20 電腦和互聯網的安全

目標

在完成這章後，你將能夠

- 知道何謂電腦災難及其後果
- 了解備份的重要性，預防未經授權的接達，及避免病毒攻擊
- 知道加密的意義和普通加密方法的操作原理
- 體會使用數碼證書在互聯網上傳送機密信息或進行電子商貿的優點

在使用電腦和互聯網方面，兩項最為人們關注的安全議題是電腦系統的**保安**及互聯網上個人的**私隱**。

圖 1　有些日常生活的標記也可能適用於電腦系統

未經授權的接達 unauthorised access　　加密 encryption

20.1　電腦系統的保安

重　點

電腦災難包括
1. 竊盜
2. 火警
3. 不當的操作
4. 錯誤程式
5. 硬件失效
6. 破壞
7. 未經授權的接達
8. 感染電腦病毒

電腦災難可能引導
1. 數據損毀
2. 金錢損失
3. 機密資訊外洩

電腦災難 (Computer disaster) 一般由下列的事件引致：盜竊、火警、操作不當、程式有誤、硬件故障、遭人為破壞、黑客攻擊、感染電腦病毒等。

電腦災難的後果一般是數據損毀、金錢損失、甚至機密資訊外洩。

以下的部分將會討論如何避免電腦災難的發生，方法包括：**為數據進行備份、防止未經授權的接達**及**預防電腦病毒的感染**。

A.　備份和復原

為了保護電腦的數據，必須定期及正確地進行**備份 (Backup)**，確保萬一電腦災難發生時，電腦系統仍能復原過來。

每個機構必須保存三個或以上，在不同時間備份的副本，如圖 2 所示。每次進行備份時，最舊的版本會被重寫，成為最新的版本。

重　點

每家公司應該保存至少三個在不同時間備份的副本。

只有災難發生時，復原才需要。

復原 (Restore) 是指電腦災難一旦發生，以備份的副本來把電腦回復到備份前的狀態，令系統得以繼續運作。若最新的備份副本未能把系統復原過來，則使用次新的，如此類推。

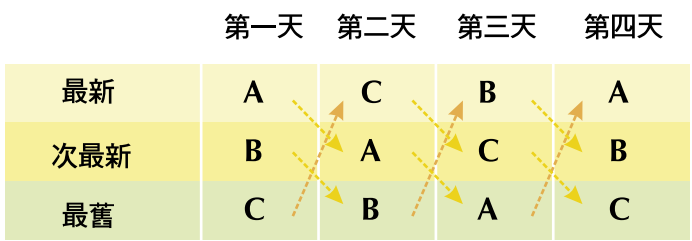


圖 2　使用三盒磁帶，A、B 和 C的備份時間表

人為破壞 tampering　　感染電腦病毒 virus infection

B. 防止未經授權的接達

1. 識別代碼和密碼

重點

密碼應該

1. 定期更改
2. 第一次使用前要立刻更改
3. 至少有 8個字元
4. 包含數字、大寫和小寫字母

電腦系統應該對所有用戶進行**鑒別 (Authentication)**，只容許獲授權的用戶進入，用戶在登入系統前，必須輸入正確的**識別代碼 (User ID)** 和**密碼 (Password)**。

用戶必須定期更改密碼；新的用戶在登入系統後，要即時更改密碼；識別代碼和密碼必須保持機密，並選擇難於猜對的組合，例如使用至少八個字元的密碼，並混合數字、大小寫英文字母。

圖 3 (a) 使用識別代碼和密碼來鑒別用戶 (b) 新的用戶要立刻更改密碼

2. 鑒別設備

除密碼外，系統亦可使用鑒別設備來鑒別用戶。鑒別設備包括磁卡、智能卡及生物測定學鑒別設備，像指紋掃描器、面型識別系統等 (見第 6 章)。

3. 防火牆

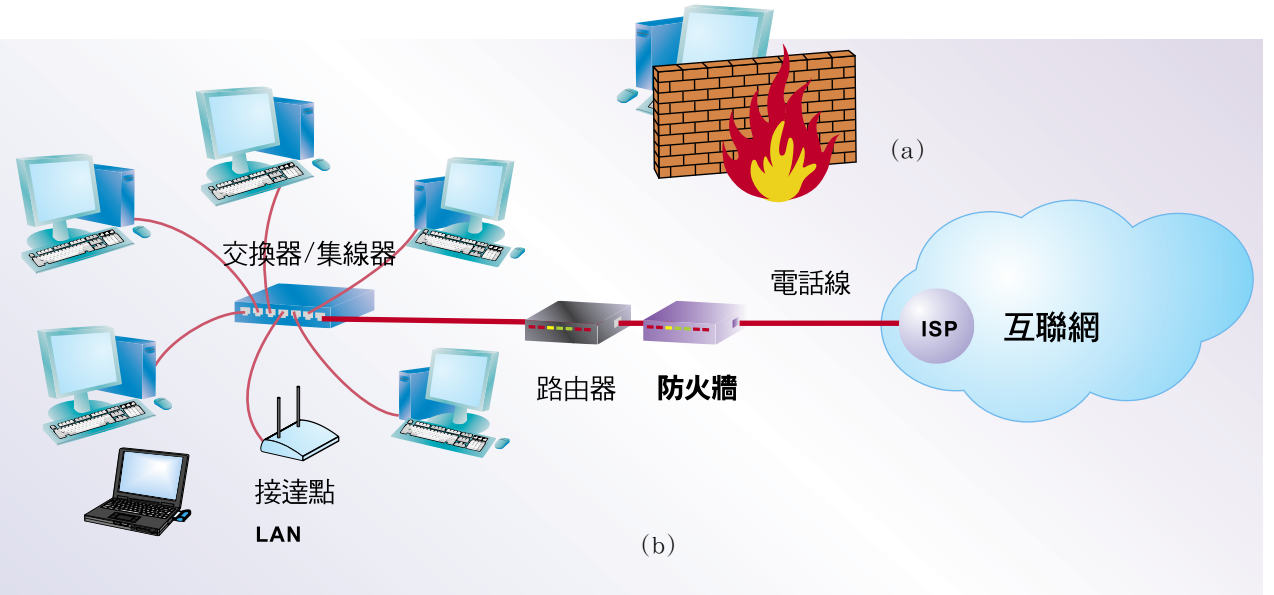


圖 4 建立防火牆避免對局域網不經授權的接達

磁卡 magnetic card
智能卡 smart card
生物測定學 biometrics
指紋掃描器 fingerprint scanner
面型識別系統 face recognition system

若局域網連接到互聯網，則應該為系統安裝**防火牆 (Firewall)**，阻止黑客闖入。防火牆可以是硬件或軟件，用於防止未經授權的接達。

重　點

病毒是自我複製的程式，設計來攻擊電腦系統。

感染病毒的途徑：

1. 開啟電郵附件。
2. 共用數據檔案。
3. 使用盜版軟件。
4. 安裝來歷不明的軟件。
5. 黑客襲擊。

C. 避免受病毒感染

病毒 (Virus) 是能自我複製的程式，目的是攻擊電腦系統。若電腦不幸受到病毒的感染，後果可能只是令人啼笑皆非的顯示，但亦有可能引致災難性的數據損毀。由於病毒可以經由網絡散播，組織內所有的電腦都有可能受到感染。

1. 電腦如何感染病毒？

電腦可能經下列的途徑感染到病毒：

1. 開啟電郵附件
2. 共用數據檔案
3. 使用盜版軟件
4. 安裝來歷不明的共用/免費軟件
5. 受專門散播病毒的黑客襲擊

2. 預防病毒感染

為了防犯受到病毒的感染，應該遵從以下的守則：

1. 為每部電腦安裝防毒軟件。
   - 每天更新病毒的定義檔案
   - 定期掃描硬碟偵測病毒
   - 掃描所有下載的檔案及電郵附件
2. 切勿開啟或轉寄來歷不明的電郵附件。
3. 拒絕使用盜版軟件。
4. 確保電腦不會以軟磁碟或光碟來啟動。
5. 若局域網連接到互聯網，則必須安裝防火牆，防止未經授權的接達。

自我複製 self-replicating　病毒定義 virus definition　掃描 scan
電郵附件 e-mail attachment　盜版軟件 illegal (pirate) software　啟動 boot

20.2 在互聯網上的安全和私隱

重 點

互聯網用戶關注的問題：
1. 私隱
2. 識別身份

A. 私隱和識別

以下兩項是互聯網用戶關注的問題：

- 信息在互聯網上傳送時，會否被人攔截，並非法讀取？
- 如何得知提供電子商貿的公司是可靠的？

上述的疑問可以歸納為下列的兩個保安議題及人們希望得到的解決方案：

1. **私隱 (Privacy)**：互聯網上所傳送的信息，最好只能由指定的收件人讀取，即使其他人取得信息，亦無法知道其內容。

2. **身份識別 (Identification)**：可以確定在互聯網上對方真正的身份，例如正在進行電子商貿的網上商店，最好能夠出示一些有效的證書，以證明它並非偽冒或虛假的公司。

同樣地，有時我們亦需要在互聯網上證明自己的身份，例如在電子商貿中或繳付政府帳單時，最好有一個安全的途徑，讓將我們展示獨特的身份證明文件，好讓對方接納我們的申請。

重 點

加密是藉著把數據轉換成亂碼以阻止他人檢視信息。

B. 加密

加密 (Encryption) 是指把數據轉換成一個必需**密碼匙 (Key)** 才能讀取的形式。若沒有密碼匙，信息會以亂碼形式出現。密碼匙可將加密後的信息進行**解密 (Decryption)**，把信息還原到原來的形式。

圖 5　使用相同密碼匙的加密和解密

C. 公開密碼匙和私人密碼匙

重　點

公開密碼匙對公眾開放；

私人密碼匙是機密的。

用其中一條密碼匙上鎖必須用另外一條密碼匙來開啟。

目前，最安全的加密方法是使用一對密碼匙：公開的和私人的。**公開密碼匙 (Public key)** 是可讓任何人知道的；**私人密碼匙 (Private key)** 則是機密的，不能公開。

用其中一條密碼匙來上鎖的文件，只能以另外對應的密碼匙來開啟。例如使用公開密碼匙來加密的信息，只能以對應的私人密碼匙來解密（見圖 6a）；同樣地，使用私人密碼匙來加密的信息，只能以對應的公開密碼匙來解密（見圖 6b）。

圖 6　使用不同密碼匙的加密和解密

你可以把公開密碼匙交給任何人，以便他們在傳送機密信息給你前，使用你的公開密碼匙來加密。在收到經加密的信息後，使用私人密碼匙，你便可為信息進行解密。

例 1　麗玲將要傳送一個信息給志明。麗玲能如何確定這個信息，除志明外，其他人將不能讀取？

解：　麗玲應該使用志明的公開密碼匙把信息加密。當志明收到加密後的信息時，他便會使用其私人密碼匙來開啟信息。

機密 confidential　　信息 message

D. 網站的保密傳送

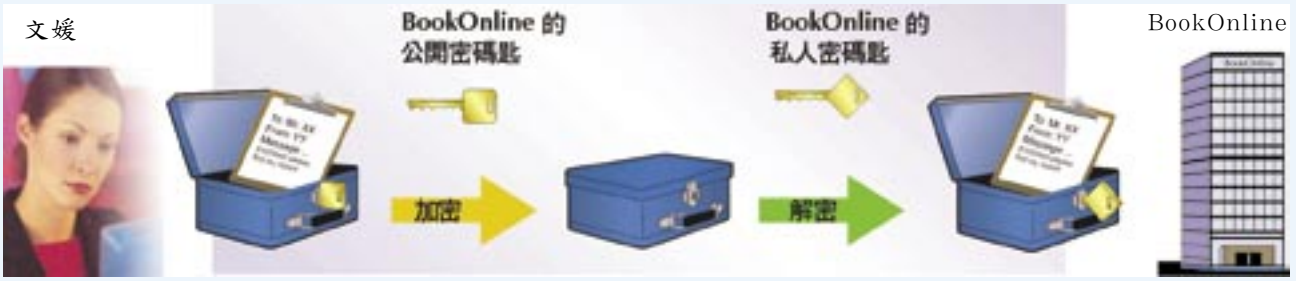
有些網站使用**保密插口層 (SSL)** 來確保數據安全地傳送。當用戶接達這些網站時，瀏覽器會顯示一個**閉鎖圖像**( )，表示數據將透過加密技術，安全地傳送。大部分電子商貿在處理財務事項時，都會使用 SSL 技術。

圖 7　使用 SSL 的網站

用戶在瀏覽 SSL 網站時，瀏覽器會收到這些網站所提供的公開密碼匙，此後在傳送任何數據往該網站前，用戶的瀏覽器都會使用這條公開密碼匙來加密。當網站收到經加密的數據時，便會使用其私人密碼匙來解密。上述的程序全部都是自動地執行的，用戶是不會察覺。

SSL 只能用於較新的瀏覽器上，例如 Internet Explorer® 3.0 或以上。

例 2　**文媛使用信用卡從網上書店 BookOnline 購買書本。文媛需要提供什麼購物數據？討論這些數據如何透過互聯網安全地傳送？**



保密插口層 SSL, Secure Sockets Layer　　閉鎖圖像 locked icon

重　點

數碼證書用於識別在互聯網上的人或組織。

解：　購物數據包括文媛的名字、地址、電郵位址、書本代碼（及相關資料，例如書名等）、數量和信用卡號碼（及相關資料，例如信用卡類型等）。

在傳送購物數據前，文媛的瀏覽器會使用 BookOnline 的公開密碼匙將這些數據加密。在收到加密的數據後，BookOnline 會使用其私人密碼匙為數據解密。

E. 數碼證書

數碼證書 (Digital certificate) 是一份包含持有者名字和其公開密碼匙的數碼文件，用於識別持有者在互聯網上的身份。持有者可以是個別用戶或組織。

用戶可以檢查網站是否持有數碼證書，當你瀏覽使用 SSL 的網站時，瀏覽器會顯示一個**閉鎖圖像**（），只需在該圖像上點兩下，便會開啟一個視窗，顯示該網站的數碼證書，如圖 8 所示。

數碼證書是由**核證機關 (Certificate authority)** 發行的。香港郵政署是本港核證機關之一，並發行「**電子證書**」**(e-cert)**。

個別人士可申請一份數碼證書，以便進行電子商貿或享用電子化公共服務。成功申請後，用戶將會收到一條私人密碼匙（16 位數字的密碼）和安裝數碼證書的軟件。安裝妥當後，你在互聯網上的身份便會得到核證機關的認可。

圖 8　有效的數碼證書

圖 9　香港郵政署是香港特區第一個核證機關 (http://www.hongkongpost.gov.hk)

識別　identify

F. 數碼簽署

重 點

數碼簽署肯定文件來自真的寄件人。

經**數碼化簽署**的文件，其部分的內容是經私人密碼匙加密的，並附有一份數碼證書（包括公開密碼匙）。加密的部分，稱為**數碼簽署 (Digital signature)**，其他人是不可能冒簽的。

由於隨同的數碼證書包括你的公開密碼匙，當電腦收到經你數碼簽署的文件時，便可用這條公開密碼匙來開啟加密的文件。由於只有你的公開密碼匙才能開啟那經加密的文件，因此這文件肯定是由你發送的。

數碼簽署也意味具有「**不可抵賴性**」**(Non-repudiation)**，即不可否認。舉例來說，顧客在電子商貿中發出附有數碼簽署的購貨指示後，便不能夠否認曾經發出指示。

注意，發送附有數碼簽署的電郵時，必須使用專用電郵軟件，例如 Microsoft Outlook®。

圖 10　數碼簽署

例 3　曼玉想透過互聯網遞交申請表給運輸署，以便申請駕駛執照。運輸署如何能確認曼玉的身份？

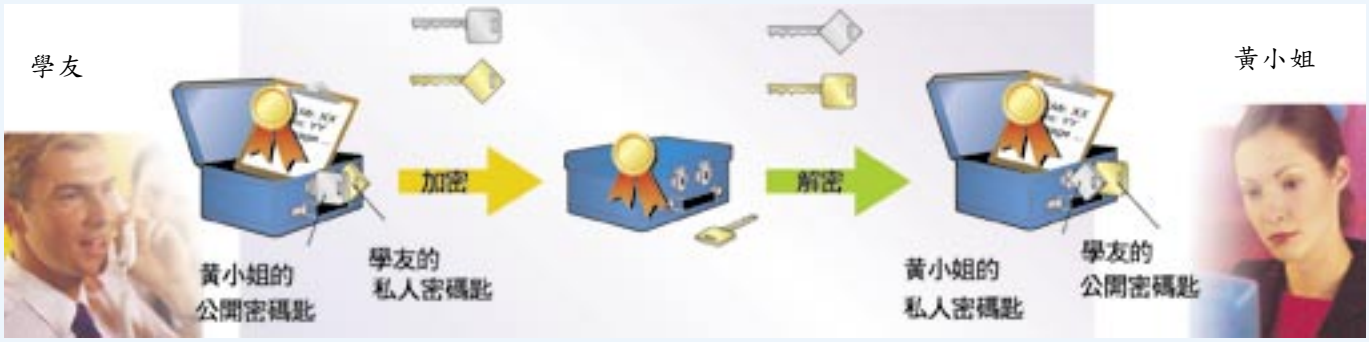
解：　首先，曼玉使用她的私人密碼匙在申請表上加上數碼簽署，然後把這文件連同她的數碼證書一起傳送到運輸署。藉使用曼玉提供（包括在數碼證書上）的公開密碼匙，運輸署便能確認寄件人是曼玉。

數碼化簽署 digitally signed　　專用電郵軟件 dedicated e-mail software

例 4　學友是某工作小組組長，他打算透過電郵，向上司黃小姐匯報小組成員的工作表現。他需要確定只有黃小姐才能讀取該電郵的內容。同時，他必須令黃小姐知道該電郵是由他本人發出的，並非偽冒。學友應該怎樣做？

解：　學友應該使用他的私人密碼匙在電郵上加上數碼簽署，再使用黃小姐的公開密碼匙把電郵加密。

當黃小姐收到電郵後，她可以用學友的公開密碼匙確認學友的身份，然後用自己的私人密碼匙將電郵解密。



20.3　在互聯網上的措施

下列的措施可保障你在互聯網上的安全：

A.　一般的安全措施

1. 在透過互聯網傳送信用卡號碼、身份證號碼等機密資料前，必須將數據加密。
2. 定期更改密碼；對任何首次開啟的帳號，必須隨即更改密碼。
3 選擇難於猜測的密碼，密碼必須同時含有數字、大小寫英文字母。
4. 為免受病毒感染，在開啟任何下載的檔案或電郵附件前，掃描所有的檔案。應該關掉電郵軟件中自動處理電郵附件的功能。
5. 定期清理電郵資料夾、刪除無用的郵件及定期清除「已刪除郵件」資料夾。電子郵件不但可在傳送期間被攔截，亦可能被電腦黑客偷取。
6. 在學校或圖書館等公共場所，使用互聯網後，離開前僅記登出系統，避免讓其他人有機可乘，利用你的帳號進行違法的活動。

措施 practices　　帳號 account　　資料夾 folder

B. 網上購物的安全措施

1. 使用安全的瀏覽器

上文提及的加密方法只適用於較先進的瀏覽器，例如 Internet Explorer® 3.0 或以上。

2. 只在確定為安全的公司購物

任何人都能以幾乎任何名字來建立網上商店，因此只有能出示有效數碼證書的網站，才可確定為安全的。你可以在瀏覽器上藉著點兩下閉鎖圖像來檢視其數碼證書。一般而言，有實體店鋪的網上商店是較為可靠的。

C. 在互聯網上的個人措施

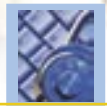
在互聯網上，個人可以隱藏其真正的身份，並假扮成其他人。

曾經發生多宗涉及孌童的不幸案件，罪犯在互聯網上到處結識孩童，裝出友善的態度，對孩童的問題假意諸般慰問，表現出理解和同情，然後安排與孩童會面。

為了保護你自己及家人的安全，你應該遵守以下的個人守則：

1 切勿隨便向網際朋友透露任何識別代碼及密碼。
2 切勿向網際朋友透露任何個人資料，包括住址、電話號碼、學校等詳情，更不要提供你或家人的相片。
3 切勿與素未謀面的網際朋友單獨外出。

實體店鋪 physical storefront　假扮 purport　孌童 pedophilia



摘要

1. 引起電腦災難包括：盜竊、火警、不當的操作、錯誤程式、硬件失效、破壞、未經授權的接達、感染電腦病毒等。電腦災難可能導致數據和金錢損失、甚至資訊外洩。
2. 備份應該至少有三個版本，並定期進行。復原只在電腦災難發生時才有需要。
3. 鑒別是防止未經授權的接達。密碼要定期更改，新的用戶更要立刻更改密碼，密碼必須保持機密，並至少有八個混合數字和大小寫字母的字元。防火牆用於網絡防止黑客。
4. 電腦系統可能經過各種不同的方法受病毒感染。應該安裝防毒程式，並定期更新病毒定義檔案。
5. 加密是把數據轉換成亂碼以阻止他人檢視信息。最好的加密方法是使用一對密碼匙：用其中一條密碼匙上鎖，並必須用另外一條密碼匙來開啟。
6. 數碼證書用於識別在互聯網上的人或組織，避免詐欺。數碼簽署可以確定信息是真的由發件人發送，具有「不可否認性」。

練習

多項選擇題

1. 復原應該
   A. 定期進行。
   B. 在每次備份後進行。
   C. 在災難發生後進行。
   D. 在每次備份前進行。

2. 某電腦系統預設每星期一至五進行備份，每天使用一盒磁帶。磁帶上備份的資料會一直保持到下星期，只有每月最後的一次備份，才會永久地保存下來，不會被重寫。一年內總共需要多少盒磁帶？如有需要，可以假設每年有 52 個星期。

   A. 5
   B. 17
   C. 52
   D. 57

3. 防火牆用於
   A. 阻止未獲授權的存取。
   B. 禁制盜版軟件。
   C. 終止侵犯版權。
   D. 防止火警發生。

4. 下列哪項可以對在互聯網之上傳送的信息進行加密及解密？
   (1) 防火牆
   (2) 瀏覽器
   (3) 專用電郵軟件

   A. 只有 (1)
   B. 只有 (2)
   C. 只有 (1) 和 (2)
   D. 只有 (2) 和 (3)

5. 下列哪項行動有可能引致系統受病毒感染？
   A. 編寫電子郵件
   B. 讀取電郵信息
   C. 開啟電郵附件
   D. 刪除電郵附件

6. 彼得的電腦使用寬頻服務接達互聯網。每天當他啟動電腦時，防毒程式會自動從某個網站下載一些檔案。所下載的檔案是
   A. 防毒程式的更新版本。
   B. 有關病毒的最新資訊。
   C. 病毒程式。
   D. 本地新聞。

7. 若信息由公開密碼匙加密，這信息可以由下列哪項解密？
   A. 同一公開密碼匙
   B. 對應的私人密碼匙
   C. 其他公開密碼匙
   D. 任何私人密碼匙

8. 數碼證書包括
   (1) 持有者的姓名
   (2) 公開密碼匙
   (3) 私人密碼匙

   A. 只有 (1)
   B. 只有 (3)
   C. 只有 (1) 和 (2)
   D. (1)、(2) 和 (3)

9. 在香港，發行數碼證書的政府部門是
   A. 保安局。
   B. 人民入境事務處。
   C. 郵政署。
   D. 貿易署。

10. 經數碼簽署的信息是具有不可抵賴性的，原因是只有寄件人才可用其
    A. 私人密碼匙簽署。
    B. 公開密碼匙簽署。
    C. 私人密碼匙解密。
    D. 公開密碼匙解密。

問答題

1. (a) 舉出**五種**電腦災難。
   (b) 寫出**兩個**電腦災難的後果。

2. (a) 解釋數據備份為什麼是重要的。
   (b) 寫出保存多個備份副本的**優點**。
   (c) 怎樣保護數據，才可抵禦嚴重的災難，例如火警？

3. 某系統的登入程式要求用戶鍵入用戶名字及密碼。
   (a) 德華是該系統的新用戶。在登入系統後，解釋為什麼他被要求立刻更改密碼。
   (b) 當德華鍵入他的新密碼時，他必須鍵入兩次。該系統要求用戶把同一數據鍵入兩次的目的是什麼？
   (c) 電腦不允許德華以英文名的首三個字母 "tim" 作為密碼。提供**一個**理由。

4. 電腦病毒每年導致數以百萬元的金錢損失。

   (a) 什麼是電腦病毒？
   (b) 寫出**四個**電腦系統受病毒感染的途徑。
   (c) 提供**四個**電腦系統可免受病毒感染的方法。

5. 某學校剛剛建立了一個局域網。學生使用 "student" 作為用戶名字而毋需鍵入密碼就能登入網絡，並透過寬頻接達互聯網。

   (a) 試解釋用戶 "student" 為什麼不能夠安裝任何程式。
   (b) 試舉出用戶 "student" 所受的**兩個**其他的限制。
   (c) 學校局域網和互聯網之間安裝了一個防火牆。防火牆有什麼目的？
   (d) 為了把局域網連接到互聯網，什麼設備是必需的？
   (e) 某天，校長接獲 ISP 的投訴，原因是學校正在不斷地把不必要的信息傳送到互聯網上。
      i) 學校的電腦系統出現了什麼問題？
      ii) 對這個問題提供**一個**原因。
      iii) 如何能解決這個問題？

6. (a) 何謂加密？
   (b) 如何能檢視經過加密的信息？

7. 富成打算從某網上商店購買貨品，該商店要求富成提供姓名、住址、電話號碼、電郵位址、信用卡號碼、信用卡類型及信用卡屆滿日期等。

   (a) 寫出**三個**電子商貿的優點。
   (b) 寫出**兩個**富成在提供上述資訊前必須考慮的防預措施。簡短地解釋你的答案。

8. 目前，最安全的加密方法是使用一對密碼匙：公開密碼匙和私人密碼匙。以其中一條密碼匙上鎖的文件，只能以另外一條密碼匙來開啟。公開密碼匙是公開的，而私人密碼匙必須保持機密。

(a) 秀文正在從一家使用密碼匙的網上商店購買貨品。在透過互聯網傳送前，她的個人資料是經過加密的。

i) 哪個密碼匙是用於為秀文所提供的資訊加密？
ii) 哪個程式負責加密的工作？
iii) 哪個密碼匙可為上述資訊解密？

(b) 卓妍和冠希各有一對密碼匙。

i) 若卓妍想向冠希發送電子郵件，並希望只有冠希才能讀取，卓妍應該使用什麼密碼匙為電子郵件加密？簡短地解釋。
ii) 當卓妍透過互聯網申請駕駛執照時，她使用自己的私人密碼匙把信息加密。這個加密程序有什麼目的？

9. (a) 能夠出示數碼證書的網上公司是較為可靠的。你如何能知道某公司是否持有一份數碼證書？

(b) 數碼證書是透過互聯網繳付政府費用所必需的，而個別人士可以向核證機關申請數碼證書。為個別人士而設的數碼證書目的是什麼？