電腦安全 Final report By 9817059 李 揚

Explanation of my code:

首先，我讓server端和client端共享一個key: “hackerneverdie”，然後我再聽到事件(keyboard相關事件)，會去執行handle，如果是按下去的時候，我會把這個按下的鍵記錄起來(英文字全用大寫表示)，用RC4演算法加密後傳到sever端，server端因擁有共享的key ”hackerneverdie”，所以可以用RC4產生同樣key stream解密回來。

Introduction to RC4:

再加密的過程中，用exclusive or搭配一個key是一個很不錯的想法。因為不論是加密和解密都可以用一樣的方式達成。RC4就是利用這樣的概念。

不過，如果只單純的用一個永不變動的key，會遭遇到一個問題，就是有可能被統計的方法破解的方式破解。

如何破解呢?先統計各個字母被使用道的次數。然後利用此資訊達到猜到此key是什麼。先從key的長度為一的狀況開始解釋吧!假設key的長度是1的話，代表每個字母每次加密都會對應到一個特定的字母。如此一來我就可以統計這些密文里各個字母出現的頻率，對應到我之前統計的資訊，猜出這字母為什麼字母。

Ex:

密文裡出現頻率 統計個字母的資訊

G: 10.2% E:9.3%

C: 7.24% A:6.8%

F: 3.68% I:4.1%

W: 2.34% O:3.2%

….,..

在此，我就可以大致猜到G很有可能為E，C很可能為A….，再加上可以刪除會出現無異議英文單字的狀況，很快就可以破解。

key長度為n也是相同道理，只是說我的在密文裡統計必須分開:

1,n+1,2n+1….的字母做一個統計

2,n+2,2n+2….的字母做一個統計

3,n+3,2n+3…的字母做一個統計

……

以此類推。

就可以破解這樣的加密方式了。

所以我們知道key如果固定是很不安全的。

除此之外，很直覺得可以知道key如果是一個普遍存在的英文單字，也是很容易破解的，太短也是很容易破解。

所以RC4考慮到了此點，設計出了這樣的演算法。

1. 先得到一個 key
2. 經過一個key scheduling algorithm(KSA)，把這個key擴充到255個字母。在此KSA中，我不斷做置換的動作，以免保留了原來的key的特性。

Ex:

如果hackerneverdie經過某很簡易的KSA

變成hackerneverdeihackerneverdeihackerneverdei….(e跟i對調)

還是會很容易破解。但如果可以經過不斷的置換就可以增加破解難度。

所以在RC4的過程中，不斷的置換。搭配一255各個不同字母的陣列(因各個字母都用不同的可以達到最離散的效果)，去做置換。

1. 因為我知道如果用固定key還是很容易被破解，所以我還要再經過一個PRGA(pseudo-random generation algorithm)的過程，使得第一個出現的key不會跟第二個一樣。
2. 利用前三步產生的key stream跟我的plain text做exclusive or就可以達到加密的效果

而接收端只要跟發送端分享通一個key並且跑RC4就會產生一樣的key stream，如此一來就可以利用此key stream作解密的動作。

Usage:

如課堂所教，RC4會在無線網路的傳輸部分，因為方法單純，執行起來並不會太花時間，不過會有一些安全性的問題。

心得:

由於我之前沒寫過socket programming的相關程式(除了這次的HW1)，所以整體來說，這次作業花了我不少心力，不過也因此學會了socket programming簡易的server, client端的撰寫方式。

Hook這個功能我也是第一次碰過，查了很多資料再加上助教的解惑才漸漸摸熟。