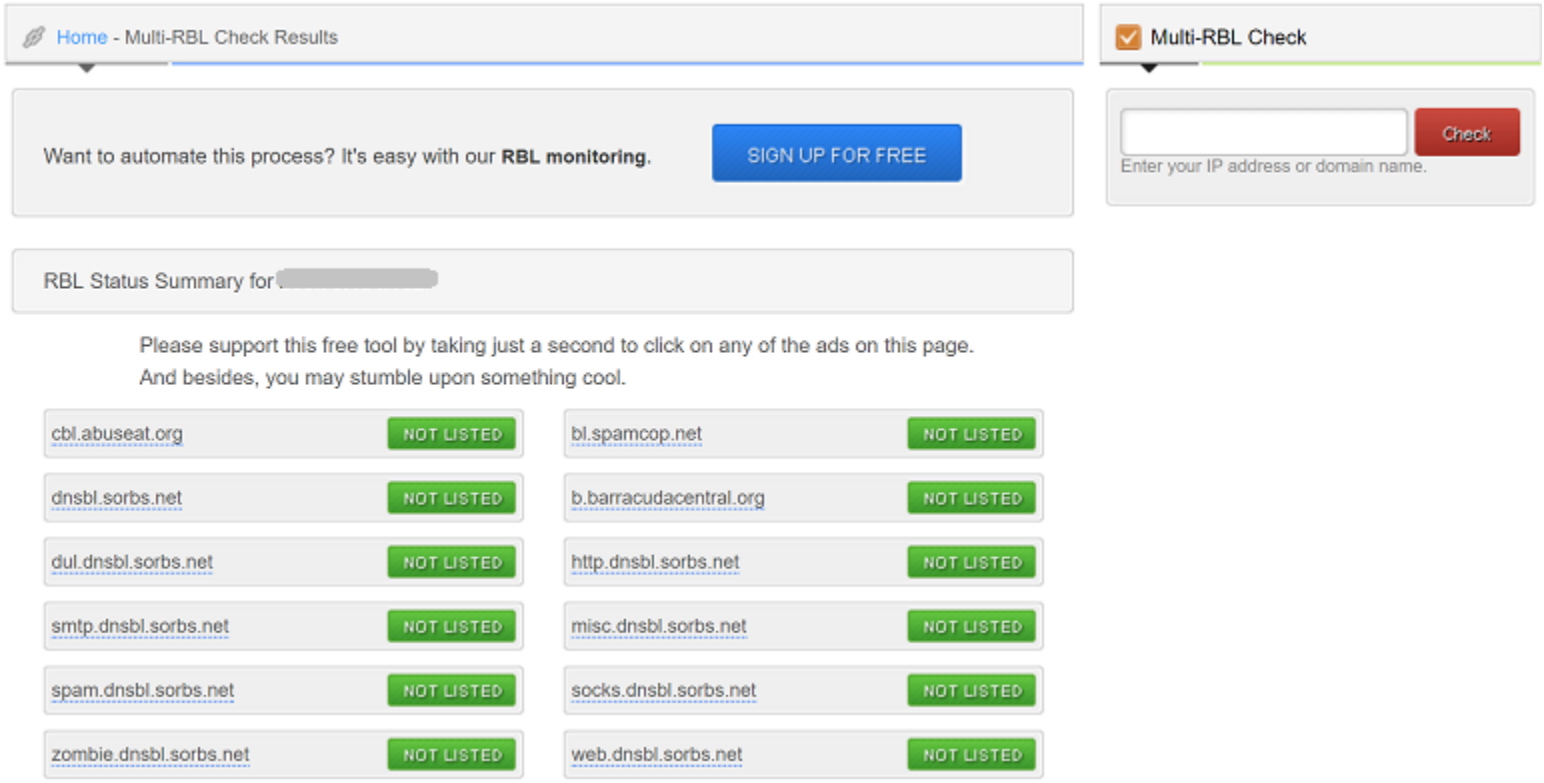
1. 現金轉帳→玉山全球通
2. 玉山→Paypal
3. Paypal→Bitcoin

Buying Bitcoins with PayPal using eToro
Buying Bitcoins with PayPal using Virwox
Buying Bitcoins with PayPal using LocalBitcoins
Buying Bitcoins with PayPal using Wirex
Buying Bitcoins with PayPal using Paxful
Buying Bitcoins with PayPal using Coinbase

Source:99bitcoins.com

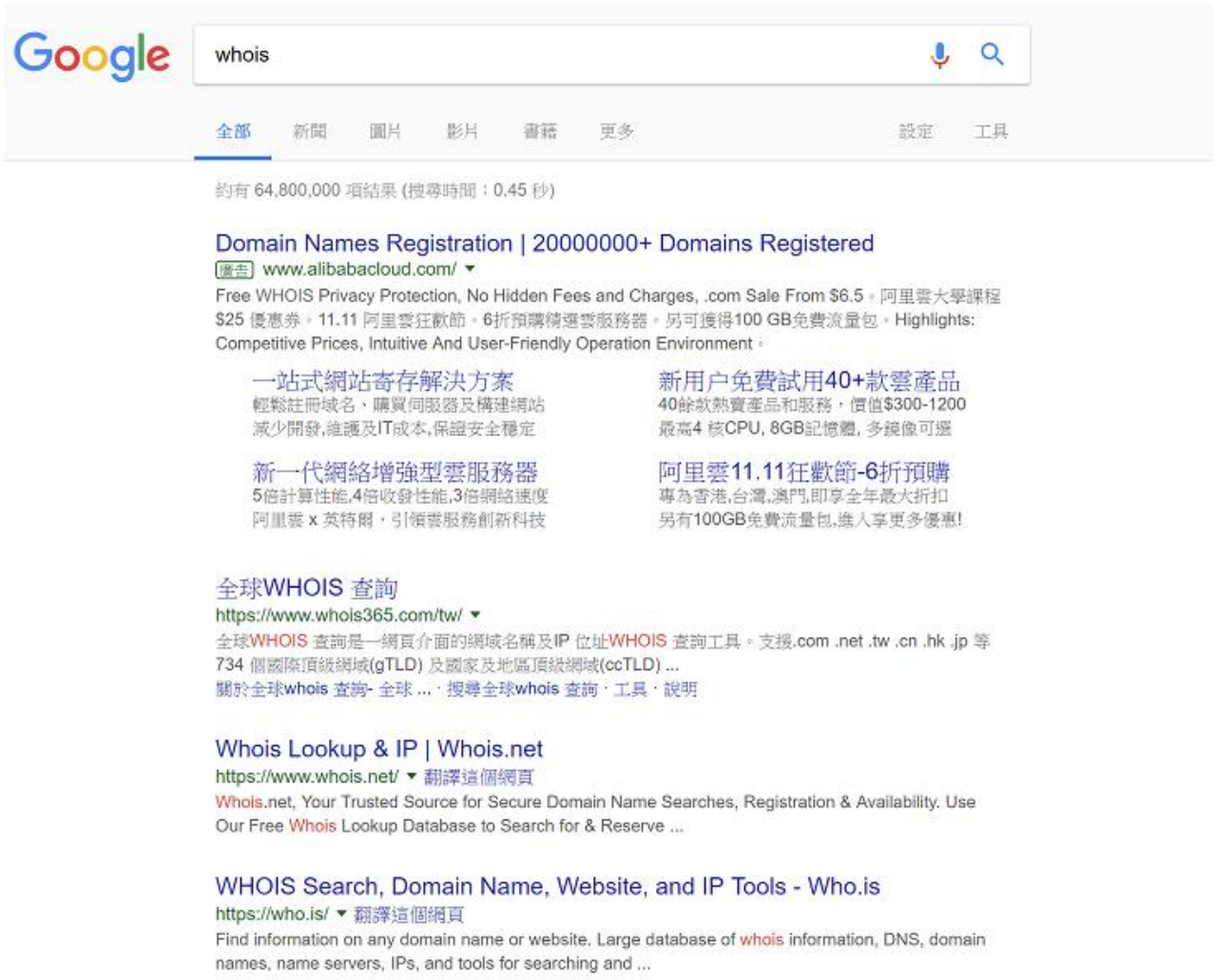
實作練習

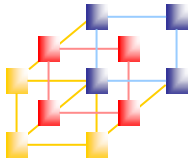
- **RBL查詢**
  - **http://www.anti-abuse.org/multi-rbl-check-results/**



實作練習

- **Whois and IP Whois**





電子郵件弱點

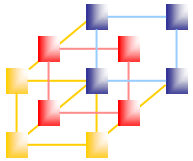
- 電子郵件發展歷史
  - 電子郵件翻譯自英文的email或e-mail
  - 早在網際網路流行以前，電子郵件就已經存在了
  - 現在已經演變成為一個更加複雜並豐富得多的系統
  - 網際網路擴展了其應用的範圍
  - 使用在支援TCP/IP協定或具有SMTP和POP的網路

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

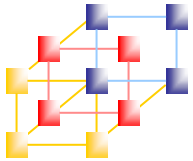
電子郵件的30年發展歷程

- 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



電子郵件的挑戰

- 電子郵件：優勢、缺點
- 即時訊息：優勢、缺點
  - ~~ICQ~~
  - ~~Yahoo Messenger~~
  - ~~MSN Messenger~~
  - Line
  - What's App
  - Skype
  - Facebook Messenger

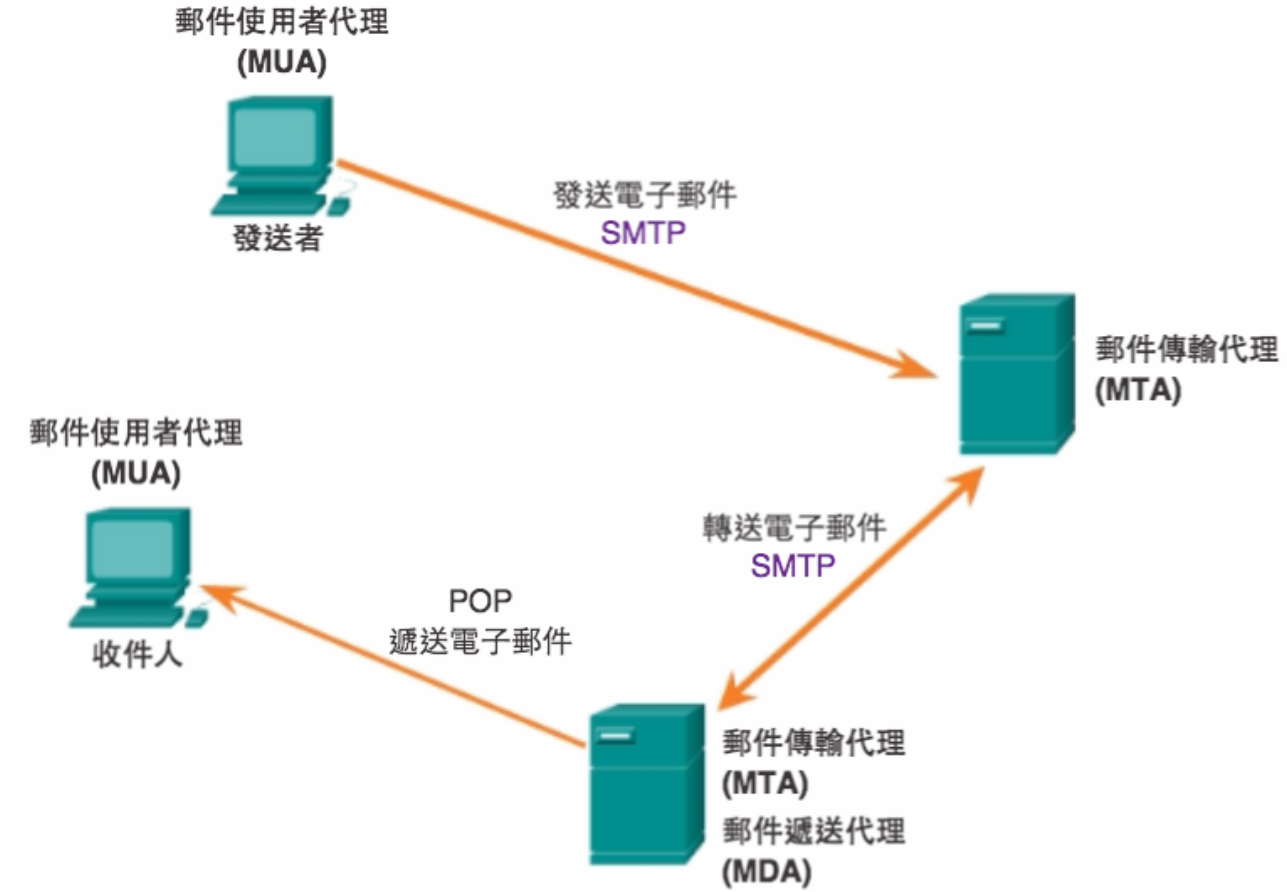


電子郵件的挑戰

- 電子郵件
- 即時訊息

→ 不同場合不同媒介

電子郵件的傳送 (1/5)

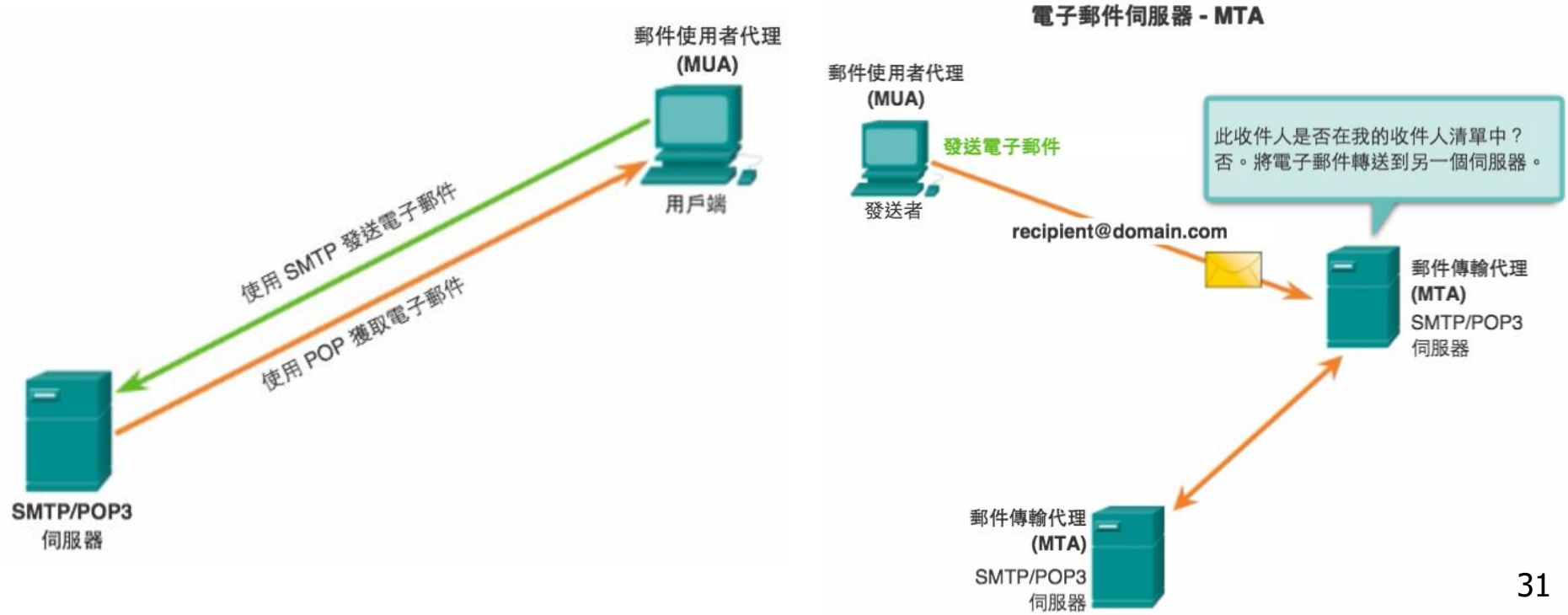


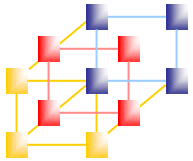
SMTP 用於將電子郵件從用戶端發送到伺服器和在電子郵件伺服器之間轉送電子郵件。

POP 用於遞送電子郵件。

電子郵件的傳送 (2/5)

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





電子郵件的傳送 (3/5)

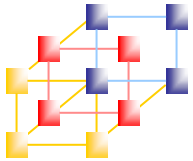
- MTA (Mail Transfer Agent) ： MTA 就是郵件伺服器，『郵件傳送代理人』的意思。主要功能有：
  - 收受外部主機寄來的信件
  - 幫使用者傳送 (寄出) 信件
  - 讓使用者自己的信可以收回去

電子郵件的傳送 (4/5)

- 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 (5/5)

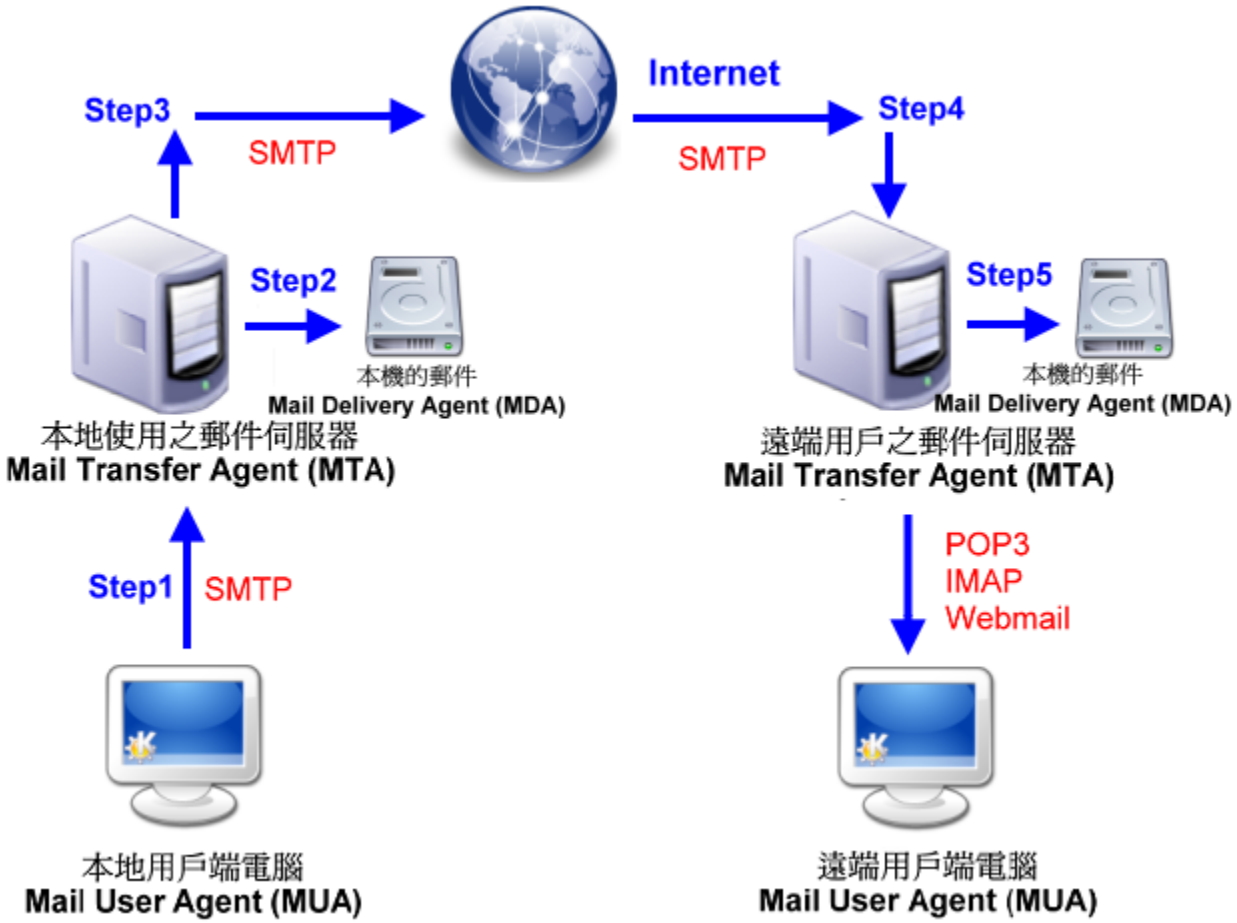
- Mailbox
  - 『郵件信箱』就是在主機上面的一個目錄下某個人『專用』的信件收受檔案。
  - 以 UNIX 來說，系統管理員 root ，有個信箱在 /var/spool/mail/root 。
  - 當 MTA 收到 root 的信時，就會將該封信件存到 /var/spool/mail/root 這個檔案中。



角色再介紹

- MUA：終端使用者收發信的介面
  - Outlook、 Mozilla Thunderbird…
- MTA/MDA：郵件伺服器
  - Exchange、Sendmail、Postfix…
  - 衍伸產品眾X、中X數位、Mail2xxx、X軟…
- Mailbox：Mailbox or MailDIR
  - Mailbox：一個人一個檔案
  - MailDIR：一個人一個資料夾

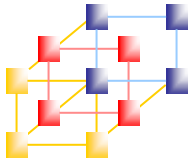
電子郵件系統運作



https://www.twbsd.org/cht/book/ch16.htm

使用的協定– SMTP

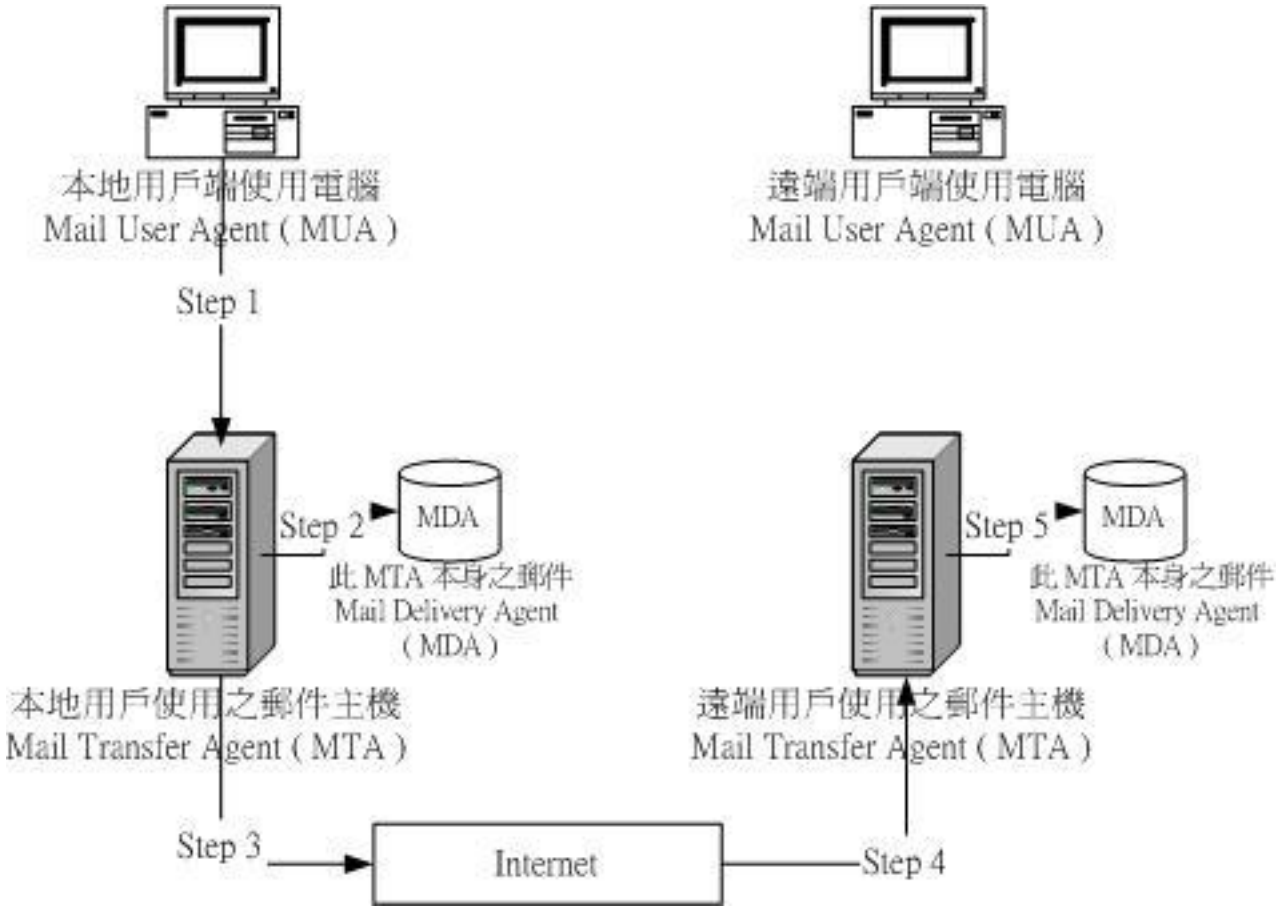
- 郵件主機使用 SMTP (Simple Mail Transfer Protocol) 這個協定，port number 為 25 。
- 寄信時，MUA 主動連接 smtp 協定 (port 25) 而送出去。
- 郵件主機 MTA 在轉遞的時，也是經下一部 MTA 的 smtp 協定 (port 25)來將信送出去。



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

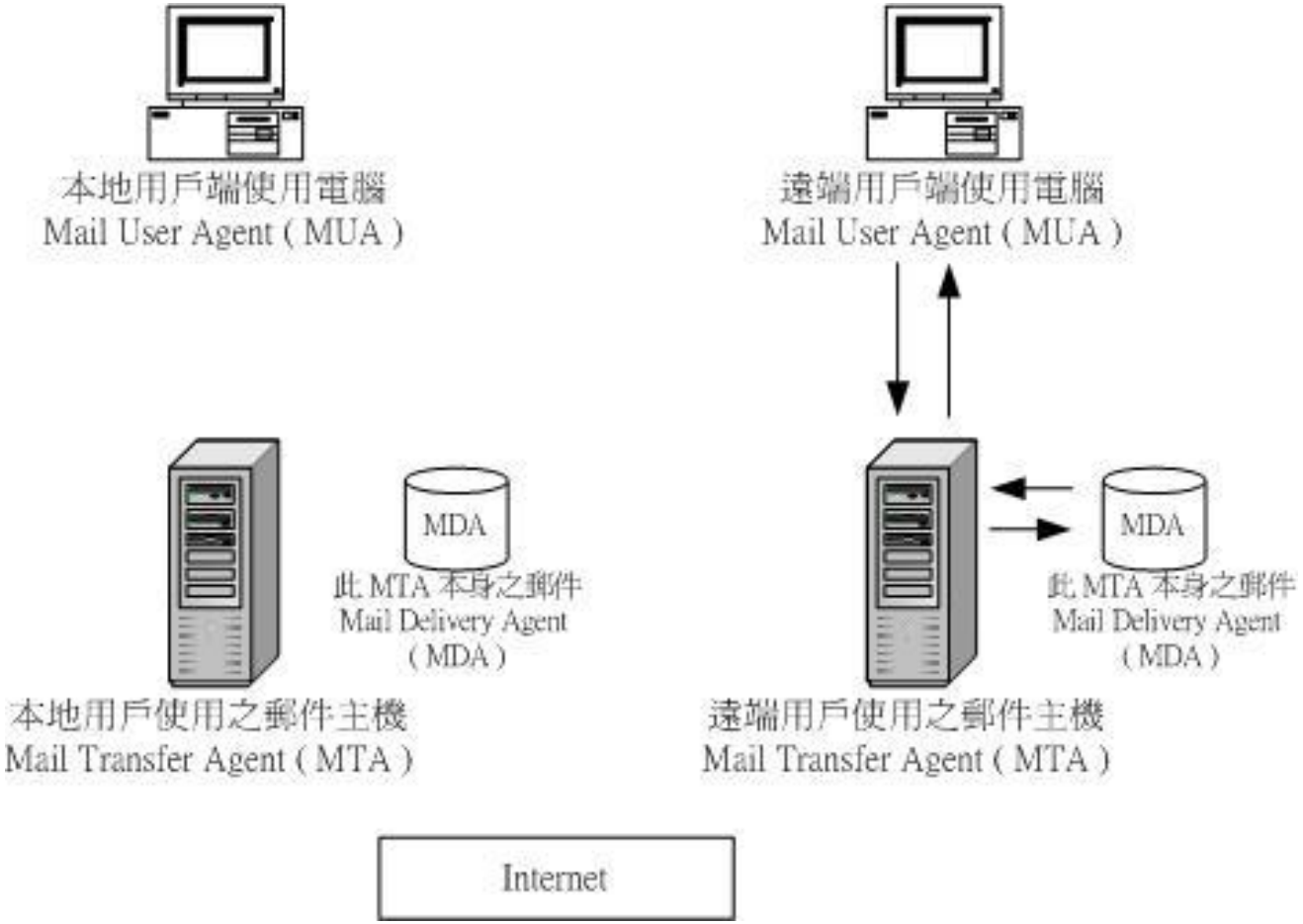


電子郵件以郵件主機寄送信件示意圖

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

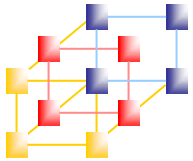
收信的動作 (1/2)



用戶端收受郵件主機的電子郵件示意圖

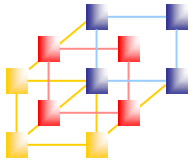
收信的動作 (2/2)

- 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。



Quiz 5

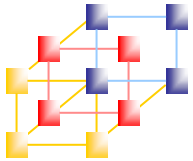
- Gmail
  - 包含哪些角色？
    - MUA
    - MTA
    - MDA
    - MailBox
    - …?
- 請將答案寫在紙條上，下課收來講桌。
- ((請記得寫上班級姓名學號



番外篇：DNS是怎麼回事？

- 申請網域名稱
  - Godaddy、Gandi →付錢
- 架設Domain Server或
- 正查：mail1.asimon.idv.tw → 118.***.***.72
- 反查：118.***.***.72 → mail1.asimon.idv.tw

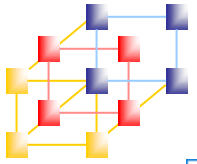
C:\> nslookup www.asimon.idv.tw



DNS的Records

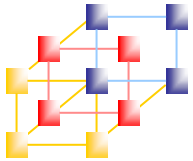
- MX Record
  - 哪一台機器負責這個Domain的收送信服務
- A Record
  - 如果沒有設定MX Record則看對應的A Record
- PTR Record
  - 這個IP反查回的Domain是誰
- SPF Record
  - 這個Domain應該從哪些IP發信
- Domain Keys
  - 簽章

DNS的Records長怎樣



root@

```
 GNU nano 1.3.12                File:

$ORIGIN .
$TTL 600        ; 10 minutes
asimon.idv.tw                           IN SOA  dns1.asimon.idv.tw. root.asimon.idv.tw (
                                                2017053029      ; serial
                                                28800           ; refresh (8 hrs)
                                                7200            ; retry   (2 hrs)
                                                1209600         ; expire  (2w)
                                                86400           ; minimum (1d)
                                                )

                                        NS      dns1.asimon.idv.tw.
                                        NS      dns2.asimon.idv.tw.
                                        A       [redacted].192.72
                                        MX      0 asimon.idv.tw.
                                        MX      10 mail1.asimon.idv.tw.
                                        MX      20 mail2.asimon.idv.tw.

                                        TXT "v=spf1 a:asimon.idv.tw a:mail1.asimon.idv.tw a:m
_dmarc.asimon.idv.tw                    TXT "v=DMARC1; p=reject ;pct=100; rua=mailto:asimon@a$
asimon._domainkey.asimon.idv.tw TXT "v=DKIM1; k=rsa; p=[redacted]

$ORIGIN asimon.idv.tw.

dns1                                    A       [redacted].192.72
dns2                                    A       [redacted]194.152
mail1                                   A       [redacted].192.72
mail2                                   A       [redacted]194.152

                                        A       [redacted].192.72

^G Get Help   ^O WriteOut   ^R Read File   ^Y Prev Page   ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is    ^V Next Page   ^U UnCut Text ^T To Spell
```



收發電子郵件和DNS的關係

大補帖

- Send Mail： 尋找收件人的Dest. IP Address
  - 送信時的DNS查詢MX Record
  - 送信時的DNS查詢A Record
- Receive Mail：確認Sender的信任度
  - 收信時的DNS查詢PTR Record
  - 收信時的DNS查詢SPF Record
  - 收信時的DNS查詢Domain Keys

看看Gmail怎麼做

- 加密、簽章方式

- 確認寄件人來源的**可信任程度**(原始郵件頁面)

郵件 ID	<031301d47340$39818e00$ac84aa00$@asimon.idv.tw>
建立時間：	2018年11月3日 下午2:41 (傳輸時間：7 秒)
寄件者：	"張舜賢(ASIMON)" <asimon@asimon.idv.tw> 使用 Microsoft Outlook 16.0
收件者：	
主旨：	
SPF：	PASS，IP .72 瞭解詳情
DKIM：	'PASS'，網域 .idv.tw。 瞭解詳情
DMARC：	'PASS'。 瞭解詳情

DKIM怎麼設-讓我們來問神
Google: DKIM check

SELECTOR

*Selectors enable a single domain to have multiple keys. Some domains, like Twitter and eBay, use "**dkim**". Google Apps domains typically use "**google**". Others simply use "**default**". Enter yours here. (Note: Do not include "_domainkey")*

asimon

DOMAIN

Base Domain Name. (e.g. example.com)

asimon.idv.tw

CHECK KEY

DNS QUERY: **asimon._domainkey.asimon.idv.tw**
QUERY STATUS: **Success**
TXT RECORD:

```
"v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDFatRAQURRSvGKI0aC/VLvutWCk+1EYCKUDRXQKD52uxtcYpvXrJ6MpnHe
n/+dpovRQAggfaYQIDAQAB"
```

KEY LENGTH (BITS): **1024**
VERSION: **DKIM1**
KEY TYPE: **rsa**

Source: https://protodave.com/tools/dkim-key-checker/

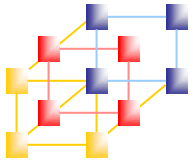
SPF怎麼設-讓我們來問神
Google: spf record check


```
v=spf1 a:asimon.idv.tw a:mail1.asimon.idv.tw a:mail2.asimon.idv.tw ip4:[redacted]192.71 ip4:[redacted]192.72 ip4:[redacted]194.152/29 mx ptr
```

Prefix	Type	Value	PrefixDesc	Description
v	version	spf1		The SPF record version
+	a	asimon.idv.tw	Pass	Match if IP has a DNS 'A' record in given domain
+	a	mail1.asimon.idv.tw	Pass	Match if IP has a DNS 'A' record in given domain
+	a	mail2.asimon.idv.tw	Pass	Match if IP has a DNS 'A' record in given domain
+	ip4	[redacted]192.71	Pass	Match if IP is in the given range
+	ip4	[redacted]192.72	Pass	Match if IP is in the given range
+	ip4	[redacted]94.152/29	Pass	Match if IP is in the given range
+	mx		Pass	Match if IP is one of the MX hosts for given domain name
+	ptr		Pass	Match if IP has a DNS 'PTR' record within given domain
	all		SoftFail	Always matches. It goes at the end of your record.

	Test	Result	
!	SPF Type PTR Check	Type PTR is discouraged	More Info
✓	DNS Record Published	DNS Record found	
✓	SPF Record Published	SPF Record found	
✓	SPF Record Deprecated	No deprecated records found	
✓	SPF Multiple Records	Less than two records found	
✓	SPF Contains characters after ALL	No items after 'ALL'.	
✓	SPF Syntax Check	The record is valid	
✓	SPF Included Lookups	Number of included lookups is OK	
✓	SPF Void Lookups	Number of void lookups is OK	
✓	SPF Exceeds Maximum Character Limit	String lengths are OK.	

Source: https://mxtoolbox.com/spf.aspx

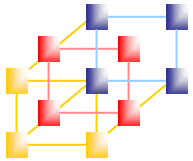


我們的Mail Server安不安全

- Online工具的使用
  - Google: nslookup online
    - 看看查出來有沒有不同？！
  - Google: dns report
    - 查詢各種Record是否有設定正確
  - Google: smtp check
    - 動態測試smtp server的狀態，他幫你測
  - Google: mail-tester
    - 另一種測試方法，寄信給他
  - Google: Sending Reputation
    - 評分查詢

垃圾郵件的來源

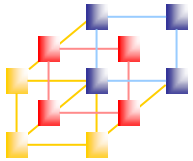
- 在網際網路開始時就有垃圾郵件。
- 垃圾郵件也被稱作是“未經收信人許可的商業郵件” 或“未經收信人許可的大量郵件” 。



電子郵件的格式與協定

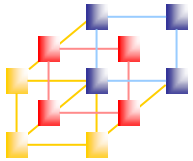
大補帖

- 信件格式
  - TEXT(文字信件格式)
  - MIME(多媒體信件格式)
  - S/MIME(安全的多媒體信件格式)
- 通信協定
  - SMTP
  - ESMTP
  - POP3
  - IMAP4



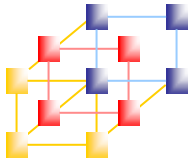
電子郵件的安全

- 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



為什麼電子郵件不安全？

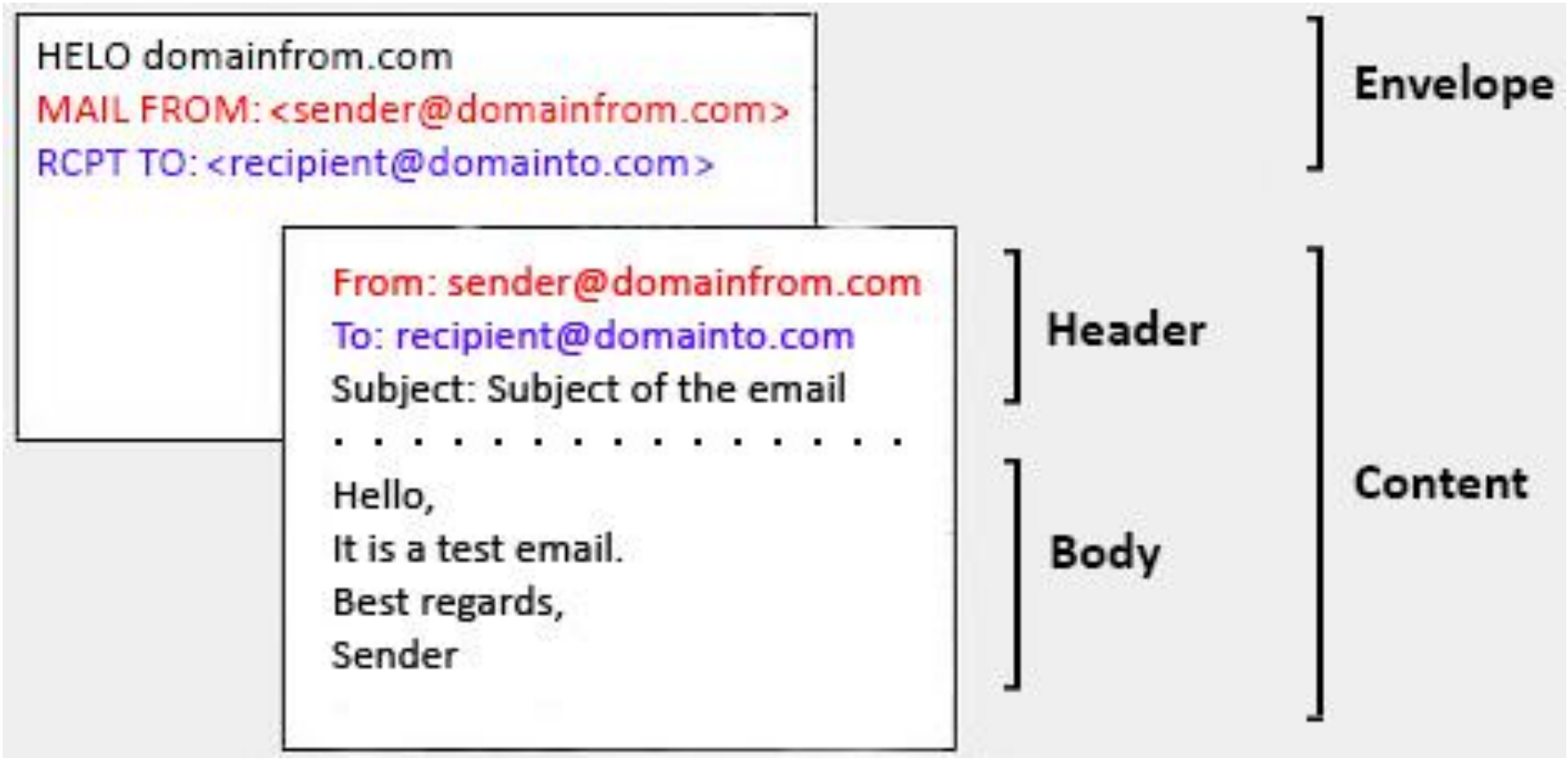
- 通訊協定
  - SMTP → 全明文傳輸
  - **ESMTP → 支援SSL/TLS傳輸加密**
  - POP3 →全明文傳輸
  - IMAP4 →全明文傳輸
- 信件格式
  - TEXT(文字信件格式) → 全明文傳輸
  - MIME(多媒體信件格式) → 全明文傳輸
  - S/MIME(安全的多媒體信件格式) → 很很很少見



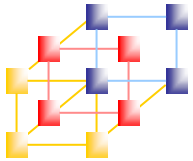
為什麼電子郵件不安全？

- 通訊協定
  - SMTP → 全明文傳輸
  - **ESMTP → 支援SSL/TLS傳輸加密**
  - POP3 →全明文傳輸
  - IMAP4 →全明文傳輸
- 信件格式
  - TEXT(文字信件格式) → 全明文傳輸
  - MIME(多媒體信件格式) → 全明文傳輸
  - S/MIME(安全的多媒體信件格式) → 很很很少見

SMTP+TEXT郵件格式



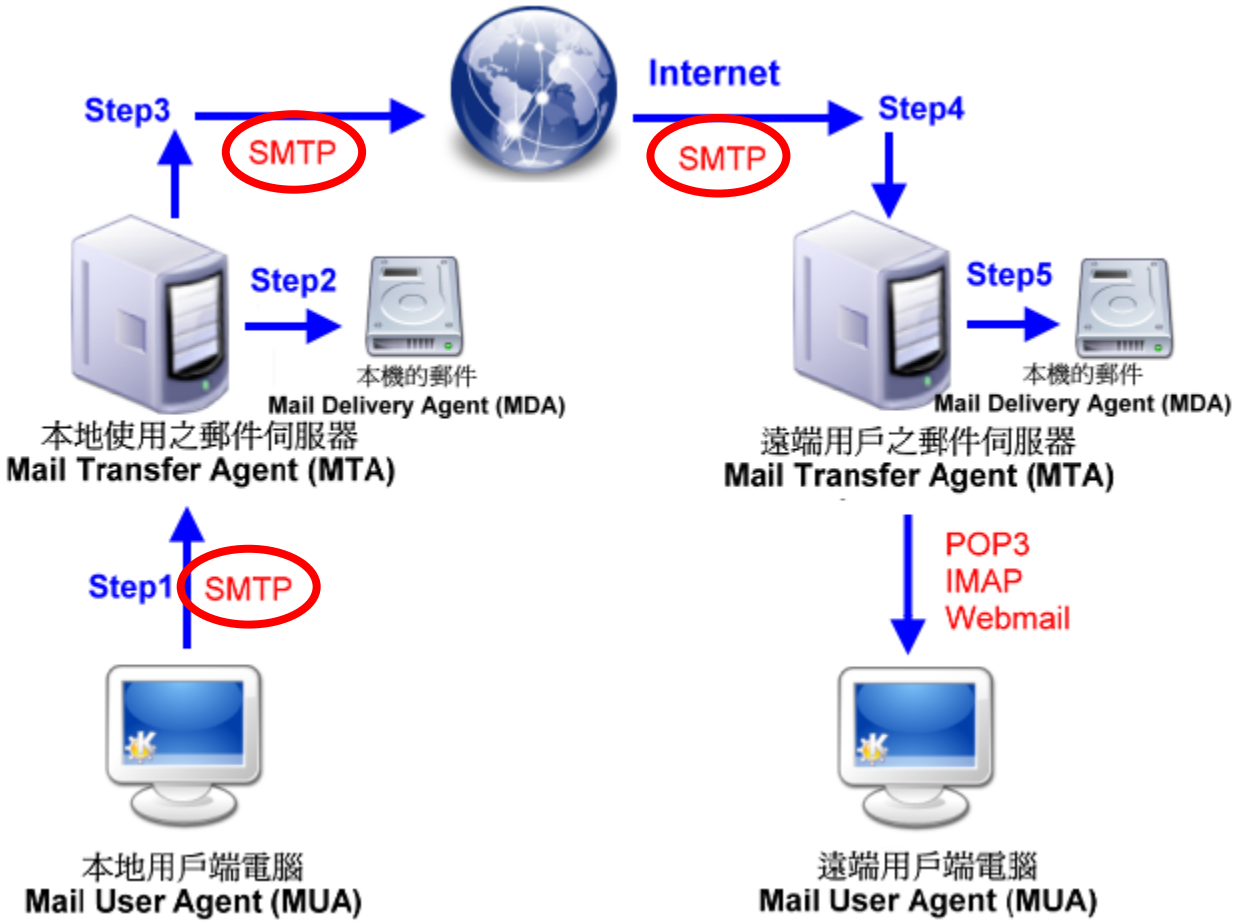
https://itgeeknotes.blogspot.com/2017/07/email-eliminate-confusion-between.html



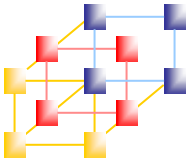
SMTP

- **Simple** Mail Transfer Protocol → 真的很簡單
- 通常使用TCP 25連接埠
- 明碼傳輸
- 使用telnet就可以快速模擬
- Sendmail、Postfix

電子郵件系統運作



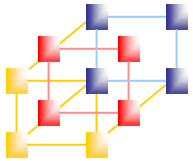
https://www.twbsd.org/cht/book/ch16.htm



SMTP指令

大補帖

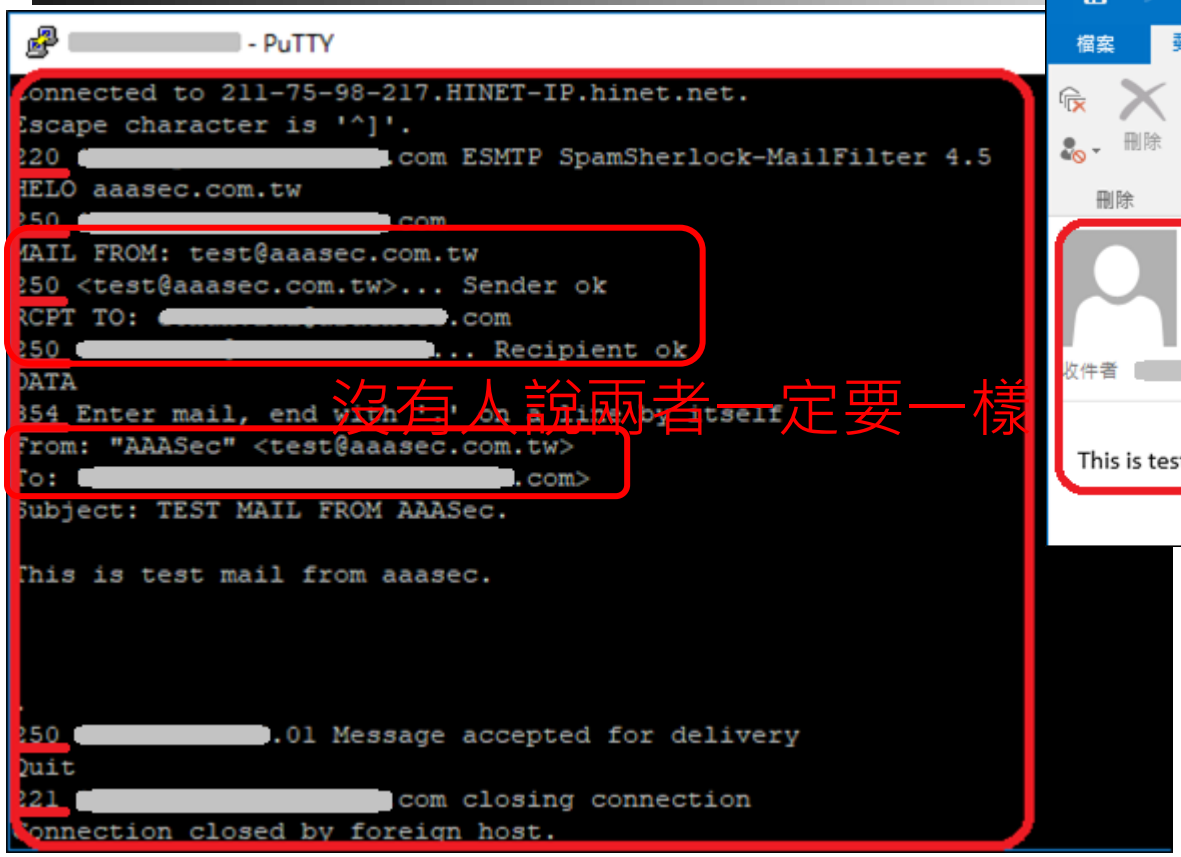
- HELO – Say Hello，開始進行SMTP通訊
- MAIL – 寄件者信箱
- RCPT – 收件者信箱
- DATA– 開始傳送信件內容
- RSET – 中斷傳送並且重置所有緩衝區資料
- NOOP– 無動作，防止斷線用
- QUIT – 確認信件已送出並中斷連線
- VRFY– 檢查帳號是否存在
- EXPN– 檢查群組帳號是否存在，並列出成員

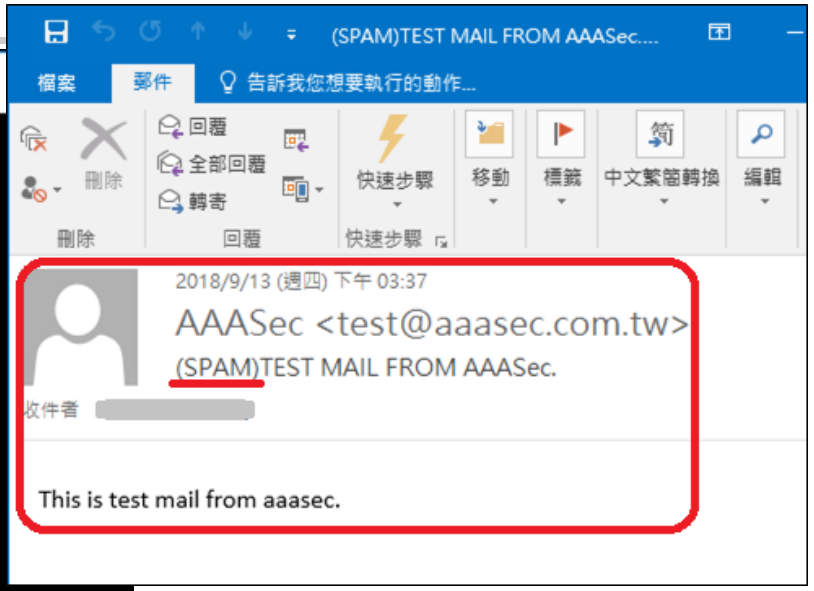


SMTP回應代碼

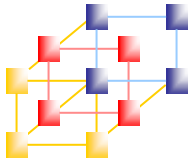
- 2** - 成功
- 3** - 接受且有其他回應資訊
- 4** - 拒絕，錯誤狀態是暫時的
- 5** - 拒絕

SMTP範例



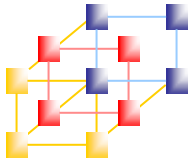


沒有人說兩者一定要一樣



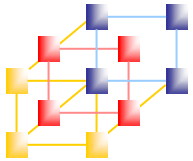
SMTP的缺點

- 前一頁就提到一個 – 可以偽冒發信者
- 沒辦法驗證身分 – 無法用帳號密碼管控全限
  - 限制MUA的IP Address
  - 限制發信者的Mail Address (但可以偽冒)
  - 容易產生Open Relay問題 (？)
- 全程都**沒有**加密



ESMTP

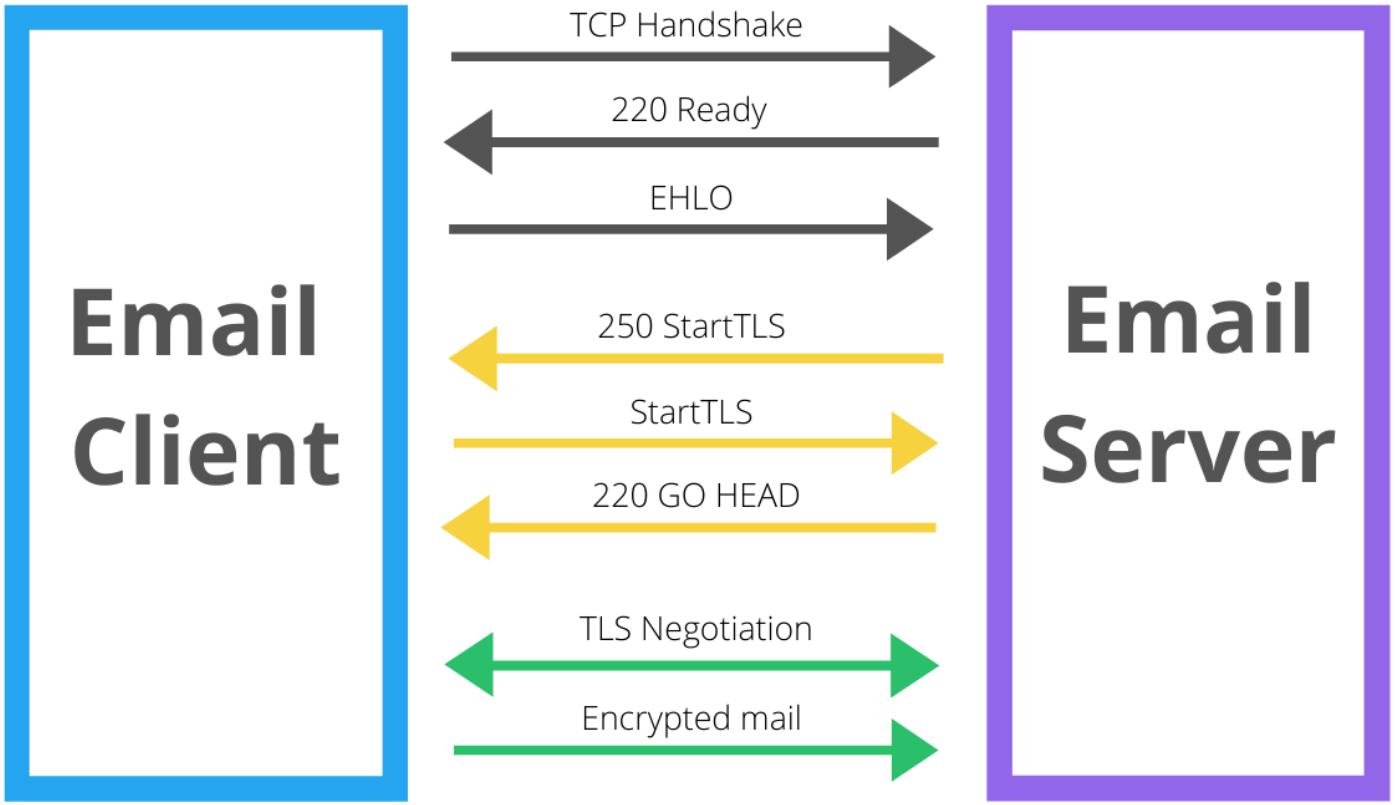
- Extended SMTP
  - HELO → EHLO xD
  - AUTH / AUTH-LOGIN (使用者登入驗證)
  - STARTTLS (TLS/SSL傳輸加密)
  - SIZE (限制傳送信件的大小)
  - TURN (Server / Client角色互換，減少連線次數)
  - DSN (Delivery Service Notification) (回覆信件狀態)
    - 回條到底是送還是不送呢？

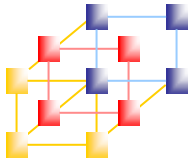


ESMTP怎麼驗證使用者

- https://ssorc.tw/4499/%E7%94%A8-telnet-%E6%B8%AC%E8%A9%A6%E9%83%B5%E4%BB%B6%E5%B8%B3%E5%AF%86%E5%8F%8A%E6%94%AF%E6%8F%B4%E7%9A%84%E8%AA%8D%E8%AD%89%E6%96%B9%E5%BC%8F/

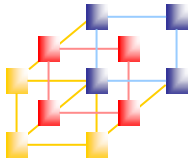
ESMTP運作方式


Email Client
TCP Handshake
220 Ready
EHLO
250 StartTLS
StartTLS
220 GO HEAD
TLS Negotiation
Encrypted mail
Email Server



SMTP v.s. ESMTP

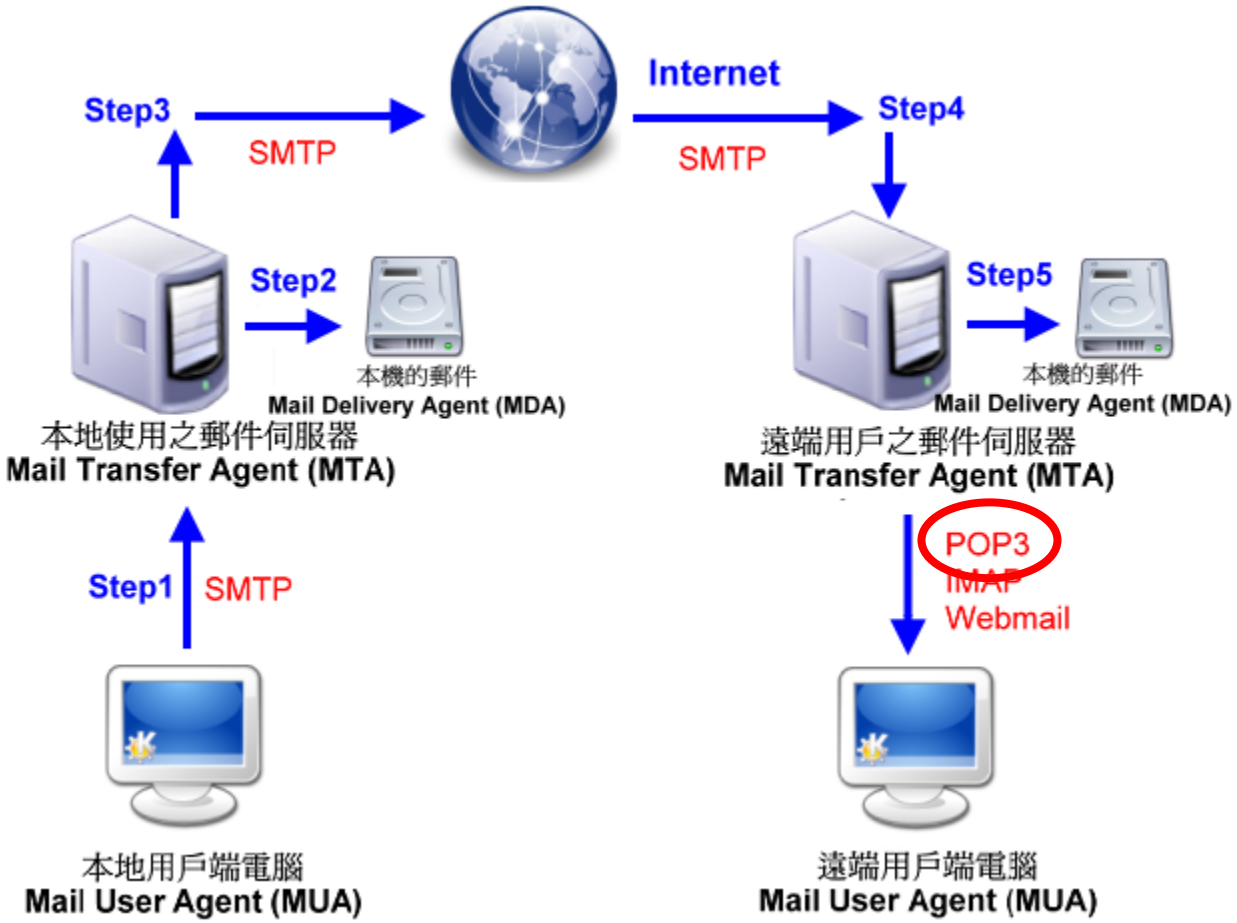
	SMTP	ESMTP
字面上	簡單的 郵件 傳輸 協定	延伸的 簡單 郵件 傳輸 協定
用途	發信、轉信協定	發信、轉信協定
連線方式	TCP三向交握	TCP三向交握
歡迎指令	HELO	EHLO
要求回條	無	可
加密傳輸	無	SSL/TLS
雙向驗證	無	帳號密碼



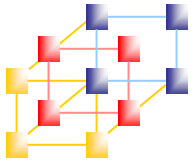
POP3

- 此協定主要用於支援使用客戶端遠端管理在伺服器上的電子郵件
- Post Office Protocol - Version 3

電子郵件系統運作



https://www.twbsd.org/cht/book/ch16.htm

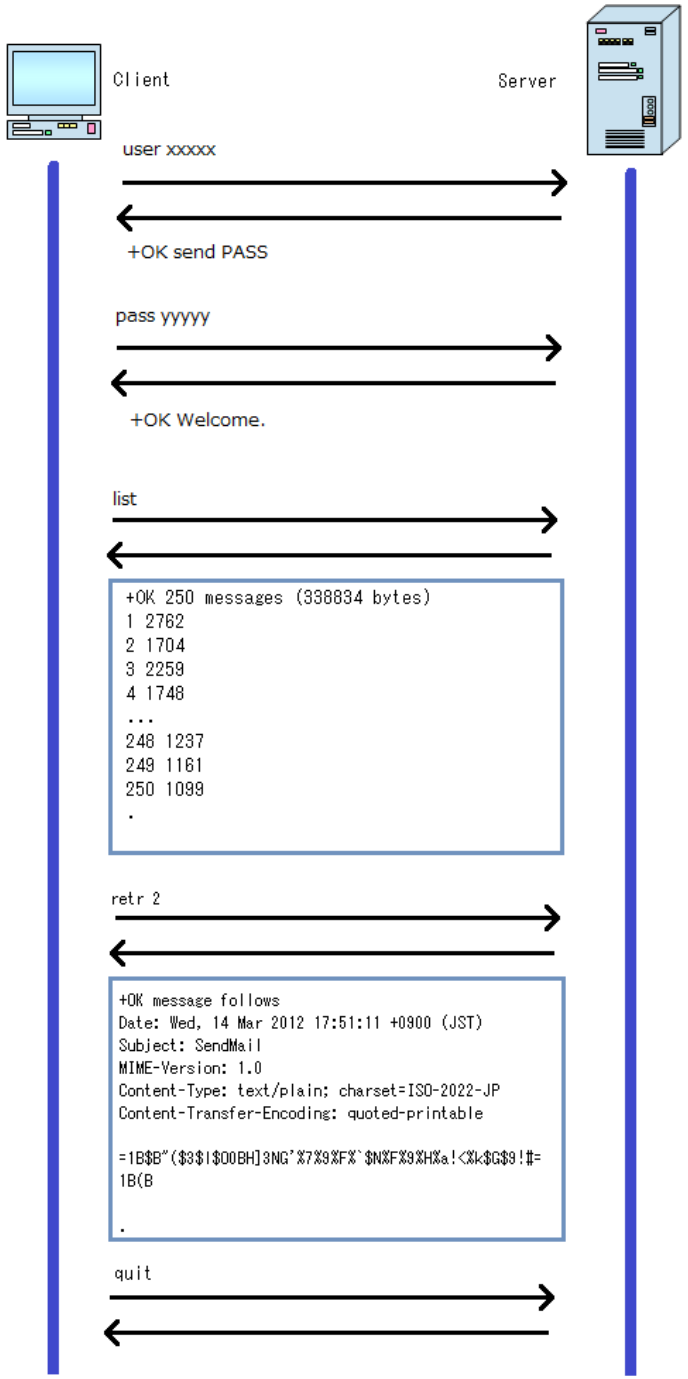


POP3

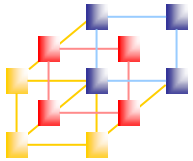
- 原始版本沒有提供加密功能
  - 通常使用TCP 110
- 提供了SSL/TLS加密的POP3協定被稱為**POP3S**
  - 通常使用TCP 995
- POP支援離線郵件處理。其具體過程是：
  - 郵件傳送到伺服器上，
  - MUA連接伺服器，並下載所有未閱讀的電子郵件
  - 將郵件從郵件伺服器端送到個人終端機器上。一旦郵件下載，郵件伺服器上的郵件將會被刪除。
  - 目前的POP3郵件伺服器大都可以「只下載郵件，伺服器端並不刪除」，也就是改進的POP3協定。

Wikipedia

POP3範例



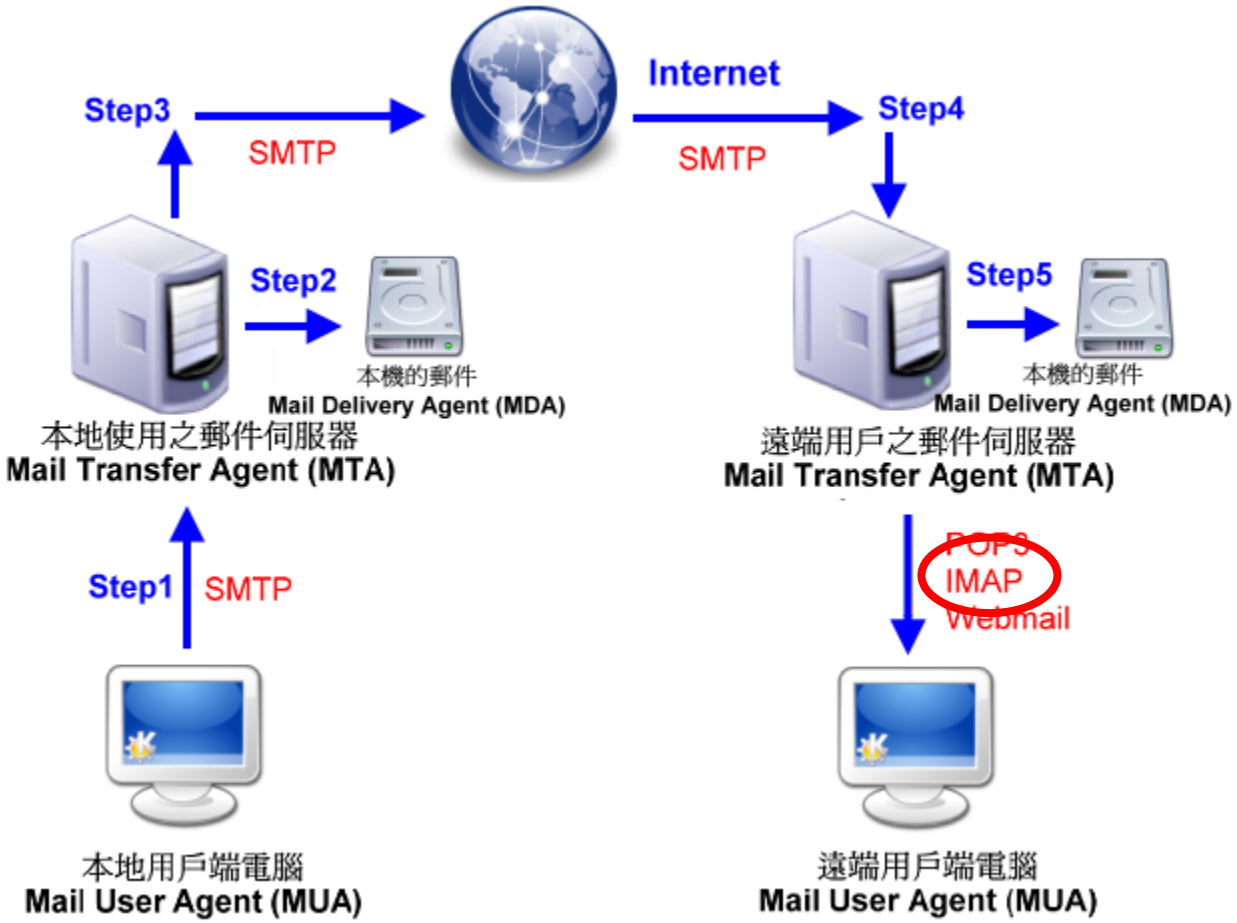
https://www.codeproject.com/



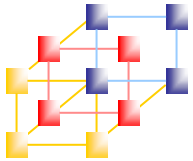
IMAP4

- Internet Message Access Protocol (IMAP)
- 以前稱作互動郵件存取協定
- 是一個應用層協定，用來從MUA（如Microsoft Outlook、Outlook Express、Foxmail、Mozilla Thunderbird）存取遠端伺服器上的郵件。
- 通常使用TCP 143
- 提供了SSL/TLS加密的IMAP協定被稱為**IMAPS**
  - 通常使用TCP 993

電子郵件系統運作



https://www.twbsd.org/cht/book/ch16.htm



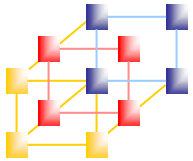
IMAP4的優勢

- 更快的回應時間：批次下載 v.s. 隨看隨載
- 支援多個裝置：信收下來就沒 v.s. 在信箱同步
- 使用者無需下載附件，便可以瀏覽訊息內容或者瀏覽正在取得的內容
- 支援伺服器檢視當前的資訊狀態。
  - 是否被讀取
  - 回覆或者刪除

  → 在伺服器上供其他設備同步
- 存取多個電子信箱
- 在伺服器端搜尋電子郵件
- 良好的擴充機制

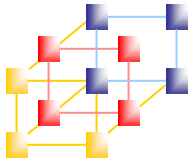
1) 某些MUA也提供暫存與索引功能，所以可以有機會離線搜尋
2) 資料還是以伺服器上為主，備份容易

Wikipedia



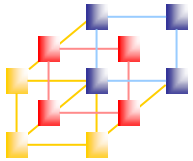
POP3 v.s. IMAP4

	POP3	IMAP4
常用埠	TCP 110 / TCP 995 (SSL)	TCP 143 / TCP 993 (SSL)
用途	收信	收信
預覽時	下載全部資料至MUA	依需求下載少許 (日期、主旨、寄/收件人、大小)
特性	預設不保留備份於伺服器	主要資料儲存於伺服器
優勢	資料一手掌握	資料連網即可取得
問題	終端設備備份	伺服器儲存與運算瓶頸
離線使用	完全沒問題	需依賴MUA的暫存功能



為什麼電子郵件不安全？

- 通訊協定
  - SMTP → 全明文傳輸
  - **ESMTP → 支援SSL/TLS傳輸加密**
  - POP3 →全明文傳輸
  - IMAP4 →全明文傳輸
- 信件格式
  - TEXT(文字信件格式) → 全明文傳輸
  - MIME(多媒體信件格式) → 全明文傳輸
  - S/MIME(安全的多媒體信件格式) → 很很很少見



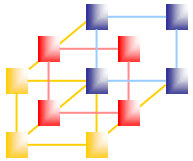
信件標頭格式

大補帖

- From: asimon@asimon.idv.tw

  有一個空格

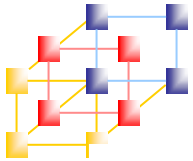
- 一些常見的標頭
  - From: 寄件人信箱
  - To: 收件人信箱
  - Date: 發信時間
  - Subject: 信件主旨
  - Message-Id: 信件唯一的編號
  - Received: 信件經過的路徑(由下往上看)
  - Return-Path: 退信的信箱
  - Reply-To: 回覆的信箱



標頭到底長怎樣

- 如何用標頭發現詐騙信的真相？
  - 這是一封最近很流行的詐騙/勒索信，我有好幾封
    - **Change your password immediately. Your account has been hacked.**

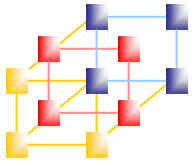
```
Return-Path: <asimon@asimon.idv.tw>
X-Original-To: asimon@asimon.idv.tw
Delivered-To: asimon@asimon.idv.tw
Received: from cpc80991-perr18-2-0-cust340.19-1.cable.virginm.net (cpc80991-perr18-2-0-cust340.19-1.cable.virginm.net [94.173.113.85])
        by mail1.asimon.idv.tw (Postfix) with ESMTP id 462214CB36A
        for <asimon@asimon.idv.tw>; Mon,  5 Nov 2018 06:03:48 +0800 (CST)
DKIM-Filter: OpenDKIM Filter v2.11.0 mail1.asimon.idv.tw 462214CB36A
Message-ID: <0E41BEFF0BF1004A05FABB4FB5440E41@1HSHC5PJ14>
From: <asimon@asimon.idv.tw>
To: <asimon@asimon.idv.tw>
Subject: Change your password immediately. Your account has been hacked.
Date: 4 Nov 2018 20:50:46 -0100
MIME-Version: 1.0
Content-Type: text/plain;
        charset="ibm852"
Content-Transfer-Encoding: 8bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Windows Live Mail 15.4.3508.1109
X-MimeOLE: Produced By Microsoft MimeOLE V15.4.3508.1109
```



TEXT格式信件長怎樣


```
S: 220 smtp2go.com ESMTP Exim
C: HELO mydomain.com
S: 250 Hello mydomain.com
C: MAIL FROM:<sender@mydomain.com>
S: 250 Ok
C: RCPT TO:<recipient@anotherdomain.com>
S: 250 Accepted
C: DATA
S: 354 Enter message, ending with "." on a line by itself
C: Subject: sample message
C: From: sender@mydomain.com
C: To: recipient@anotherdomain.com
C:
C: Greetings,
C: Typed message (content)
C: Goodbye.
C: .
S: 250 OK
C: QUIT
S: 221 www.sample.com closing connection
```

https://www.smtp2go.com/

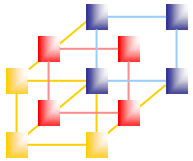


為什麼會有MIME

- 為什麼會有圖文並茂的信件？！

→ MIME (Multipurpose Internet Mail Extension)

- MIME定義的新標頭：
  - MIME-Version: 1.0 → 版本
  - Content-Type: Text/Plain: Charset=UTF-8 → 格式
  - Content-Type: text/html; charset="utf-8" → 格式
  - Content-Transfer-Encoding: base64 → 編碼方式



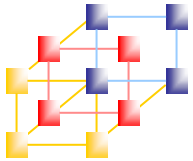
Content-Type

- Text – 文字
- Image – 圖片 (gif、jpeg)
- Audio – 聲音
- Video – 影片(mpeg)
- Application – 特定應用程式可處理的資訊
- Multipart – 複合式多媒體的信件

標頭到底長怎樣

- 如何用標頭發現詐騙信的真相？
  - 這是一封最近很流行的詐騙/勒索信，我有好幾封
    - **Change your password immediately. Your account has been hacked.**

```
Return-Path: <asimon@asimon.idv.tw>
X-Original-To: asimon@asimon.idv.tw
Delivered-To: asimon@asimon.idv.tw
Received: from cpc80991-perr18-2-0-cust340.19-1.cable.virginm.net (cpc80991-perr18-2-0-cust340.19-1.cable.virginm.net [94.173.113.85])
        by mail1.asimon.idv.tw (Postfix) with ESMTP id 462214CB36A
        for <asimon@asimon.idv.tw>; Mon,  5 Nov 2018 06:03:48 +0800 (CST)
DKIM-Filter: OpenDKIM Filter v2.11.0 mail1.asimon.idv.tw 462214CB36A
Message-ID: <0E41BEFF0BF1004A05FABB4FB5440E41@1HSHC5PJ14>
From: <asimon@asimon.idv.tw>
To: <asimon@asimon.idv.tw>
Subject: Change your password immediately. Your account has been hacked.
Date: 4 Nov 2018 20:50:46 -0100
MIME-Version: 1.0
Content-Type: text/plain;
        charset="ibm852"
Content-Transfer-Encoding: 8bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Windows Live Mail 15.4.3508.1109
X-MimeOLE: Produced By Microsoft MimeOLE V15.4.3508.1109
```

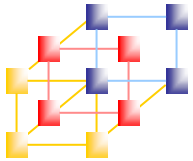


有關Base64

- 常用的編碼方法
  - 編碼不是加密、編碼不是加密、編碼不是加密
  - (很重要，念三遍！！！)
  - 任何人都可以解碼
  - 把Binary Data、圖片或其他複雜的資料轉換為可視字元

MIME的內容

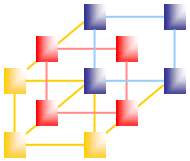
- 文字 <font>
- 圖片連結 <img src=“”>
- 超連結 <a href=“”>



Multipart

- 如果
  - 想要直接在信件中嵌圖片 → 斷網也看得到
  - 想要放圖片又要放動畫 → 不只一種內容
  - 想要夾帶附件 → 除了文字還要附帶檔案

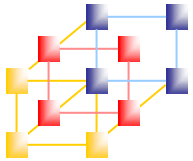
→ Multipart是您的好朋友



Multipart


```
From: "Smith, John" <jsmith@college.edu>
To: "Peter Adams" <peter_adams@hotmail.com>
Subject: CS Mid Term
Date: Fri, 3 Mar 2006 09:08:10 -0500
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="----_=_NextPart_001_01C3AF7F.35820A9B"

Received: from EXCHANGEMAIL.COLLEGE.EDU ([67.251.112.30]) by
bay0-mc10-f2.bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.211); Fri, 3
Mar 2006 06:08:12 -0800
X-Message-Info: JGTYoYF78jEHjJx36Oi8+Z3TmmkSEdPtfpLB7P/ybN8=
Content-class: urn:content-classes:message
X-MimeOLE: Produced By Microsoft Exchange V6.5.7226.0
X-MS-Has-Attach: X-MS-TNEF-Correlator: Thread-Topic: CS Mid Term
Thread-Index: AcY+qoksCm67V+jHSd+jwoRpQ5vCCwAICufp
References: <BAY108-F243FC3114EBD6165216203E9EA0@phx.gbl>
Return-Path: jsmith@college.edu
X-OriginalArrivalTime: 03 Mar 2006 14:08:12.0085 (UTC)
FILETIME=[E827E650:01C63ECB]

This is a multi-part message in MIME format.

------_=_NextPart_001_01C3AF7F.35820A9B
Content-Type: text/plain;
        charset="utf-8"
Content-Transfer-Encoding: base64

RGVhciBTdHVkZW50LA0KIA0KVG9uaWdodCBhZnRlciBvdXIgQ1M1NTMgY2xhc3MgKGF0IDc6MzAg
UE0pIHlvdSBhcmUgaW52aXRlZCB0byB2aXNpdCBvdXIgY29sbGVnZSBJVCBMQU4gQ2VudGVyIGxv
Y2F0ZWQgaW4gdGh1IFNUSCBidW1sZGluZyBvbiB0aGUgZmlyc3QgZmxvb3IgbmVhci4=

------_=_NextPart_001_01C3AF7F.35820A9B
Content-Type: text/html;
        charset="utf-8"
Content-Transfer-Encoding: base64

PCFET0NUWVBFIEhUTUwgUFVCTElDICItLy9XM0MvL0RURCBIVE1MIDQuMCBUcmFuc2l0aW9uYWwv
L0VOIj48SFRNTD48SEVBRD48TUVUQSBIVFRQLUVRVU1WPSJDb250ZW50LVR5cGUiIENPTlRFTlQ9
InRleHQvaHRtbDsgY2hhcnNldD11dGYtOCI+PC9IRUFEPjxCT0RZPjxESVY+RGVhciBIdHVkZW50
LDwvRE1=
```

https://www.researchgate.net/

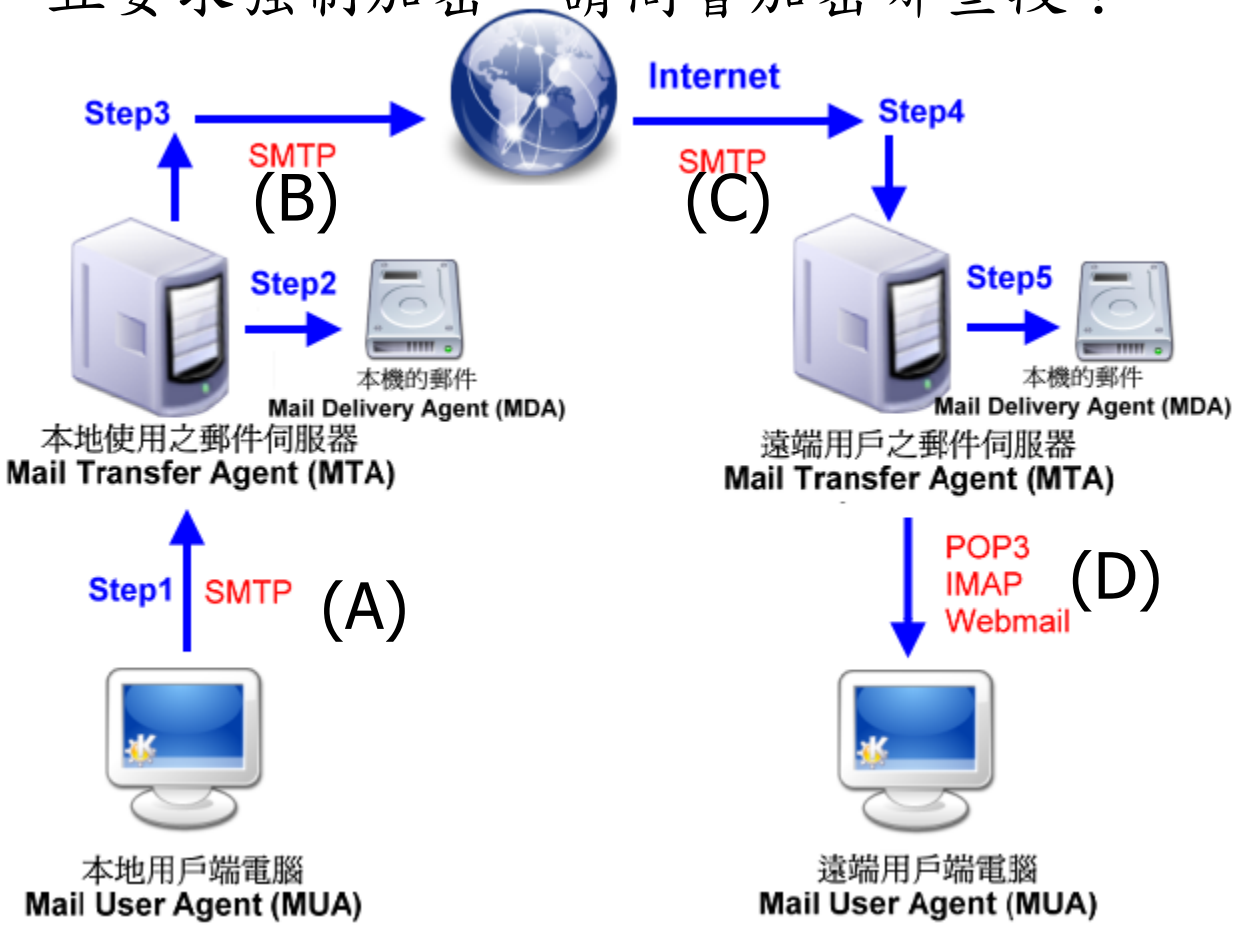


但是...

- 內容越豐富
- 價值越高
- 越容易被OOXX

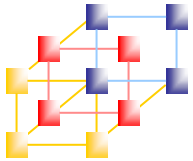
Quiz 6

- 我使用Outlook送信時設定使用ESMTP…
  - 且要求強制加密，請問會加密哪些段？



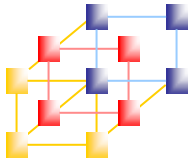
https://www.twbsd.org/cht/book/ch16.htm

(E)：A、B、C、D都加密



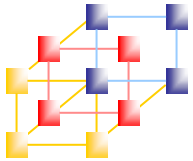
電子郵件的安全

- 電子郵件的弱點
  - Sniffer
  - Security Key



電子郵件的安全

- Sniffer
  - 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



電子郵件的安全

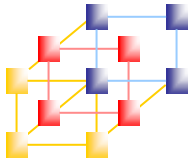
- Security Key
  - 防止電子郵件被未授權的讀取最常用的方法是使用軟體加密
  - 任何沒有解碼器（decoder）或者鑰匙（key）的人無法讀取它

電子郵件的安全

- 有兩個主要的商業加密標準：PGP 和S/MIME

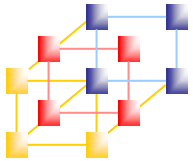
  S/MIME使用PKI和公開金鑰架構替信件加密、簽章

- 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



Outline

- S/MIME
- Pretty good privacy (PGP)
- DomainKeys Identified Mail (DKIM)



Secure/Multipurpose Internet Mail Extension

- Security enhancement to MIME email
  - The original Internet email (RFC822) was text only
  - MIME provided support for varying content types and multi-part messages
  - With encoding of binary data to textual form
  - S/MIME added security enhancements
- S/MIME support in various modern mail agents
  - MS Outlook, Netscape, etc.

MIME 郵件標準 (1/3)

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

From: 志明 <bob@cc.cma.edu.tw>

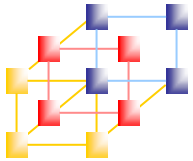
To:春嬌 <alice@pchome.com.tw>

Subject: See you tomorrow

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

Please come to meet me at tomorrow.

<LF>&<CR>



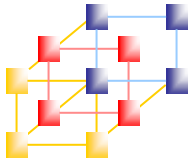
MIME 郵件標準 (2/3)

- 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 (3/3)

- 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 (1/4)

- S/MIME 安全郵件 (Secure/Multipurpose Internet Mail Extension)
  - 訊息摘要：MD5, SHA-1, SHA-256, SHA-512, …
  - 數位簽章：RSA / DSA 演算法
  - 訊息加密：RC2/40 , Triple DES, AES 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 (2/4)

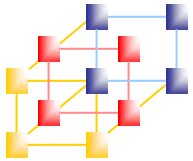
- 安全郵件型態 (2)
  - Application/pkcs-7-mime
    - 信件包裝成 CMS (Cryptographic Message Syntax)
    - 數位信封格式
    - PCKS #7 安全套件

```
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 (3/4)

- 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
```

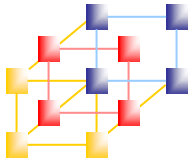


S/MIME 安全郵件 (4/4)

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

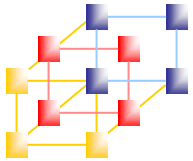
```
Content-Type: multipart/signed;
        protocol="application/pkcs7-signature"; micalg=sha1; boundary=boundary42
--boundary42Content-Type: text/plain
      This is a clear-signed message.
--boundary42
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: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



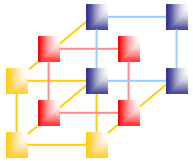
S/MIME functions

- Enveloped data
  - Encrypted content and associated keys
- Signed data
  - Encoded message + signed digest
- Clear-signed data
  - Cleartext message + encoded signed digest
- Signed & enveloped data
  - Nesting of signed & encrypted entities



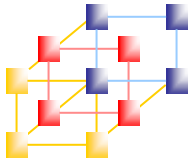
Cryptographic algorithm used in S/MIME

- Create a message digest
  - SHA-1 (MUST), MD5 (SHOULD)
- Encrypt message digest to form digital signature
  - DSS (MUST), RSA (SHOULD; key size 512 ~ 1024)
- Encrypt session key
  - ElGamal (MUST; a variant of Diffie Hellman)
  - RSA (SHOULD)
- Encrypt message
  - 3DES (MUST; recommended), 40-bits RC2 (MUST), AES



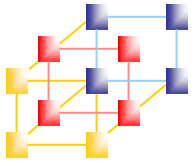
S/MIME messages

Type	Subtype	smime Parameter	Description
Multipart	Signed		A clear-signed message in two parts: one is the message and the other is the signature.
Application	pkcs7-mime	signedData	A signed S/MIME entity.
	pkcs7-mime	envelopedData	An encrypted S/MIME entity.
	pkcs7-mime	degenerate signedData	An entity containing only public-key certificates.
	pkcs7-signature	—	The content type of the signature subpart of a multipart/signed message.
	pkcs10-mime	—	A certificate registration request message.



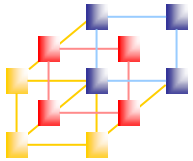
Registration request

- An application or user will apply to a certification authority for a public-key certificate
- The application/pkcs10 S/MIME entity is used to transfer a certificate request
- The certificate request
  - certificationRequestInfo block
    - A name of the certificate subject
    - A bit-stream representation of the user's public key
  - An identifier of the public-key encryption algorithm
  - The signature of the certificationRequestInfo block



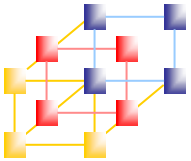
Certificates only message

- Contain only certificate revocation list (CRL)
- The message is an application/pkcs7-mime type/subtype with an smime-type parameter of degenerate



S/MIME certificate processing

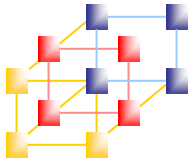
- S/MIME uses X.509 v3 certificates
- Managed using a hybrid of a strict X.509 CA hierarchy & PGP's web of trust
- Each client has a list of trusted CA's certs and own public/private key pairs & certificates
- Certificates must be signed by trusted CA's
- Key management functions on S/MIME user
  - Key generation
  - Registration
  - Certificate storage and retrieval



Certificate authorities

- Have several well-known CA's
- Verisign one of most widely used
  - Verisign issues several types of Digital IDs
  - with increasing levels of checks & hence trust

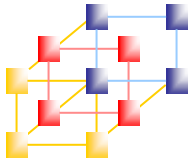
Class	Identity Checks	Usage
1	name/email check	web browsing/email
2+	enroll/addr check	email, subs, s/w validate
3+	ID documents	e-banking/service access



VeriSign public-key certificate classes

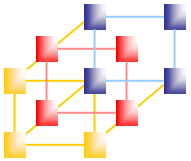
	Summary of Confirmation of Identity	IA Private Key Protection	Certificate Applicant and Subscriber Private Key Protection	Applications implemented or contemplated by Users
Class 1	Automated unambiguous name and E-mail address search	PCA: trustworthy hardware; CA: trust-worthy software or trustworthy hardware	Encryption software (PIN protected) recommended but not required	Web-browsing and certain e-mail usage
Class 2	Same as Class 1, plus automated enrollment information check plus automated address check	PCA and CA: trustworthy hardware	Encryption software (PIN protected) required	Individual and intra- and inter-company E-mail, online subscriptions, password replacement, and software validation
Class 3	Same as Class 1, plus personal presence and ID documents plus Class 2 automated ID check for individuals; business records (or filings) for organizations	PCA and CA: trustworthy hardware	Encryption software (PIN protected) required; hardware token recommended but not required	E-banking, corp. database access, personal banking, membership-based online services, content integrity services, e-commerce server, software validation; authentication of LRAAs; and strong encryption for certain servers

IA Issuing Authority
CA Certification Authority
PCA VeriSign public primary certification authority
PIN Personal Identification Number
LRAA Local Registration Authority Administrator



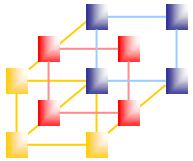
TEXT v.s. MIME v.s. S/MIME

	TEXT	MIME	S/MIME
字面上	純文字	多用途郵件擴展協議	安全的多用途…(略)
用途	信件內容的格式	信件內容的格式	信件內容的格式
內容	文字	文字/網頁/圖片/影音/附檔…	文字/網頁/圖片/影音/附檔…
編碼	無	Base64	Base64
簽章 Only	無	無	可
數位信封	無	無	可



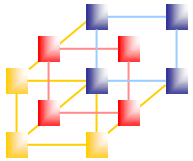
數位信封 v.s. 加密傳輸

	數位信封	加密傳輸
支援協定	S/MIME	ESMTP
保護標的	信件內容	連線行為
雙方來源	明文	明文
雙方信箱	明文	密文
信件內容	密文	密文
保障內容	由簽署者發信，僅收件者可讀	寄、收件伺服器間傳輸安全
不能保護	從標頭取得雙方信箱間有通訊的事實	在雙方伺服器中被偷看或竄改



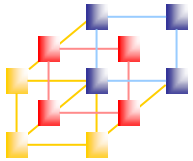
Outline

- S/MIME
- Pretty good privacy (PGP)
- DomainKeys Identified Mail (DKIM)



Pretty good privacy (PGP)

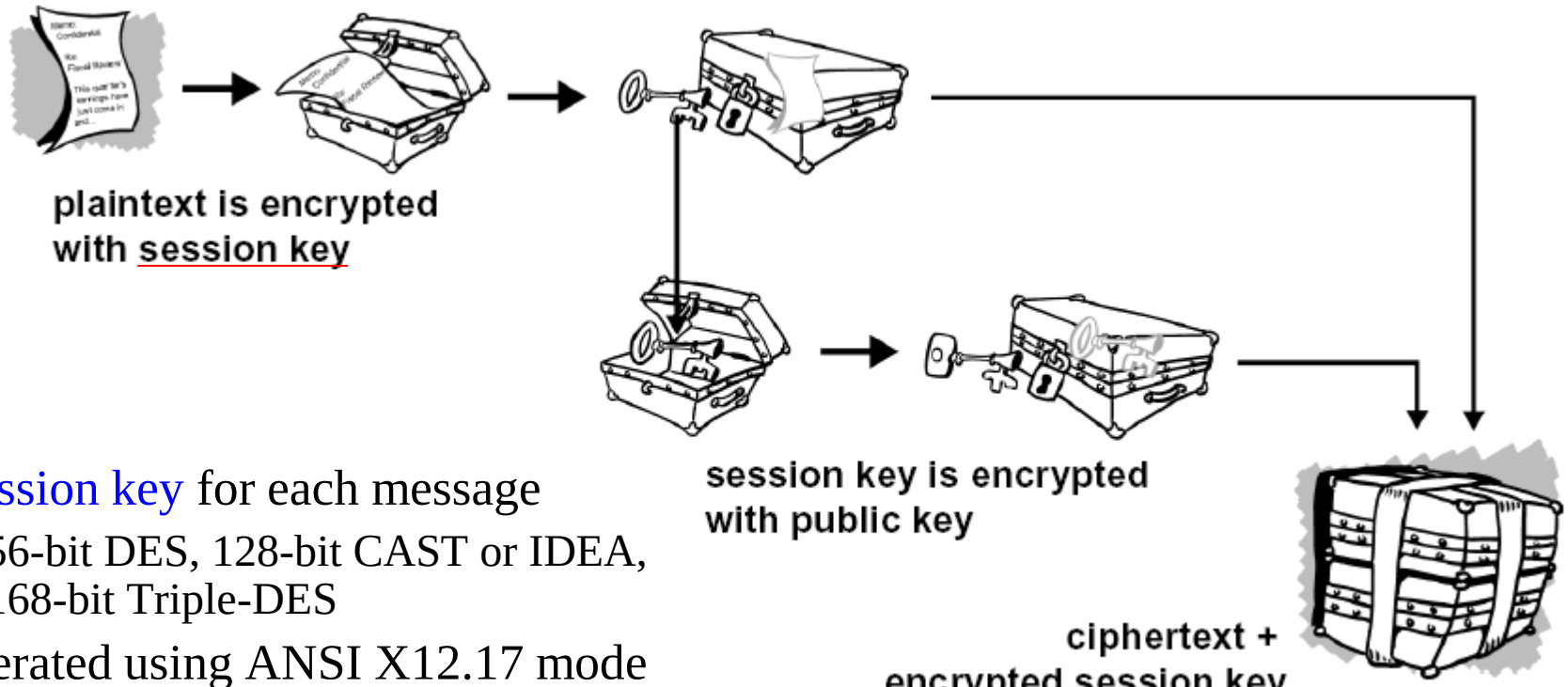
- PGP has grown explosively and is now widely used
- Developed by Phil Zimmermann
- Selected best available crypto algorithms to use
- Integrated into a single program
- Available on Windows, Unix, Macintosh …
- Originally free, now have commercial versions available also



PGP operations

- Authentication
- Confidentiality
- Compression
- E-mail compatibility
- Segmentation

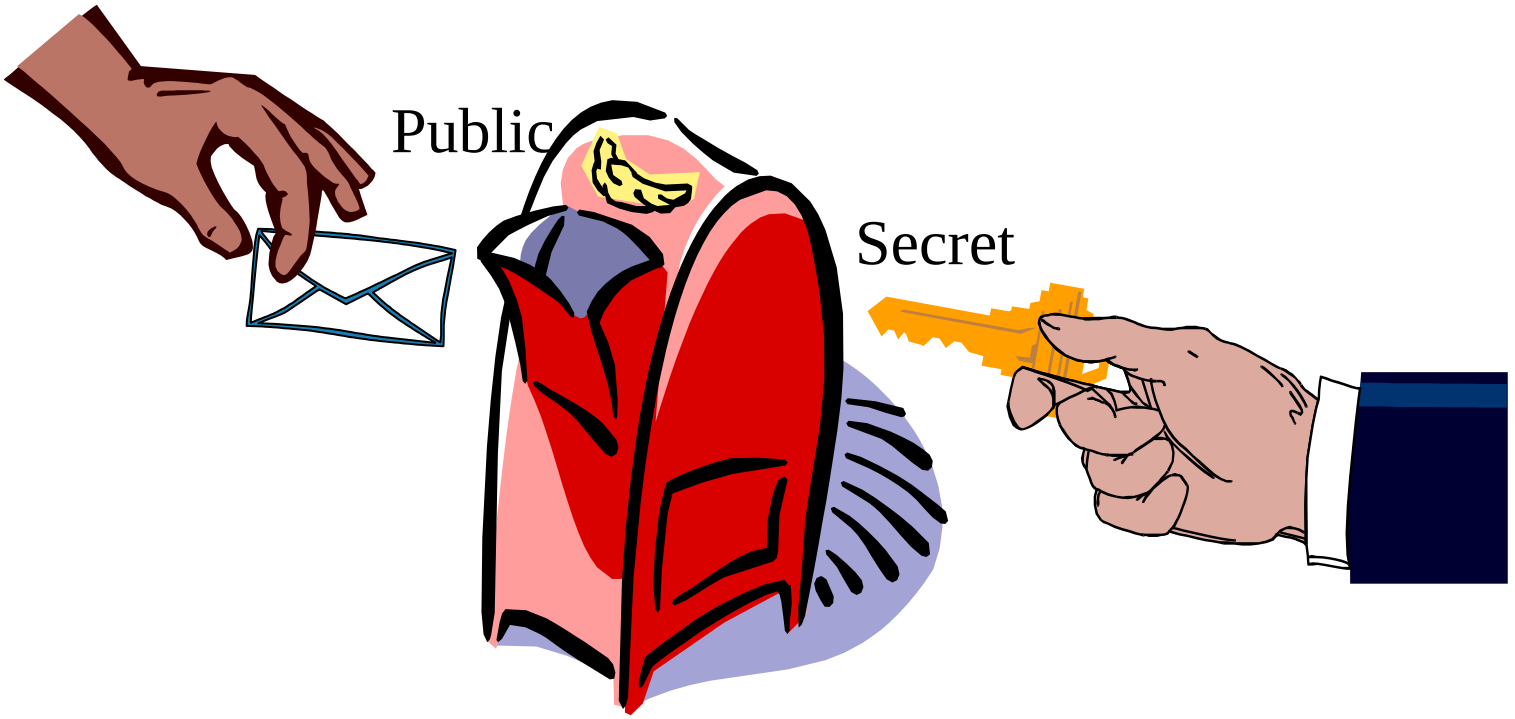
PGP session keys

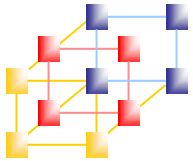


- A session key for each message
  - 56-bit DES, 128-bit CAST or IDEA, 168-bit Triple-DES
- Generated using ANSI X12.17 mode
  - X12: an Electronic data interchange (EDI) and Context Inspired Component Architecture (CICA) standards along with XML schemas which drive business processes globally
- Uses random inputs taken from previous uses and from keystroke timing of user

Conventional cryptosystem

Public Key cryptosystem



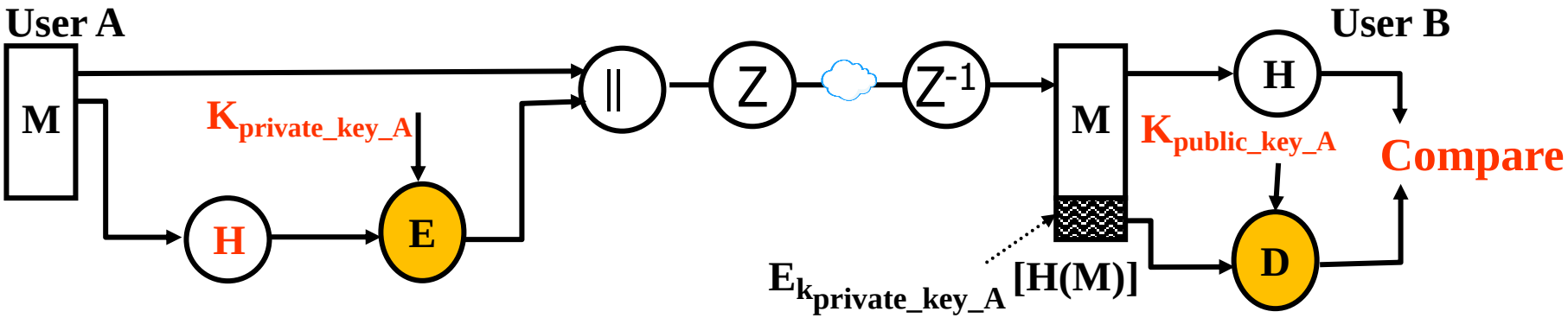


Conventional and public-key

- Advantages of public key cryptosystem
  - Increase security and convenience
  - Provide digital signature
- Disadvantage of public key cryptosystem
  - Speed
  - Vulnerable impersonation
- Public key cryptography is not mean to replace conventional cryptography, but rather to supplement it, to make it more secure
  - Digital envelope
    - Public key system + conventional system

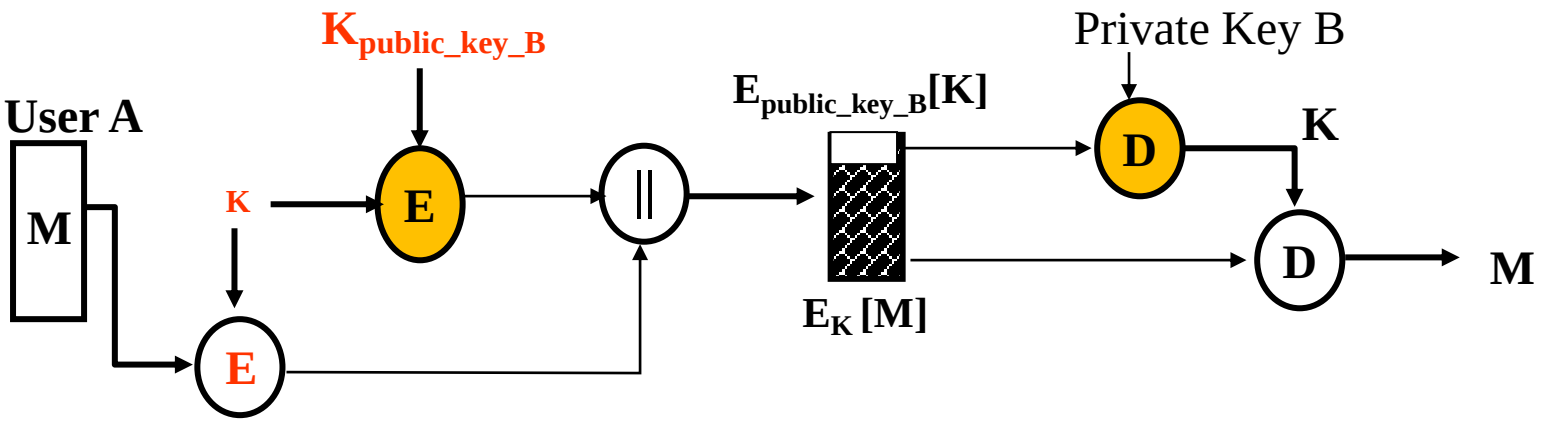
PGP operation -- authentication

The assurance that the communicating entity is the one that it claims to be.

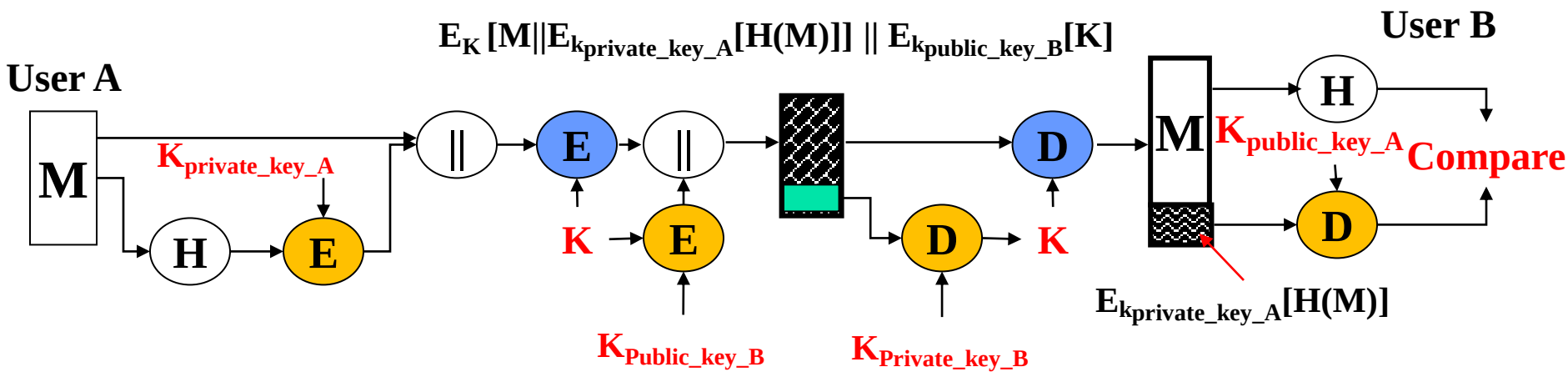


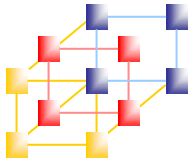
PGP operation -- confidentiality

The protection of data from unauthorized disclosure.



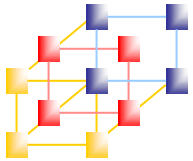
PGP operation – confidentiality and authentication





PGP operation – compression

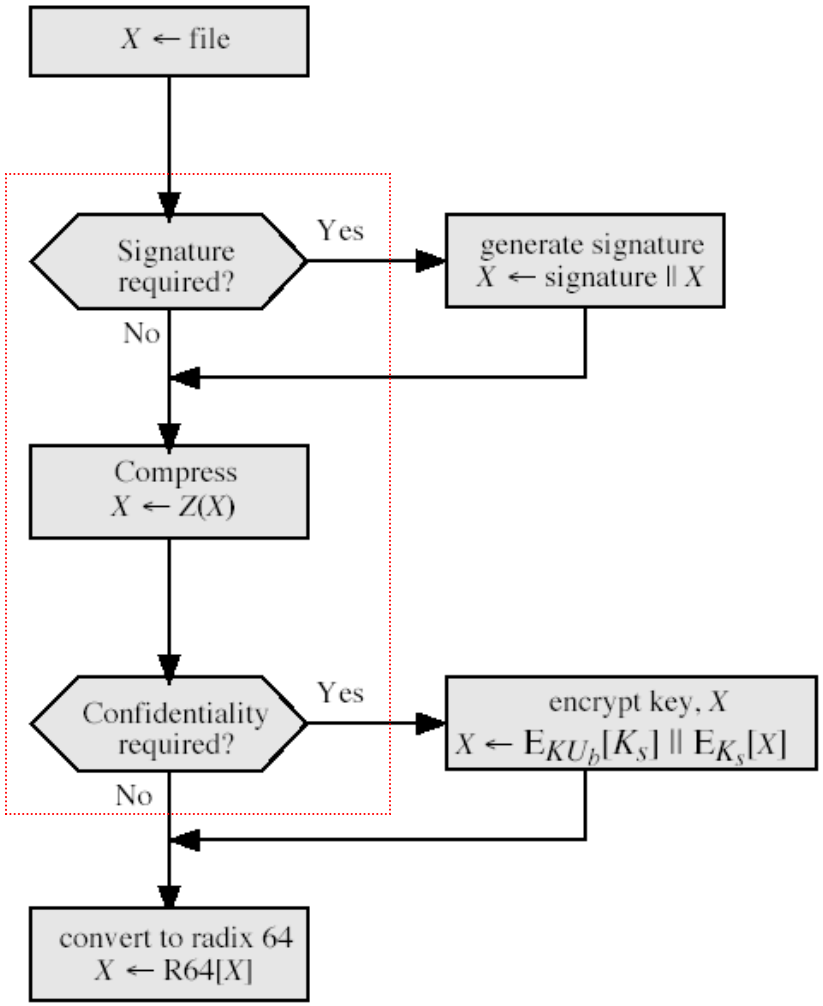
- PGP compresses message after signing but before encrypting
  - Compress -> encryption *v.s.* encryption -> compression?
- Uses ZIP compression algorithm



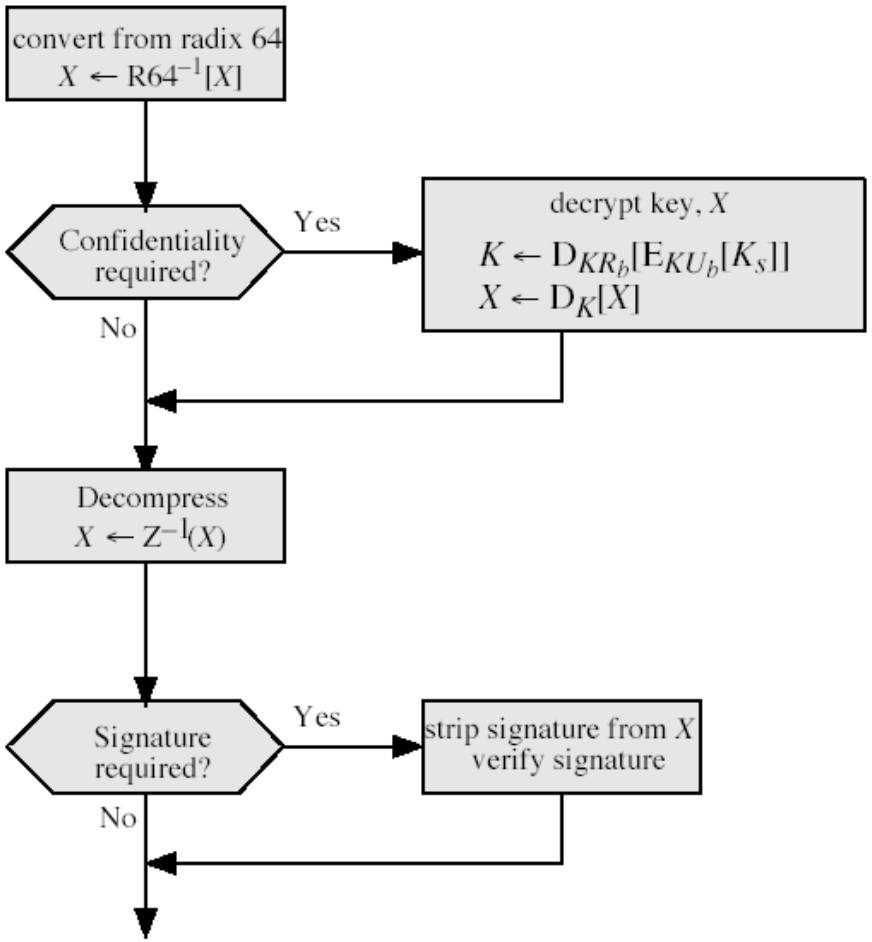
PGP operation – e-mail compatibility

- When using PGP will have binary data to send
  - some email system was designed only for text
    - encode raw binary data into printable ASCII characters
    - Uses radix-64 algorithm
- PGP also segments messages if too big

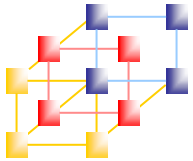
PGP operation – summary



(a) Generic Transmission Diagram (from A)



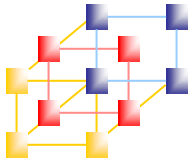
(b) Generic Reception Diagram (to B)



Quiz 7

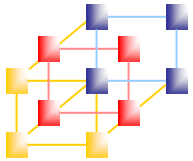
- 當需要同時簽章加密時誰先誰後？
  - 先產生數位簽章，再進行訊息加密
  - 先進行訊息加密，再產生數位簽章
  - 為什麼？！

- 請將答案寫在紙條上，下課收來講桌。
- ((請記得寫上班級姓名學號



Key identifier

- A unique identifying number associated with each key.
  - This identification number is useful for distinguishing between two keys that share the same user name and email address.
- The key ID associated with each public key consists of it least significant 64 bits
  - The Key ID of public key KUa is (KUa mod 2^{64})
  - The probability of duplicate key ID is very small
- A key ID is also required for the PGP digital signature



PGP key rings

- Each PGP user has a pair of keyrings
  - Public-key ring contains all the public-keys of other PGP users known to this user, indexed by key ID
  - Private-key ring contains the public/private key pair(s) for this user, indexed by key ID & encrypted keyed from a hashed passphrase

General structure of private/public key ring

Private Key Ring

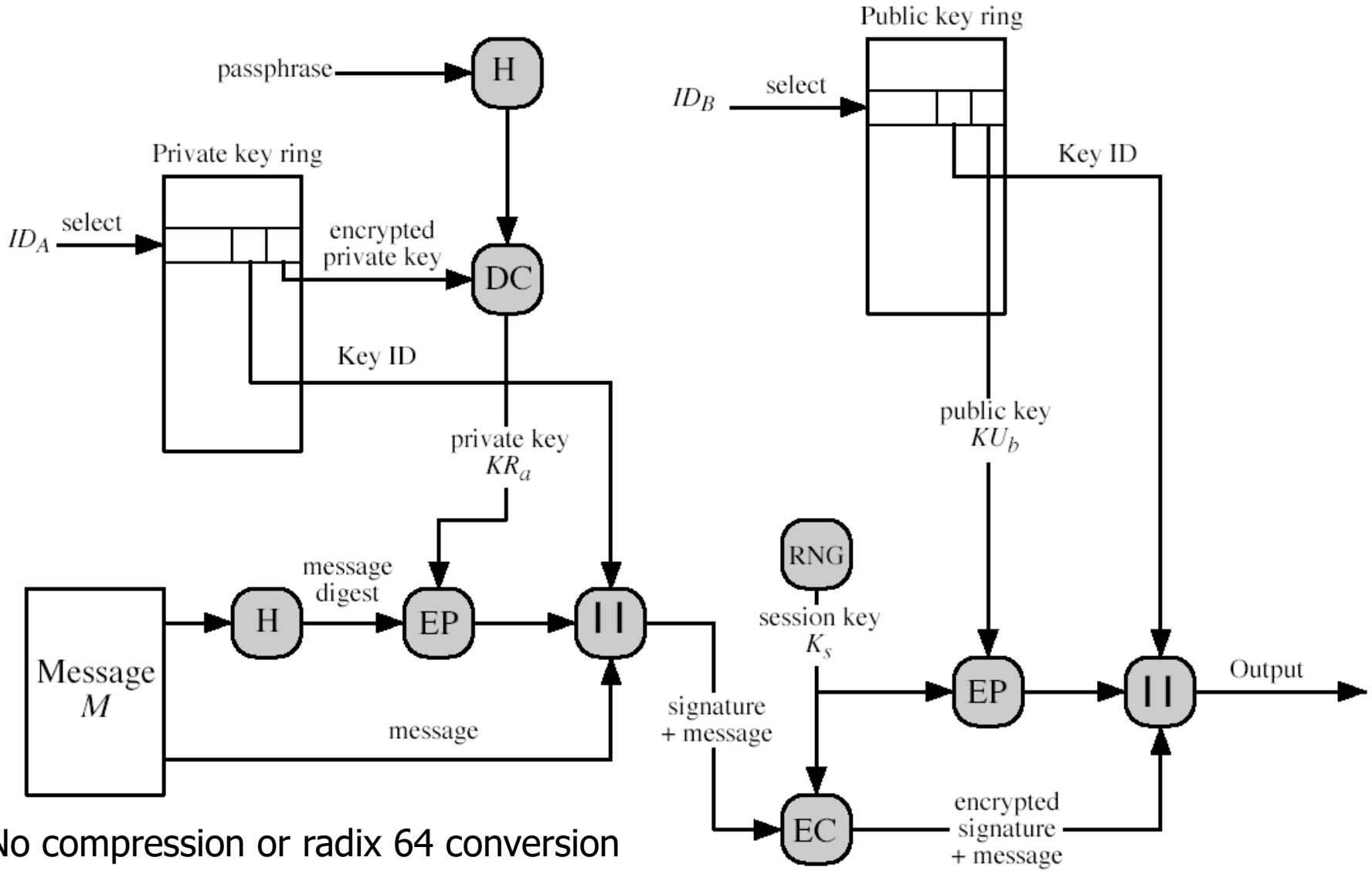
Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
•	•	•	•	•
•	•	•	•	•
•	•	•	•	•
T_i	$KU_i \bmod 2^{64}$	KU_i	$E_{H(Pi)}[KR_i]$	User i
•	•	•	•	•
•	•	•	•	•
•	•	•	•	•

Public Key Ring

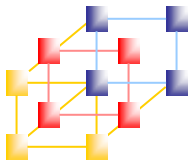
Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
T_i	$KU_i \bmod 2^{64}$	Ku_i	$trust\_flag_i$	User i	$trust\_flag_i$		
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•

* = field used to index table

PGP message generation

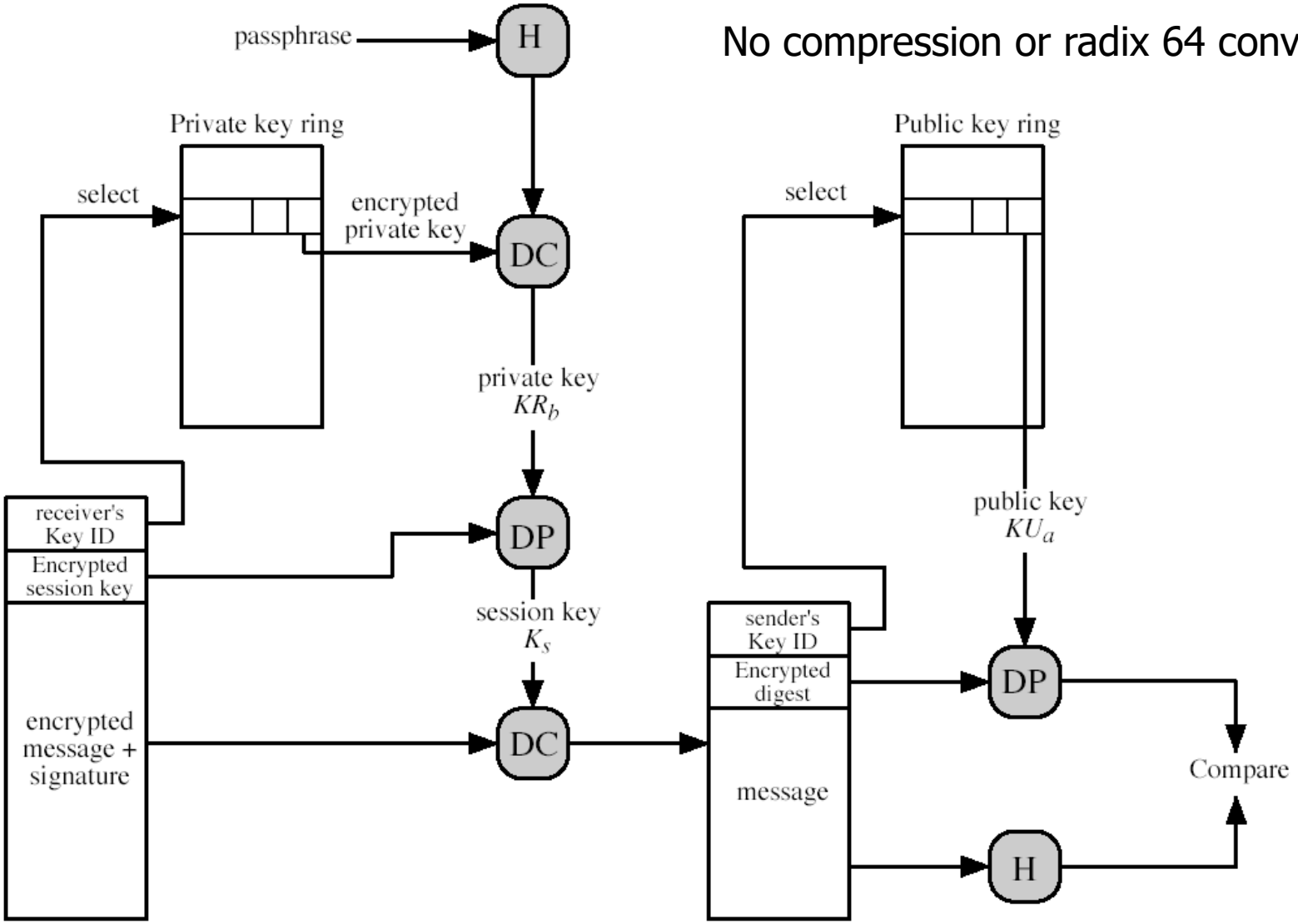


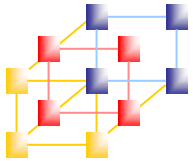
No compression or radix 64 conversion



PGP reception

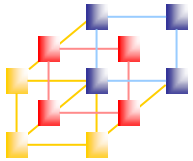
No compression or radix 64 conversion





PGP Key Management

- Rather than relying on certificate authorities, in PGP every user is own CA
  - Can sign keys for users they know directly
- Forms a "web of trust"
  - Trust keys have signed
  - Can trust keys others have signed if have a chain of signatures to them
- Key ring includes trust indicators
- Users can also revoke their keys

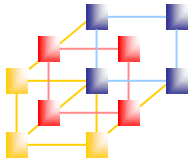


S/MIME V3和OpenPGP的比較 (1/2)

- 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

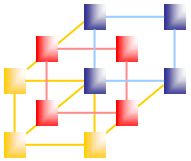
S/MIME V3和OpenPGP的比較 (2/2)

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



Outline

- S/MIME
- Pretty good privacy (PGP)
- DomainKeys Identified Mail (DKIM)

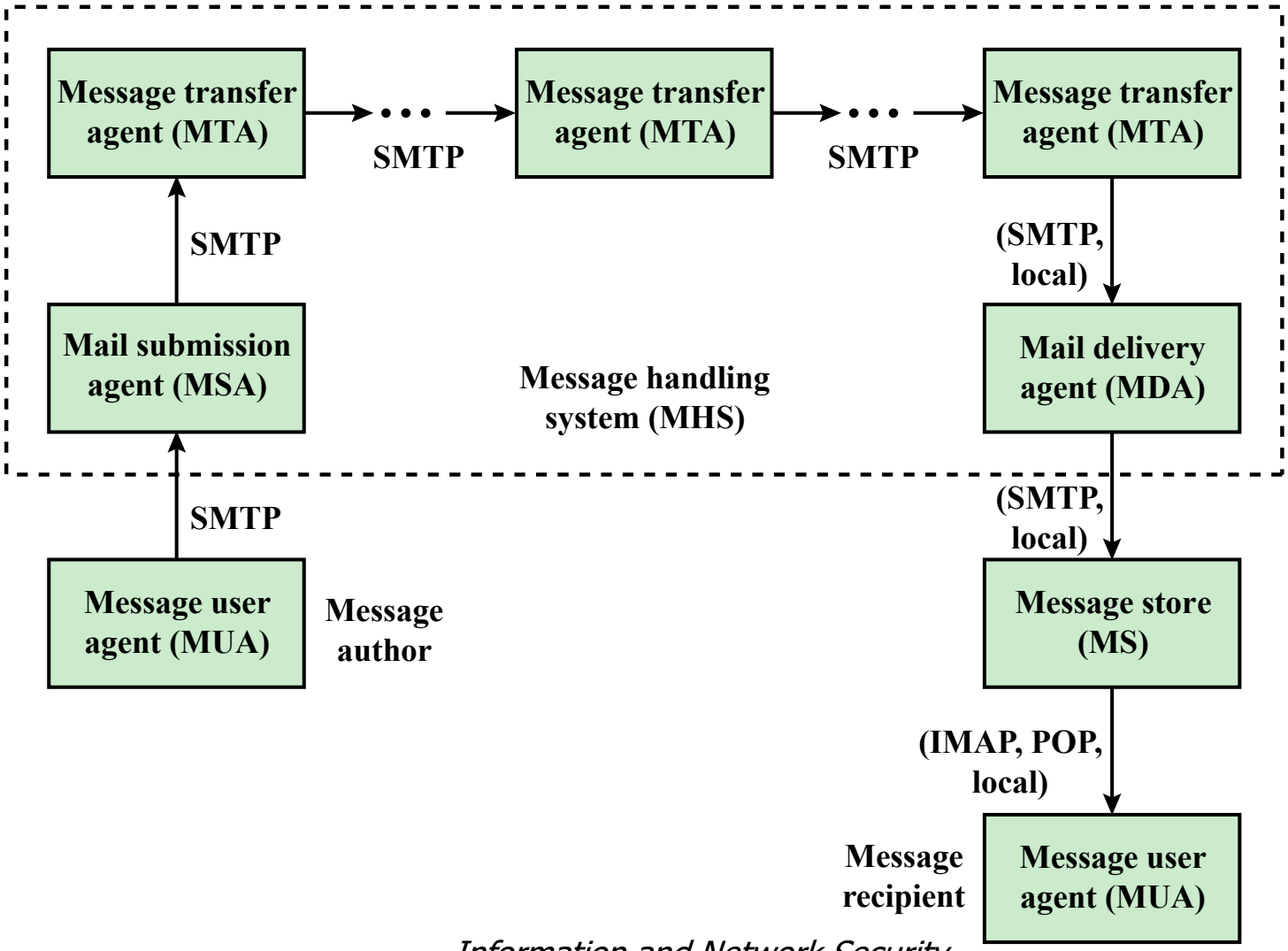


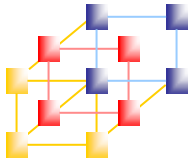
DomainKeys Identified Mail (DKIM)

- A specification for cryptographically signing e-mail messages, permitting a signing domain to claim responsibility for a message in the mail stream
- Message recipients can verify the signature by querying the signer's domain directly to retrieve the appropriate public key and can thereby confirm that the message was attested to by a party in possession of the private key for the signing domain
- Proposed Internet Standard RFC 4871
- Has been widely adopted by a range of e-mail providers and Internet Service Providers (ISPs)

DKIM 會在所有外寄郵件的標頭加上加密簽名，收到簽名郵件的電子郵件伺服器則會使用 DKIM 來解密郵件標頭，驗證郵件寄出後並未遭人竄改。

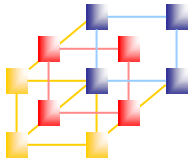
Internet Mail Architecture





E-mail Threats

- RFC 4684 (Analysis of Threats Motivating DomainKeys Identified Mail) describes the threats being addressed by DKIM in terms of the characteristics, capabilities, and location of potential attackers
  - At the low end are attackers who simply want to send e-mail that a recipient does not want to receive (廣告、垃圾信)
  - The next level are professional senders of bulk spam mail and often operate as commercial enterprises and send messages on behalf of third parties (非法廣告提供者)
  - The most sophisticated and financially motivated senders of messages are those who stand to receive substantial financial benefit, such as from an e-mail based fraud scheme (詐騙)

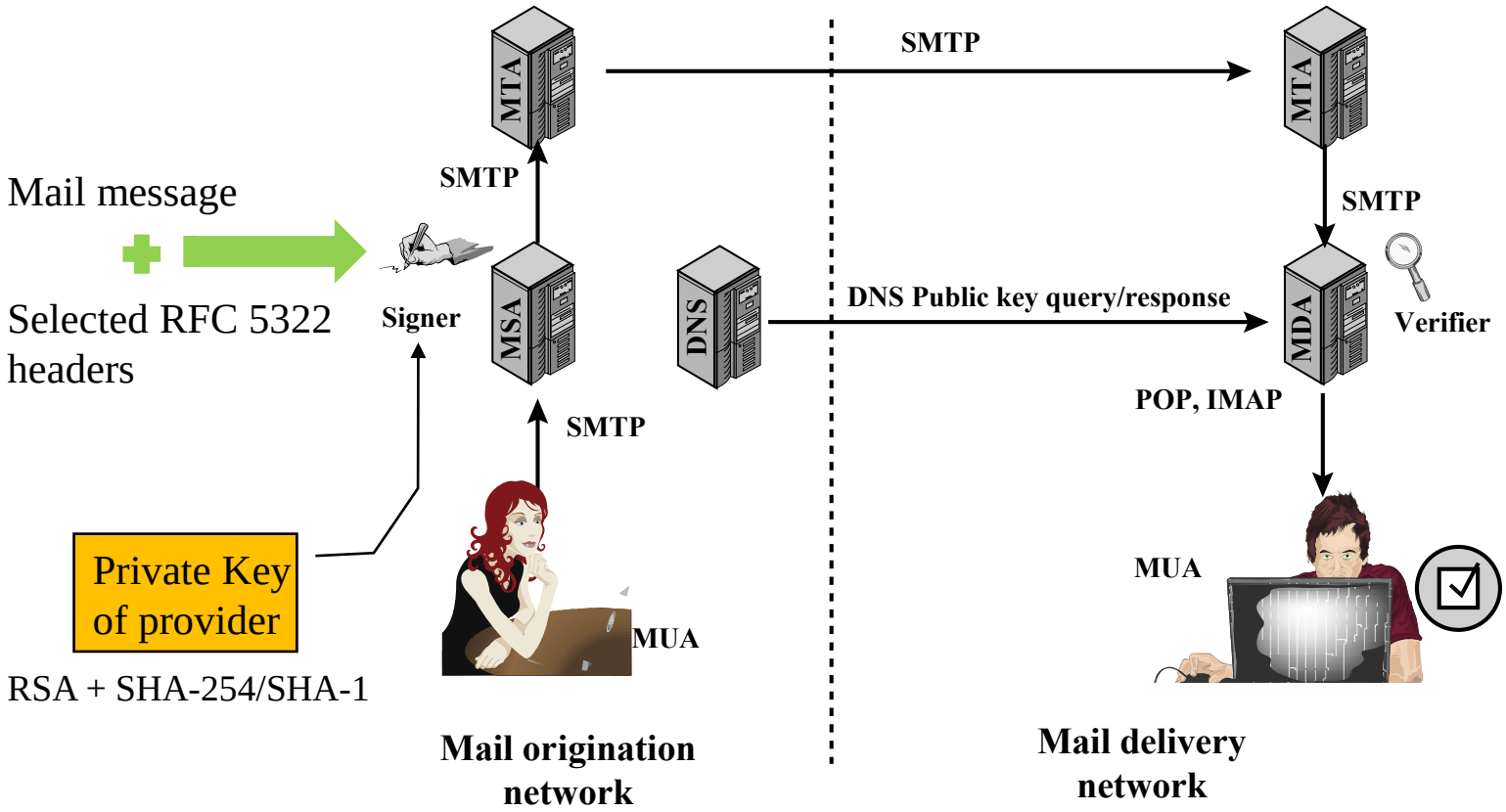


郵件炸彈與垃圾郵件

- 郵件炸彈
  - 短時間大量相同的信
  - 可以一次刪除
- 垃圾郵件
  - 大量內容無用的信件
  - 要慢慢看慢慢刪

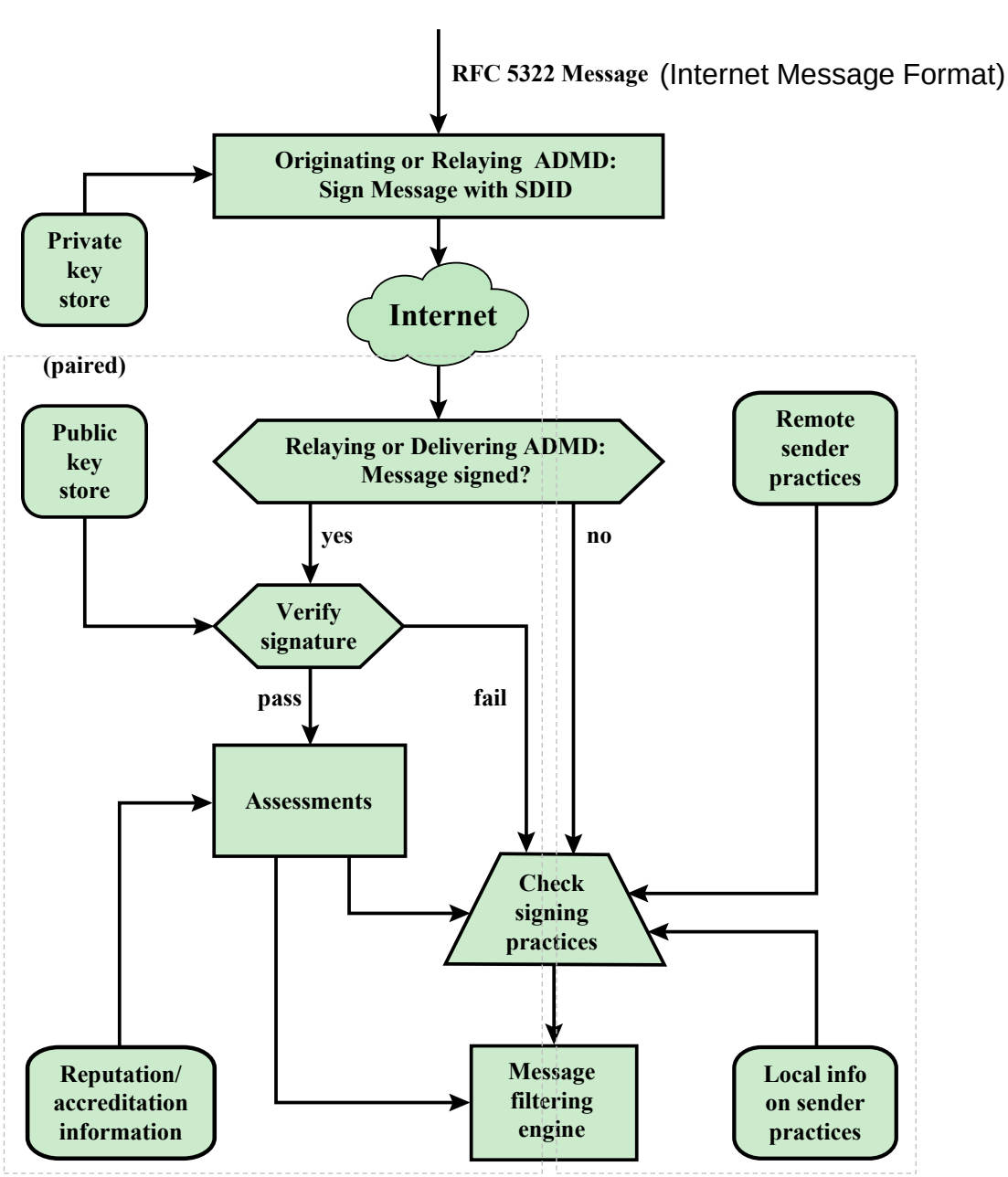
哪一種比較令人煩惱？

DKIM Deployment

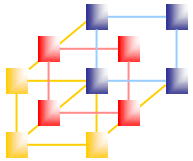


DNS = domain name system
MDA = mail delivery agent
MSA = mail submission agent
MTA = message transfer agent

DKIM Functional Flow



ADMA: Administrative Management Domain
SDID: Signing Domain IDentifier



真實世界往往不太美妙

- S/MIME → 沒人用
- Pretty good privacy (PGP) → 沒人用
- DomainKeys Identified Mail (DKIM) → 沒有用

但是憑證不是萬靈丹

- 有錢就買得到憑證
- 簽憑證的金鑰外洩

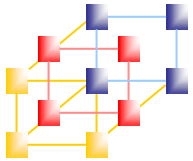
新聞

又有rootkit利用微軟數位簽章偽裝成合法程式，竊取用戶線上遊戲帳密及金錢

名為FiveSys的rootkit利用微軟WHQL（Windows Hardware Quality Labs）數位簽章獲取受害者信任，暗中竊取中國地區使用者帳密，劫持其線上遊戲帳戶的金錢支付

讚 6.7 萬 按讚加入iThome粉絲團 讚 73 分享

文/ 林妍溱 | 2021-10-25 發表



課外補充

- 有關SPF過濾
  - https://blog.xuite.net/jack.ycchuang/jack/25149902
  - https://bojack.pixnet.net/blog/post/12262340

- 垃圾信過濾方法大集合
  - https://workaround.org/ispmail/wheezy/smtpd-restrictions-spf-dkim-and-greylisting