主題 13.3

密碼學的應用

題型13–6 數位簽章

【重點說明】

1. 憑證：

憑證就像是一張電子身分證，上面記載了用以辨別憑證所有人的個人資料、憑證所有人的公開金鑰、發行憑證單位的名稱及數位簽章、以及憑證有效期限及用途等資訊。憑證由認證中心核發給該憑證的所有人，所有人在傳送資料的同時，可以將憑證一起傳送給收件人以辨別自己的身分。申請憑證是為了確保個人資料在網路傳輸的安全性。它具備了下面幾項特性：

⑴完整性（integrity）：

透過憑證的核對能確保資料在網路傳輸的正確性。換句話說，政府單位收到的資料會與你所傳送的資料完全一樣。

⑵身分辨識（authentication）：

憑證可確認資料傳送者的身分。

⑶不可否認性（non-repudiation）：

憑證就像數位簽章可讓資料傳送者不能否認曾經傳送過這筆資料。

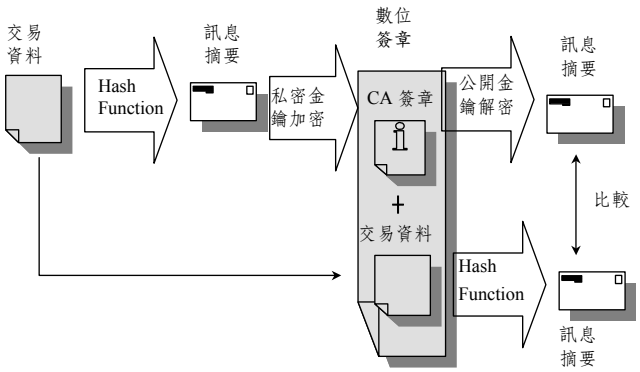
⑷機密性（confidentiality）：

文件可以金鑰加解密，以達到機密性。

2. 數位簽章（digital signature）：

在傳統商務活動中，文件起草人為了對自己所簽發的文件表示負責，通常文件起草人或是發件人會在文件末端簽上自己的姓名。由於親筆簽名不容易被偽造，因此一旦文件上的簽名通過檢驗，文件的出處便獲得證實。而數位簽章便可以為數位文件創造出與親筆簽名相似的效果。

公開金鑰密碼系統（PKCS）常被用來作的數位簽章的技術，以私有鑰匙對個人數位簽名作加密，接收訊息者再用相對應的公開鑰匙作解密。如此就可以做到數位簽章的功能。目前常被採用的數位簽章標準是由美國制定的數位簽章演算法（Digital Signature Algorithm，簡稱DSA）。根據DSA所提出的數位簽章標準最初採用的長度是512位元，也可以擴大到1024位元。利用公開金鑰進行的數位簽章步驟與上述加解密步驟剛好相反。當文件發送方要為一份數位文件產生一個專屬的數位簽章時，會使用公開的雜湊函數（Hash Function）為數位文件產生一個訊息摘要，常用的雜湊函式有MD5、SHA、SHA-1，然後用自己的私密金鑰對訊息摘要加密產生一個數位簽章，接收方利用發送方私密金鑰配對之公開金鑰，可將接收到的數位簽章還原為原來的訊息摘要，同時依其接收之交易資料，經公開的雜湊函數運算也會產生一個訊息摘要。比對二個訊息摘要，若兩者相同，即表示該文件確實由文件發送方送出。否則，他就認定該文件的原始起草人不是訊息發送方。



範題 《重要題》

名詞解釋：

digital signature.

【解】見本題型【重點說明】部分。

範題 《常考題》

申請憑證是爲了確保個人資料在網路傳輸的安全性，請問它至少具備了那些特性？

【解】

至少具備下面幾項特性：

⑴完整性（integrity）：

透過憑證的核對能確保資料在網路傳輸的正確性。換句話說，政府單位收到的資料會與你所傳送的資料完全一樣。

⑵身分辨識（authentication）：

憑證可確認資料傳送者的身分。

⑶不可否認性（non-repudiation）：

憑證就像數位簽章可讓資料傳送者不能否認曾經傳送過這筆資料。

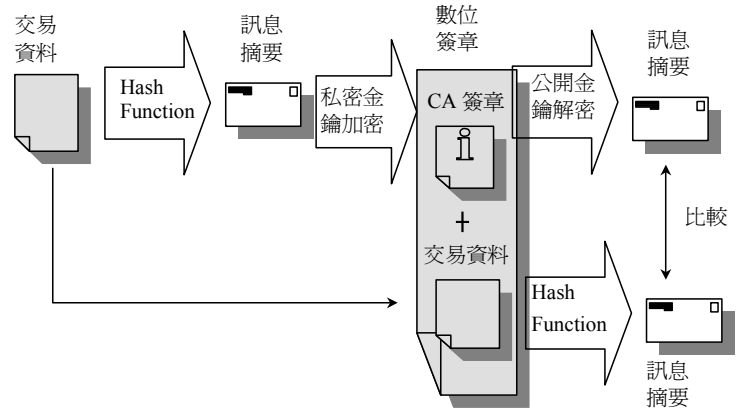
⑷機密性（confidentiality）：

文件可以金鑰加解密，以達到機密性。

範題

試說明數位簽章之機制與原理。 （淡江運管）

【解】



範題

微軟（Microsoft）與VeriSign公司所共同發展出來的一種軟體認證標準，使軟體開發者可在他們所開發的軟體（包含Java applet或ActiveX控制元件等）中加上這種認證標記，能夠讓使用者在下載執行這些軟體元件之前，知道它們是由誰所開發出來的。請問這種認證爲：

(A)Verification Code　(B)Authenticode

(C)Parity Checking code　(D)Privacy code

(E)以上皆非。　（暨南資管）

【解】(B)

範題

下列哪一種技術可有效的用來作著作權的保護？

(A)數位簽章　(B)電子認證

(C)數位浮水印　(D)金鑰加解密技術

(E)以上皆非。　（暨南資管）

【解】(A)(B)(C)(D)

範題

單選題（Multiple choice question）：

_____ is a unique identifier for a document which is used to provide proof that the data has not been altered or tampered with.

(A)Triple DES (B)Spoofing

(C)Digital certificate (D)Watermark

(E)Message digest. （成大資管）

【解】(C)；

In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document which uses a digital signature to bind a public key with an identity.