

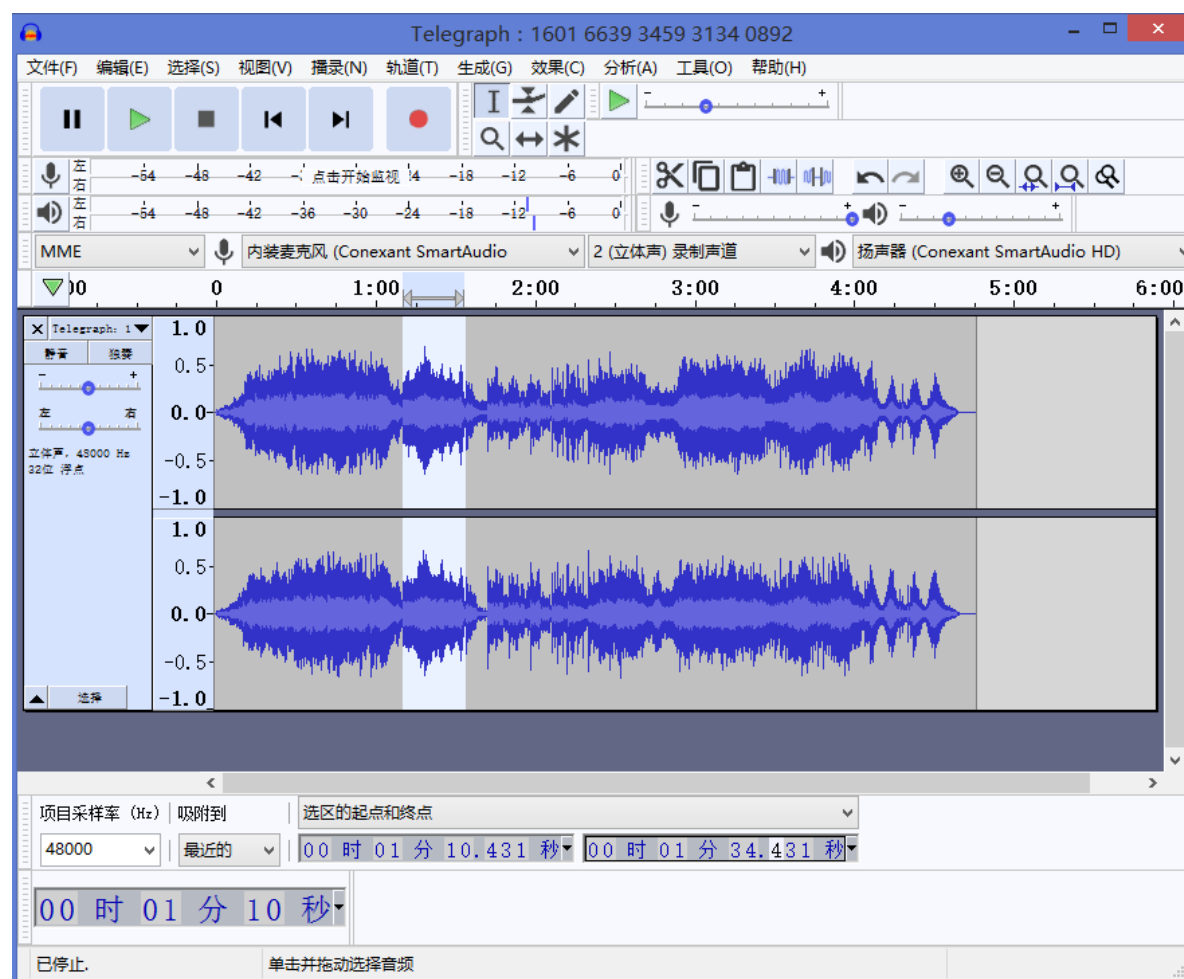
Week 2 Writeup

MISC

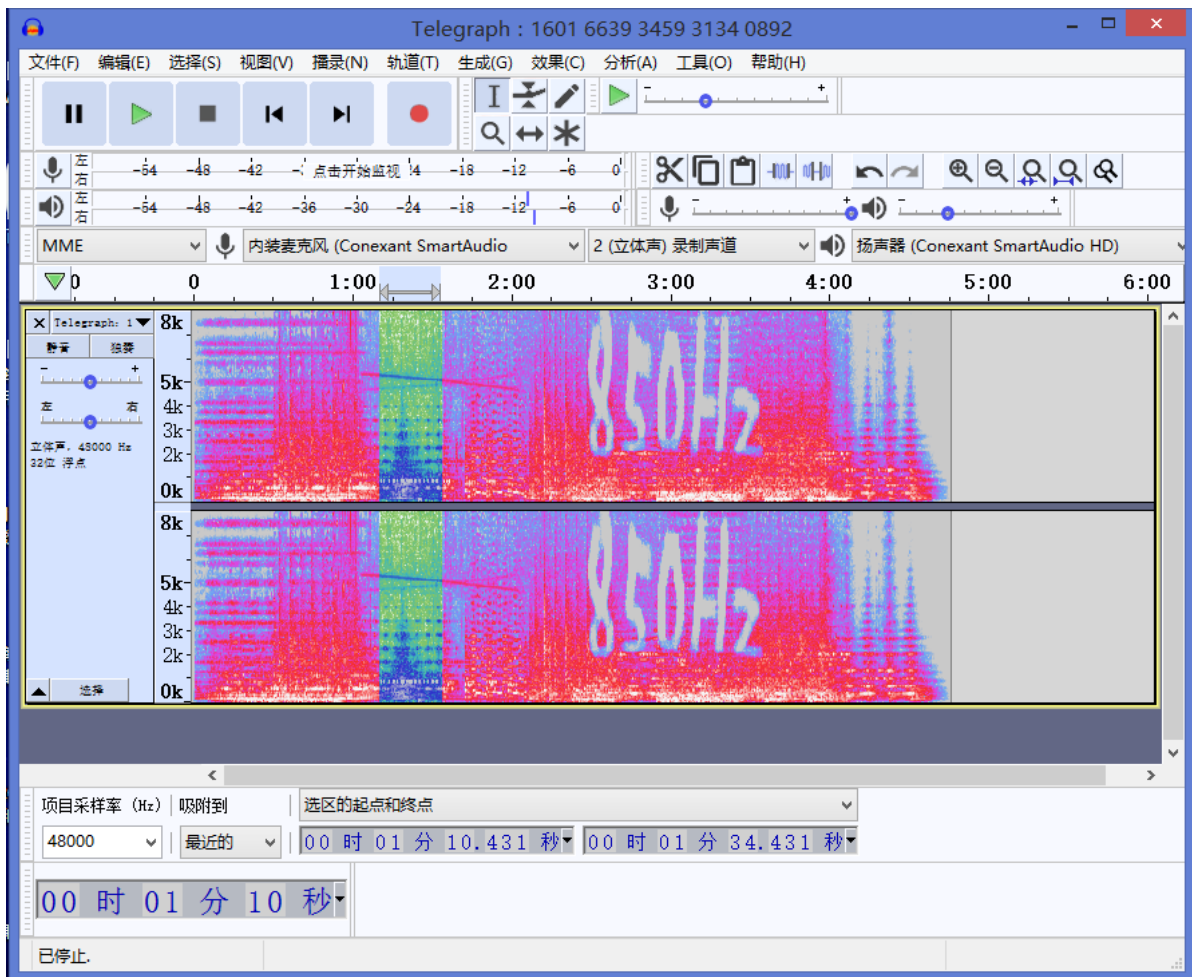
Telegraph : 1601 6639 3459 3134 0892

打开链接是一首 mp3 格式的曲子，存到本地后用 Audacity 打开。

试听一遍察觉中间 1:10 至 1:34 处有类似摩尔斯电码的声音。

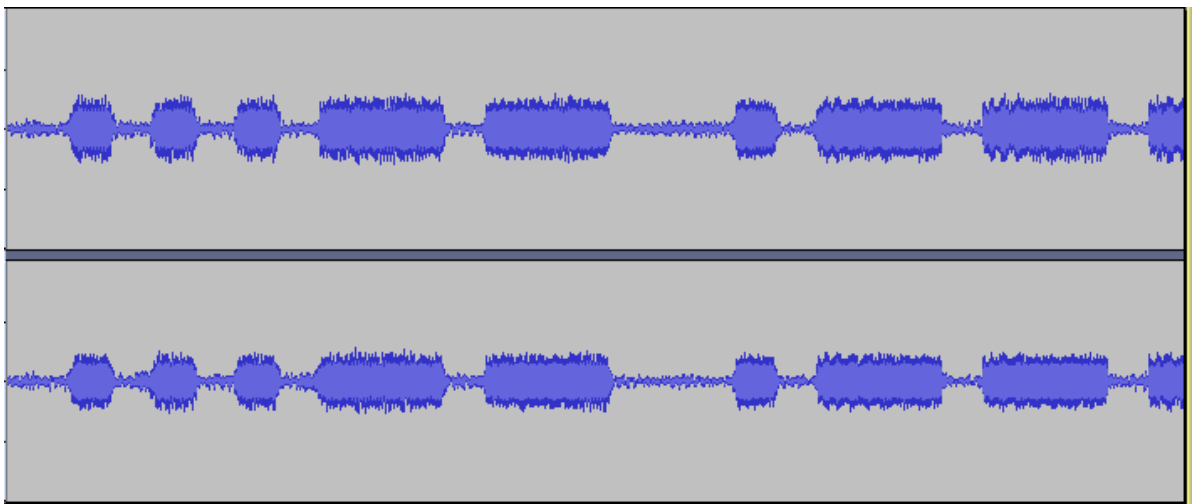


打开频谱图，发现提示 850Hz。



(然而解完题了发现这个提示好像没有也行)

将 1:10 至 1:34 的片段剪出，放大波形图视图，可以发现明显的摩尔斯电码。



逐个解出摩尔斯电码后可得到flag。

Crypto

WhitegiveRSA

题目给出了如下条件：

N = 882564595536224140639625987659416029426239230804614613279163

e = 65537

c = 747831491353896780365654517748216624798517769637260742155527

先用 yafu 将 N 分解为两个质数 p、q。

```
p = 1029224947942998075080348647219  
q = 857504083339712752489993810777
```

然后计算 d，代码如下：

```
def exgcd(a, n):  
    if n == 0:  
        return 1, 0  
    else:  
        x, y = exgcd(n, a % n)  
        x, y = y, x - (a // n) * y  
        return x, y  
  
def getReverse(a, n):  
    re, y = exgcd(a, n)  
    while(re < 0):  
        re += n  
    return re  
  
p = int(input("p:"))  
q = int(input("q:"))  
e = int(input("e:"))  
d = getReverse(e, (p - 1)*(q - 1))  
print('d = ' + str(d))
```

```
d = 121832886702415731577073962957377780195510499965398469843281
```

根据 $m = \text{pow}(c, d, n)$ ，得出：

```
m = 2559974471936861332250695601896749831380586717227729822077
```

最后用 libnum.n2s 将 m 转化为字符，得到 flag。