S0254023 顏梵文

網路安全AES報告

本次在課堂上，學到了關於AES的相關知識，並且又再度利用本次作業，上網觀摩他人寫的AES程式。AES為美國國家標準與技術學院徵選的加密法比賽中評選出來的最終標準，在AES中一共可以使用3種不同的金鑰，分別為128, 192, 256位元。同時AES是使用Substitution-Permutation而非Feistel架構，因此加解密速度較DES更加快速、需要更少記憶體，並且容易實作，同時所有的加密系統皆為公開的，因此目前被廣泛的使用。

而在AES中，最為重要的就是四個步驟：1、AddRoundKey 2、SubBytes 3、ShiftRows 4、MixColumns。四者功能分別為1、每回合金鑰與原矩陣使用xor合併，並產生新的回合金鑰。2、將矩陣和s-box進行轉換，因為和GF 反元素有關，因此本操作具非線性特性，因此能夠避免簡單的代數攻擊。3、每一行遵循一定偏移量進行偏移。4、每一列的四個位元透過線性變換結合，並且每一列元素分別作為1, x, x^2, x^3的係數，合併之後變成GF中的一個多項式，最後在和一個固定的多項式作modulo。在這四個步驟中，ShiftRow和MixColumns 為這個系統提供了diffusion。

目前AES加密法算是相對比較安全的，唯一有成功攻擊的方法D.J.Bernstein公布的一個快取時序攻擊法，並且以此破解了AES加密系統的伺服器。但是由於攻擊演算法使用了兩億多條明碼，因此在實用性上並不好。