資訊科技與社會 第二課：數據私隱和數據安全 溫習筆記

學習目標：

- 避免在網絡披露過多個人資料。
- 判斷網上註冊時所收集的資料是否合理。
- 學習保護個人資料的方式。
- 明白使用公開密碼匙基礎建設的基本原則和目的。

I. 數據私隱與數據安全概覽

網上個人資料注意事項：

- 社交平台容易造成個人資料過度_____。
- 即使刪除內容，資料可能仍未完全移除，並可能被商業公司利用。
- 需警惕公開住址、身份證號碼、信用卡資料、電話號碼、帳戶密碼等個人敏感資料。
- 網站可能要求不必要的個人資料（如住址、電話號碼）作為註冊或追蹤用途。

II. 資料洩漏的風險及預防

造成資料洩漏的原因：

- _____：例如不小心遺失存有秘密資料的儲存裝置。
- _____：管理員設定過寬的連結共用功能，導致未經授權者可存取資料。
- _____：透過惡意軟件、密碼匙或利用服務供應商漏洞竊取資料。

防止資料洩漏的方法（一般措施）：

- 檢查您共享的檔案或設定是否恰當。
- 加密檔案或整個儲存裝置。
- 使用複雜且不重複的密碼，包含_____、_____及_____，並定期_____。
- 關閉自動_____功能，避免瀏覽器記住帳戶名稱及密碼。
- 啟用「_____模式」（例如 Safari 私密瀏覽、Google Chrome 無痕模式），可防止瀏覽記錄、cookie 被儲存，但無法阻止網站獲取數據或 ISP 追蹤。

清除儲存裝置資料的方法：

- 為了避免存儲裝置內的資料外洩，我們可以加密儲存裝置。

1. _____（**Formatting Data**）：
    1. **定義**：把存儲裝置格式化，還原裝置至最初的設定，以清除自訂數據。
    2. **目的**：刪除儲存裝置內的所有資料。
2. _____（**Erasing Data**）/ 用_____清除裝置（**Wiping Data**）：
    1. **定義**：利用軟件在磁碟中重複改寫舊資料，確保舊資料磁極永久退極化，並使這些資料不能被復原。
    2. **步驟**：需要運行刪除數據的軟件數次，以確保儲存於裝置內的所有資料已被刪除。
3. _____（**Destroying Hard Drive**）：
    1. **定義**：直接把存儲裝置銷毀。
    2. **優點**：可令內裏的資料難以被復原。
4. **其他注意事項**：
    1. 直接把資料檔案置於資源回收筒，並清除資源回收筒，該檔案並不可被永久清除。

加密儲存裝置：

- 透過加密，只有你和已授權人士能讀取，其他人無法閱讀其中的資訊。
- 可以利用專業軟件（如 Rohos Mini Drive 或 WinRAR）對 USB 儲存裝置或檔案進行加密，設定密碼。

III. 公開密碼匙基礎建設（PKI）與數據安全

定義：

PKI 是一組驗證機制，確保身份並防止第三方修改資料。它採用_____系統，運用公鑰和私鑰。

公鑰與私鑰：

公鑰（Public Key）：

- 能被_____看見的數碼鑰匙。
- 用作證明發送人的身份。
- 在數據簽署中，用於核實答署信息
- 在數據加密中，用於加密信息給接收者。

私鑰（Private Key）：

- 只有_____才可使用的數碼鑰匙。
- 在數碼簽署中，用於簽署信息。
- 在數據加密中，用於解密由其對應公鑰加密的信息。

公鑰和私鑰的特性

- 公鑰和私鑰都是由同一個_____共同生成的，形成一對
- 所以它們之間存在著獨特的數學關聯：
  這種獨特的數學關聯確保了：
  - 用特定的公鑰加密的信息，只能由與之配對的私鑰來解密。
  - 反過來也是一樣，用私鑰簽署的訊息，需要用其配對的公鑰來驗證。

PKI 的主要功能/目標（PAIN 原則）：

P - _____（Privacy）：

- 目的：確保只有指定接收者才能解密訊息。
- 機制：發送人使用接收者的公鑰加密信息，只有接收者的私鑰才能解密。

A - _____（Authentication）：

- 目的：確認發送人的身份，確保信息確實由指定簽署者發出。
- 機制：透過數碼簽署實現。

I - _____（Integrity）：

- 目的：確保資料內容在傳輸過程中未被人修改的狀態。
- 機制：數碼簽署可驗證資料在傳輸過程中未被修改。

N - _____（Non-repudiation）：

- 目的：發送人不能否認自己曾寄出訊息的特性。
- 機制：公鑰和私鑰的組合使用，配合數碼簽署確保發送人無法否認訊息。

數碼簽署（Digital Signature）：

目的：

確認發送人的身份和證明信息未被篡改。

機制：

- 簽署：發送人使用自己的_____對訊息進行簽署。
- 驗證/核實：接收人使用發送人的_____來核實簽署。

具體來說：

1. 在數碼簽署的過程中，發送人會使用自己的私鑰來簽署訊息。
2. 而接收人或其他網絡使用者則會使用發送人對應的公鑰來核實這個簽署。
3. 如果核實成功，就可以證明訊息確實是由聲稱的發送人所發出，因為只有擁有對應私鑰的人才能生成有效的簽署。
4. 當訊息被數碼簽署後，任何對訊息內容的篡改都會導致簽署驗證失敗。因此，透過成功驗證數碼簽署，可以確認訊息在傳輸過程中沒有被篡改。

數據簽署滿足了A，I，N：

1. 認證 (Authentication)
   。數碼簽署如何滿足：數碼簽署的核心目的是確認發送人的身份。在數碼簽署的過程中，發送人會使用自己的私鑰對訊息進行簽署，而接收人則使用發送人對應的公鑰來核實這個簽署。如果核實成功，就證明了訊息確實是由聲稱的發送人所發出。
2. 完整性 (Integrity)
   。數碼簽署如何滿足：數碼簽署透過其驗證機制，能夠確保資料內容在傳輸過程中未被人修改的狀態。當訊息被數碼簽署後，任何對訊息內容的篡改都會導致簽署驗證失敗。因此，透過成功驗證數碼簽署，可以確認訊息在傳輸過程中沒有被篡改。公鑰和私鑰提供不可否認性，其中一個原因就是「可確保訊息於傳送過程中未被修改」。
3. 不可否認性 (Non-repudiation)
   。數碼簽署如何滿足：不可否認性指的是發送人不能否認自己曾寄出訊息的特性。由於數碼簽署是使用發送人獨有的私鑰來完成的，並且這個簽署可以被所有知道發送人公鑰的人核實，一旦訊息被成功簽署並驗證，發送人就無法否認是他發送了該訊息。

然而，值得注意的是，數碼簽署本身並不滿足私隱 (Confidentiality/Privacy) 的要求。

- 數碼簽署並不能保密通訊內容，也不會為互聯網上的訊息添加密碼。

知識重溫：

- 公鑰是「所有人均可見的數碼鑰匙」，其作用就是「用作證明發送人的身份」。
- 這種核實機制也是「認證 (Authentication)」的一環，透過公開密碼匙來證實發件人的真確性。

總結來說，公鑰在數碼簽署中扮演著驗證工具的角色，讓接收方能夠確認訊息的來源和發送方的身份。

局限性：

數碼簽署無法確保通訊內容的私隱，因為發送人的公鑰本身是公開的，任何人都能用發送人的公鑰核實和閱讀被簽署的訊息。。

數據加密（Data Encryption）：

目的：

確保信息在互聯網傳送中的私隱，不被未經授權的人士存取。

機制：

1. 加密過程：發送人會使用接收者的_____來加密訊息。由於公鑰是公開的，任何人都可以取得它。
2. 解密過程：只有持有與該公鑰配對的私鑰的人，才能成功解密被加密的訊息。私鑰是只有持有者才可使用的數碼鑰匙。

數據加密主要確保的是_____(Privacy)，它的用意在於確保資訊在互聯網傳送時的私隱，使資訊不會被未經授權的人士存取。

- 透過使用接收者的公鑰加密資訊，PKI 能確保只有指定的接收者才能解密和閱讀資訊，從而保障數據的私隱。
- 此外，將儲存裝置「加密」也是為了避免資料外洩，確保只有授權人士才能讀取其中的內容。

局限性：

數據加密單獨使用時，其主要局限性在於無法認證訊息的_____ 。

- 儘管數據加密確保了只有指定接收者能夠閱讀訊息，但它無法驗證發送這條加密訊息的人是誰。
- 這是因為所有網絡使用者都可以取得接收者的公鑰，並用它來加密訊息，傳送給接收者。因此，接收者雖然能解密訊息，但難以確認信息的發送人身份。

數碼簽署及數據加密的結合：

- 為了彌補數碼簽署在保密性上的不足，以及數據加密在認證上的不足，可以結合使用。
- **簽署及加密**：發送人使用**自己的私鑰**簽署訊息，然後再用**接收者的公鑰**加密訊息。
- **核實及解密**：接收人先用**自己的私鑰**解密訊息，然後再用**發送者的公鑰**核實簽署。
- **目的**：確保發送人的身份和訊息的完整性，同時確保只有指定接收人才能閱讀訊息。