Final Project

成員:

60947005S古佳儫 Email: johnson530893@gmail.com

60947038S鄭博升 Email: s7023369667@gmail.com

主題:

# A Formal Analysis of IEEE 802.11's WPA2:

# Countering the Kracks Caused by Cracking the Counters

動機:

在作業一中破解WEP的題目，我們花了很長的時間對WEP做基本的探討，也在途中發現WPA2也已經被破解，但後來發現WPA2和WEP最大的差別在於Key是否是固定的，這也讓破解的難度大大提升，所以希望能試看看能否實作出破解WPA2的wifi密碼。

參考文獻:

網路上的wpa2破解介紹

<https://www.techbang.com/posts/54483-wpa2>

4-way handshake介紹

<https://kezeodsnx.pixnet.net/blog/post/35561270-4-way-handshake>

此篇paper網址

<https://www.usenix.org/conference/usenixsecurity20/presentation/cremers>