University of Taipei

Computer Science

Homework 4

Student ID: U10916024

Student: Cheng-Hao, Zhang

張呈顥

2023

1.評估保密技術之優劣

要評估加密技術之優劣，目前主要是根據計算安全性來評估之。現行主流的加密方式主要根據數學理論來保全其安全性，如質因數分解與離散對數，這些理論基礎的演算法於**現代電腦**具有計算安全的。

但由於量子電腦的誕生，量子計算的速度遠超過現今的二進位制電腦，到了那時候現代之加密演算法將再無計算安全性可言。鑒於此，進而發展出量子密碼學、後量子密碼學等研究領域，以未雨綢繆抵禦量子電腦對於加密技術之威脅。

2. 密碼系統之安全性程度

- **無條件安全(Unconditionally Secure)**

非法使用者不管截獲多少個密文，用盡各種方法還是沒有足夠資訊可以導出明文之機密資料。

- **計算安全(Computationally Secure)**

以目前或未來預測之科技、合理之資源設備下，要破解密碼系統需要一段相當長的時間，例如數百年。

關鍵在於破解密碼是否合乎下列兩種條件：破解密碼所需的成本是否合乎該訊息的價值。破解密碼所需的時間是否超過該鑰匙的壽命。

如果能克服上述兩個條件的密碼系統，便稱之為計算上的安全（Computationally Secure）；密碼系統安全與否的衡量標準在於破解者需要多少時間、花費多少成本才能破解密碼。

8.DES vs. AES

	DES	AES
資料區塊	64 bits	128 bits
金鑰長度	56 bits	128/192/256 bits
重複運算次數	16 次	10/12/14 次

|X|是輸入區塊的大小，L 是單次輸入最長長度，q 是有幾則訊息。用 3DES 和 AES 試算一下:

3DES 的$|X|$是 64bit，若希望$q^2/|X| = 1/2^{32}$(攻擊者區分真亂數和 CBC/CTR 的機率是$1/2^{32}$)，$q^2 = 2^{32} \rightarrow q = 2^{16}$，加密 65536 個訊息後要換 key。

AES 的|X|是 128 bit，$q^2/|X| = 1/2^{32}$，$q^2 = 2^{96} \rightarrow q = 2^{48}$，這個大小夠用非常非常久。

14. 密碼系統之安全性程度

- 無條件安全(Unconditionally Secure)

  非法使用者不管截獲多少個密文，用盡各種方法還是沒有足夠資訊可以導出明文之機密資料。

- 計算安全(Computationally Secure)

  以目前或未來預測之科技、合理之資源設備下，要破解密碼系統需要一段相當長的時間（例如數百年）。