University of Taipei

Computer Science

Homework Ch.6

Student ID: U10916024

Student: Cheng-Hao, Zhang

張呈顥

2023

1. 請說明訊息鑑別碼跟數位簽章的差異

訊息鑑別碼（Message Authentication Code，MAC）和數位簽章是兩種確保訊息完整性和真實性的機制，但有一些差異：

訊息鑑別碼（MAC）[1]是一種對訊息應用密鑰的雜湊函數，以生成固定長度的摘要。這個摘要可以用於驗證訊息是否被篡改。MAC 使用共享密鑰，並且只能由知道該密鑰的人來驗證和產生。因此，MAC 提供了訊息的完整性和真實性。通常，MAC 是將訊息與密鑰作為輸入，通過訊息鑑別碼算法進行運算，生成一個摘要，這個摘要與訊息一起發送。

接收者在接收到訊息後，使用相同的密鑰和相同的訊息鑑別碼算法對接收到的訊息進行運算，得到一個新的訊息鑑別碼。接著，接收者將計算得到的訊息鑑別碼與發送者傳遞的訊息鑑別碼進行比對。如果兩者相同，則可以確定訊息在傳輸過程中未被篡改或損壞。

訊息鑑別碼主要提供了訊息的完整性驗證，因為只有擁有正確的密鑰才能生成相符的訊息鑑別碼。然而，訊息鑑別碼無法提供訊息的真實性驗證或非否認性，因為發送者和接收者可能共享相同的密鑰，無法證明特定的發送者身份。

數位簽章（Digital Signature）是基於公開金鑰加密技術的機制，用於證明訊息的完整性、真實性和身份驗證。數位簽章使用發送者的私鑰來加密訊息的摘要，接收者可以使用發送者的公鑰來驗證簽章的有效性。數位簽章提供了訊息的完整性、真實性和非否認性，因為只有擁有私鑰的人才能生成有效的簽章，並且任何人都可以使用公鑰來驗證簽章。

---

[1] Message Authentication Code (MAC), also referred to as a tag, is used to authenticate the origin and nature of a message. MACs use authentication cryptography to verify the legitimacy of data sent through a network or transferred from one person to another.

總結來說，MAC 和數位簽章的主要差異在於使用的技術和提供的安全屬性。MAC 使用對稱密鑰加密，只提供完整性和真實性的保護，而數位簽章使用非對稱密鑰加密，提供完整性、真實性和非否認性的保護。

2. 請問文件訊息鑑別碼的作用為何

文件訊息鑑別碼的主要作用是驗證文件的完整性和真實性。當文件需要在傳輸或存儲過程中被保護時，文件訊息鑑別碼可以用來檢測文件是否被篡改或損壞。

完整性驗證：文件訊息鑑別碼可用於確定文件是否在傳輸或存儲過程中被修改或損壞。接收者可以重新計算文件的訊息鑑別碼並將其與原始的訊息鑑別碼進行比對。如果兩者相同，則可以確定文件的完整性，即文件未被篡改。

真實性驗證：文件訊息鑑別碼可以用於確定文件的真實性，即確認文件是由特定的發送者創建或授權的。只有具有正確密鑰的發送者才能生成相符的訊息鑑別碼，這使得接收者能夠驗證文件的真實性。

防篡改保護：文件訊息鑑別碼可以作為一種保護機制，防止文件在傳輸或存儲過程中被未經授權的人修改或篡改。即使文件的一個小部分被修改，重新計算的訊息鑑別碼也將與原始的訊息鑑別碼不匹配，從而提供了對文件的防篡改保護。