物件導向程式設計

期末報告

B10756029 吳振聖

B10756020 李佳錚

B10756051 陳廷宇

指導老師：許志仲 老師

1. **研究動機**

之前在資料庫的課程中，都會做註冊,登入系統，如果一個註冊系統在存你的pw是直接存明碼的話，相當的不安全，而這次在找演算法的時候發現了雜湊演算法，可以在要存去資料庫的密碼先進行雜湊處理在存到DB，而登入時就把User輸入的pw進行雜湊處理再與資料庫比對，在傳遞密碼時就不是明碼在跑了，而是雜湊值，相對來說就比較安全。

1. **演算法**
2. **SHA-256**

SHA-2，名稱來自於安全雜湊演算法2（Secure Hash Algorithm 2）的縮寫，SHA256是SHA-2下細分出的一種演算法。

是一種從任何一種資料中建立小的數字“指紋”的方法。雜湊函式把訊息或資料壓縮成摘要，使得資料量變小，將資料的格式固定下來。該函式將資料打亂混合，重新建立一個叫做雜湊值（或雜湊值）的指紋。雜湊值通常用一個短的隨機字母和數字組成的字串來代表。

對於任意長度的訊息，SHA256都會產生一個256bit長的雜湊值，稱作訊息摘要。

1. **AES高階加密標準(AES,Advanced Encryption Standard)**

AES為最常見的對稱加密演算法。

對稱加密演算法也就是加密和解密用相同的金鑰。

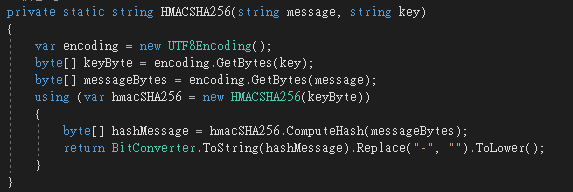
AES加密解密的祕鑰有一對，一個是IV一個是KEY，並且他們的長度都有嚴格要求。

1. **困難**

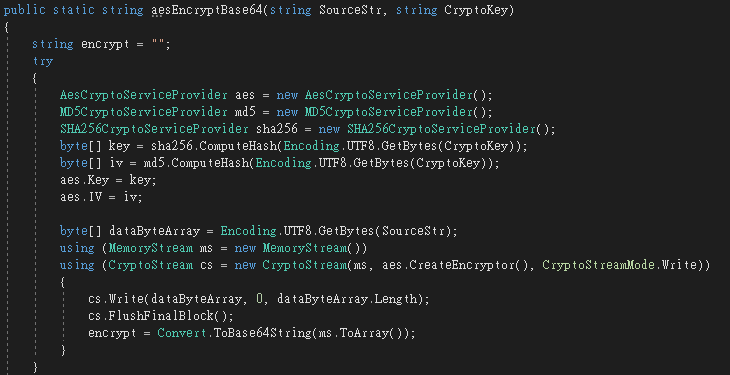
我覺得要理解加解密真的要花時間，但最困難的點我自己是覺得在要如何應用所學，我的題目是校務管理系統，我想了很久都還是不知道要怎麼用上課所學，網上所看的演算法去應用到我的題目，後來想到的就只有字串的加解密，以及密碼的雜湊處理。

1. **關鍵程式碼**

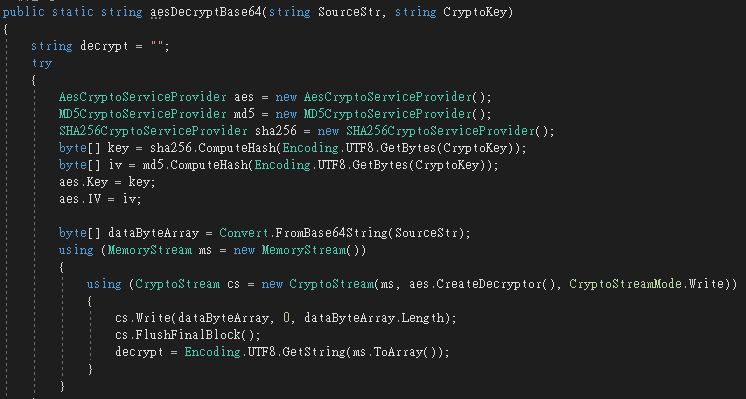
**SHA-256**

****

**AES加密**



**AES解密**



1. **心得**

**B10756029 吳振聖:**

這次做期末專題看了很多演算法，讓我學到很多東西，以前聽過彩虹表但不知道它的用途是幹嘛，這次也讓我了解原來密碼學也是門好深的學問，就像以前用DES加密後來DES被破解說不安全就有就出了AES來取代原先的DES，AES又分很多的加密模式CBC、ECB、CTR、OCF、CFB光看我就頭昏眼花了，還有就是像是MD5以及SHA-1已經被證明不夠安全（在可接受的時間範圍內，可以找到內容不相同輸入卻得到相同輸出）雜湊不是加密，加密需要密鑰，且可以透過解密得到原文（加密可逆）

雜湊不需密鑰，無法逆向解出原始輸入（雜湊不可逆）透過這次讓我對加解密有更進一步的認識，也讓我了解雜湊演算法是如何運行的，這次的期末專題去了解演算法應用到系統上，對我來說是一個很好的學習經驗。