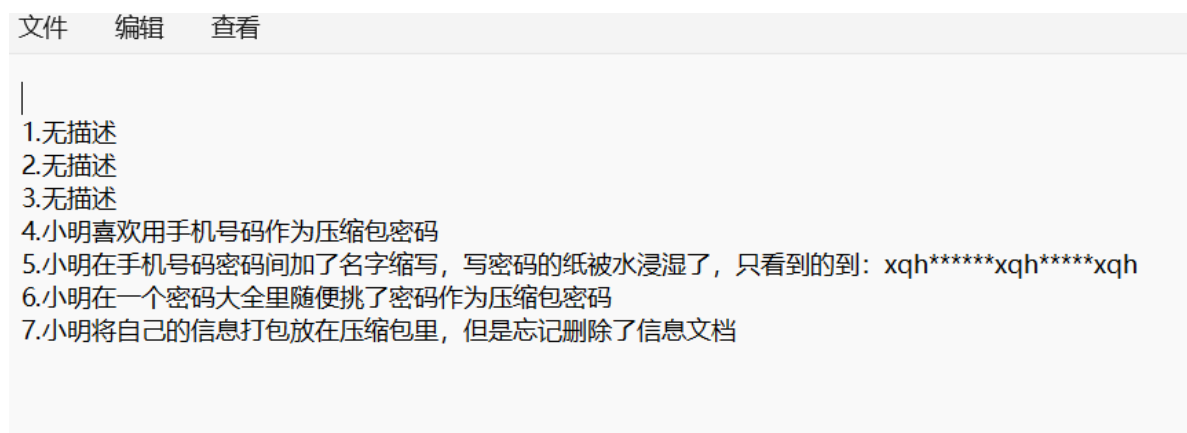
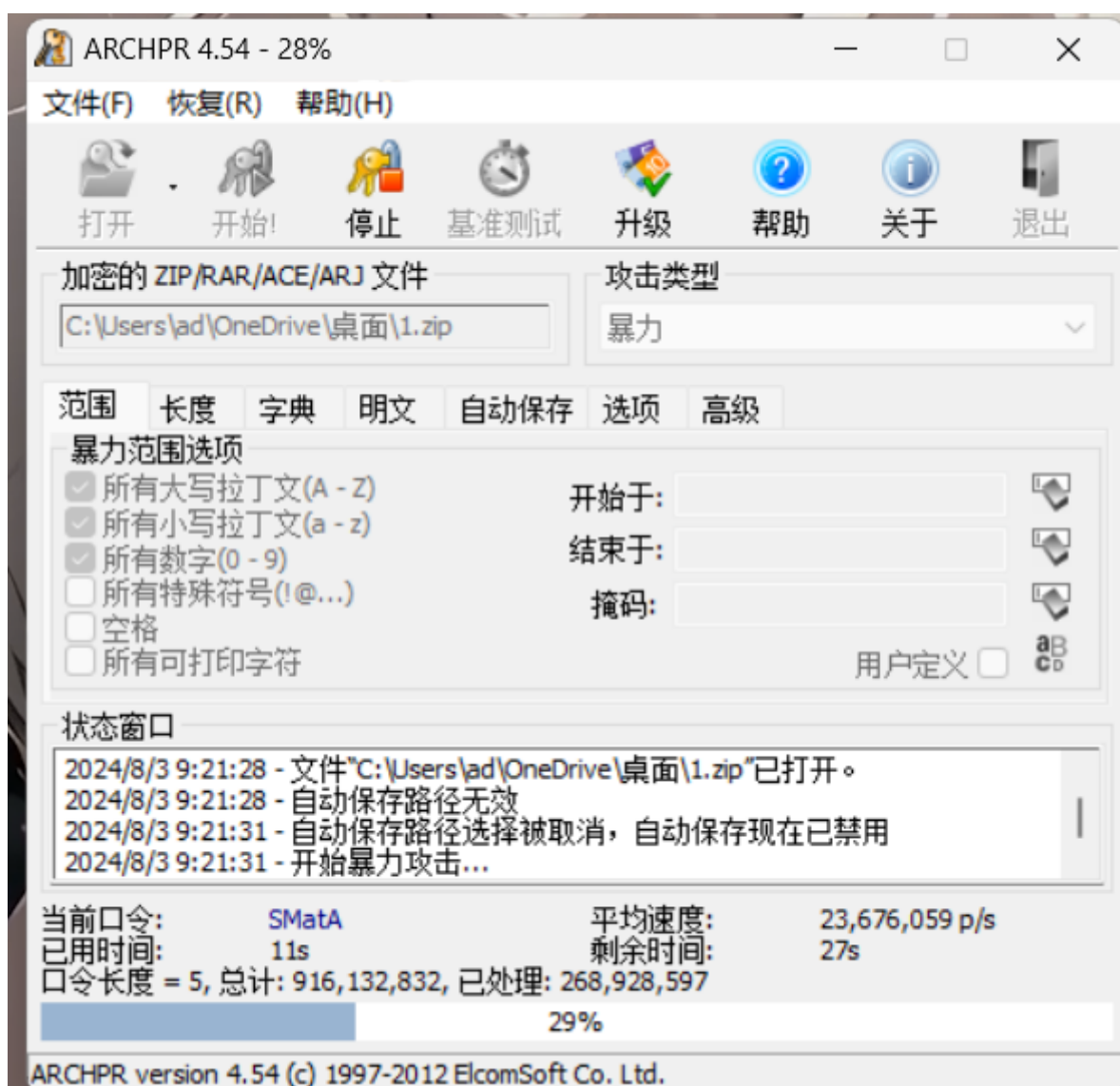


### 8.3

详读文件所有内容



第一次看见前三个全无描述直接断定暴力，后发现时间破解过长，随后改变思路

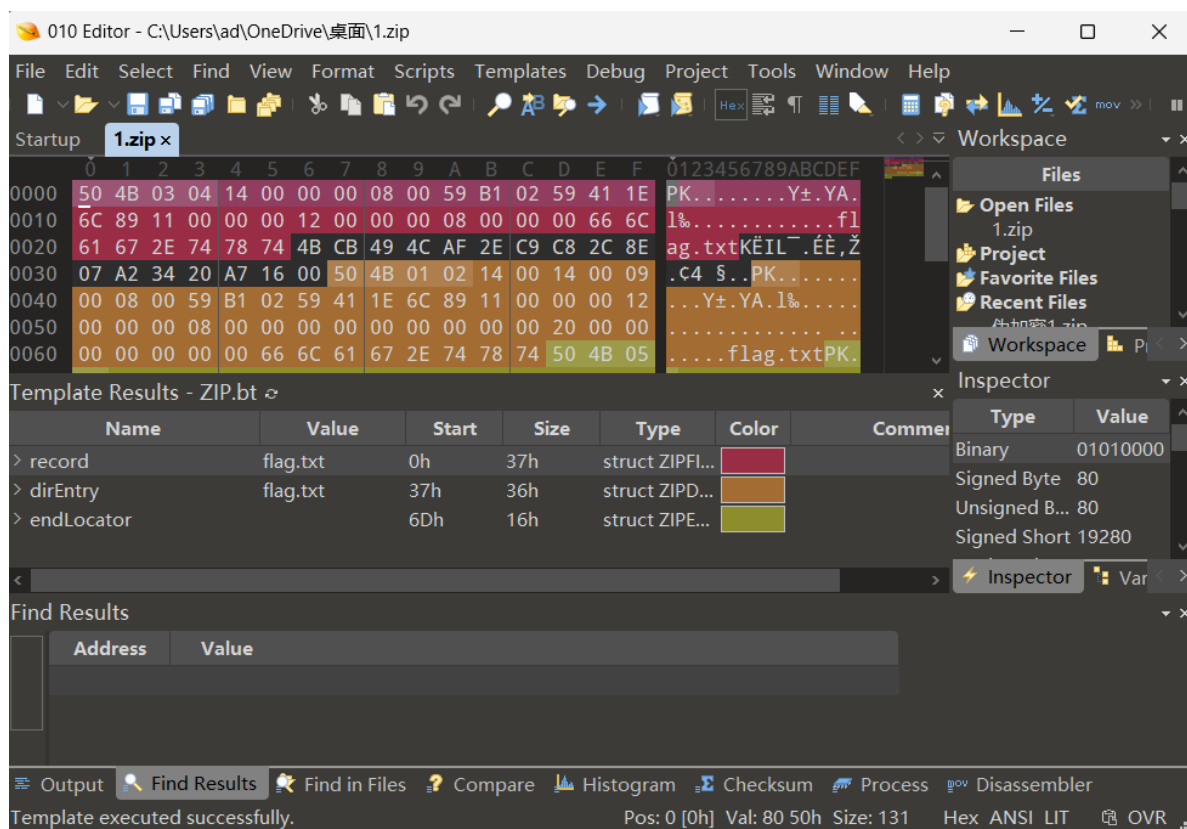


重新开始做题，明白不要太过武断想当然

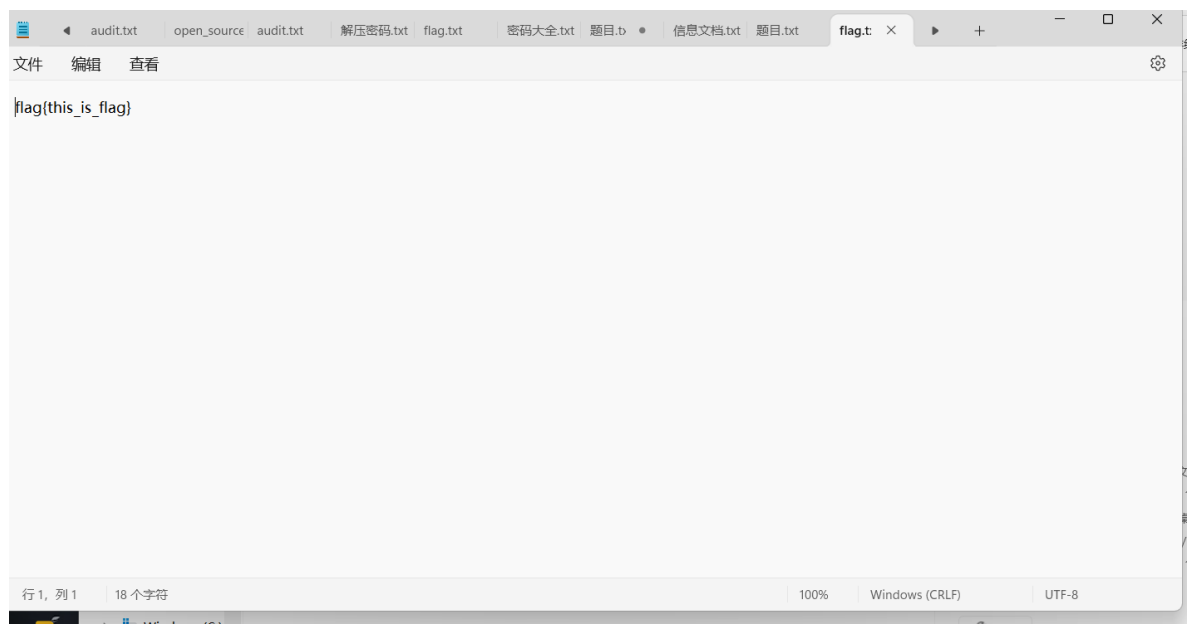
# 1.

用010打开文件发现第二处为14 00 09 00

判断其为伪加密



随后将其09改为了00 再打开文件顺利得到flag

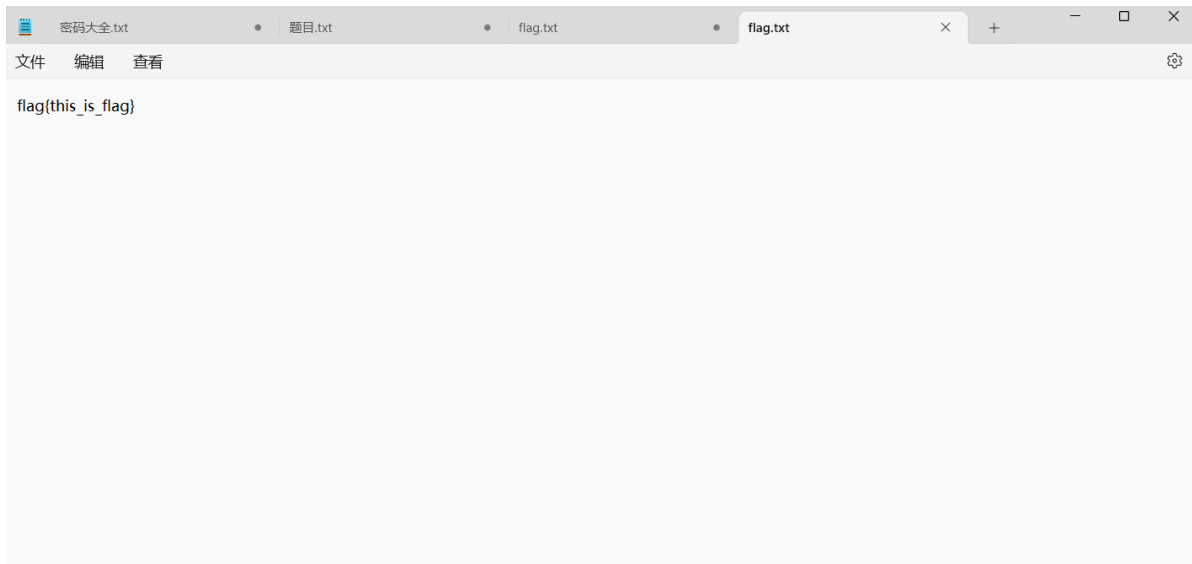


# 2.

用010打开文件发现第一处和第二处都为00 09 00

此时在思考是伪加密还是真加密，先试着在此处篡改判断是否为伪加密

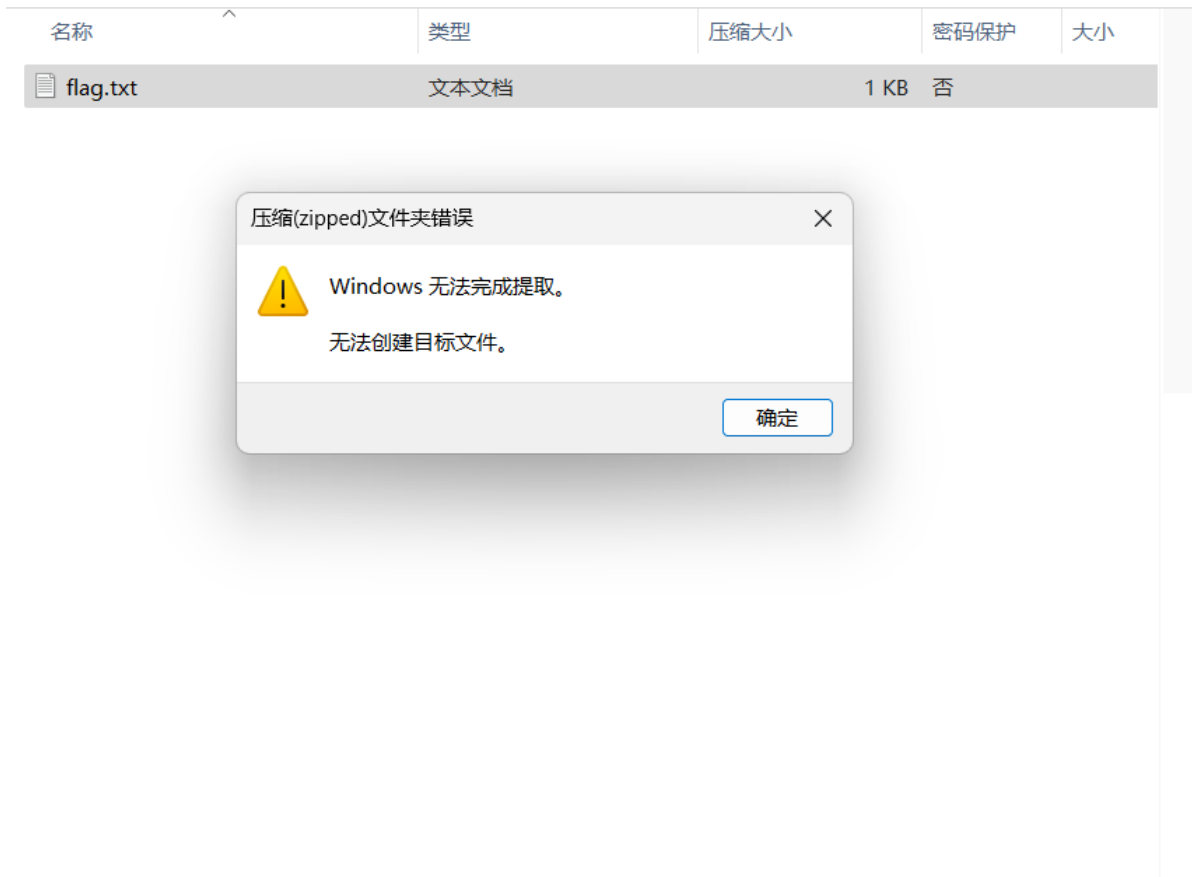
成功破解，确定其同为伪加密



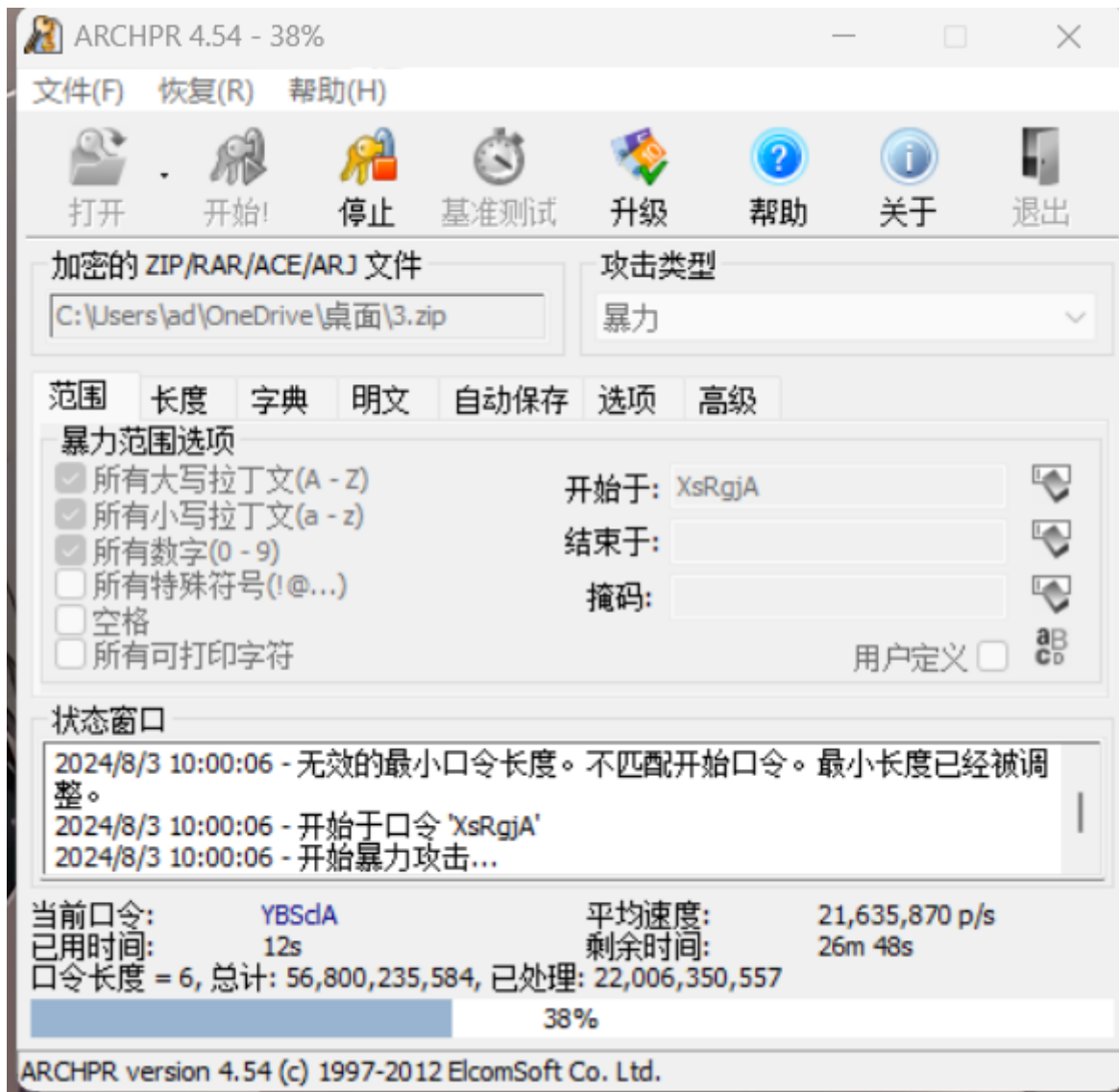
### 3.

依旧用010打开，发现第一处和第二处同为 00 09 00，在伪加密和真加密中待判断

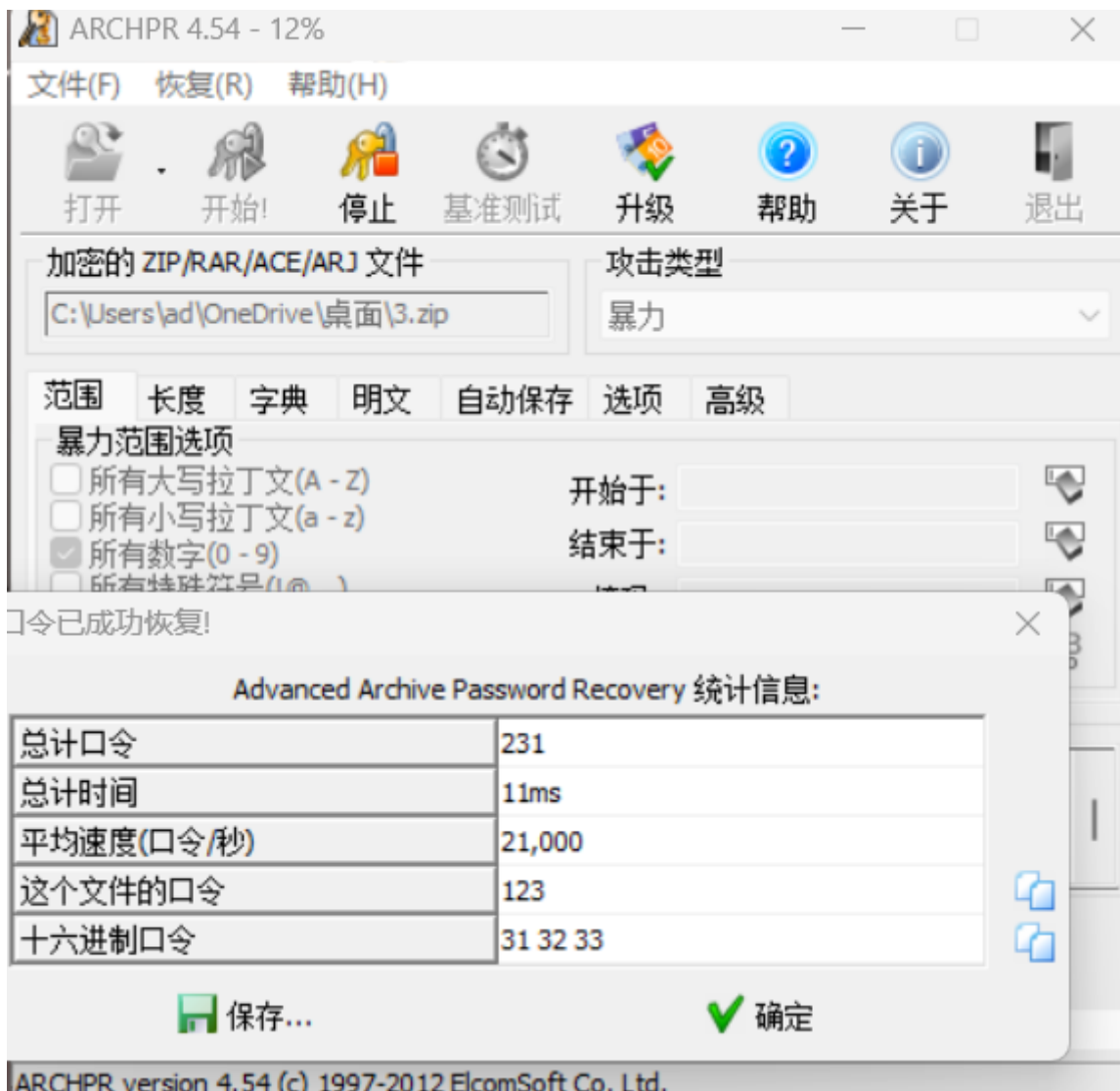
随后试着改09为00判断是否为伪加密



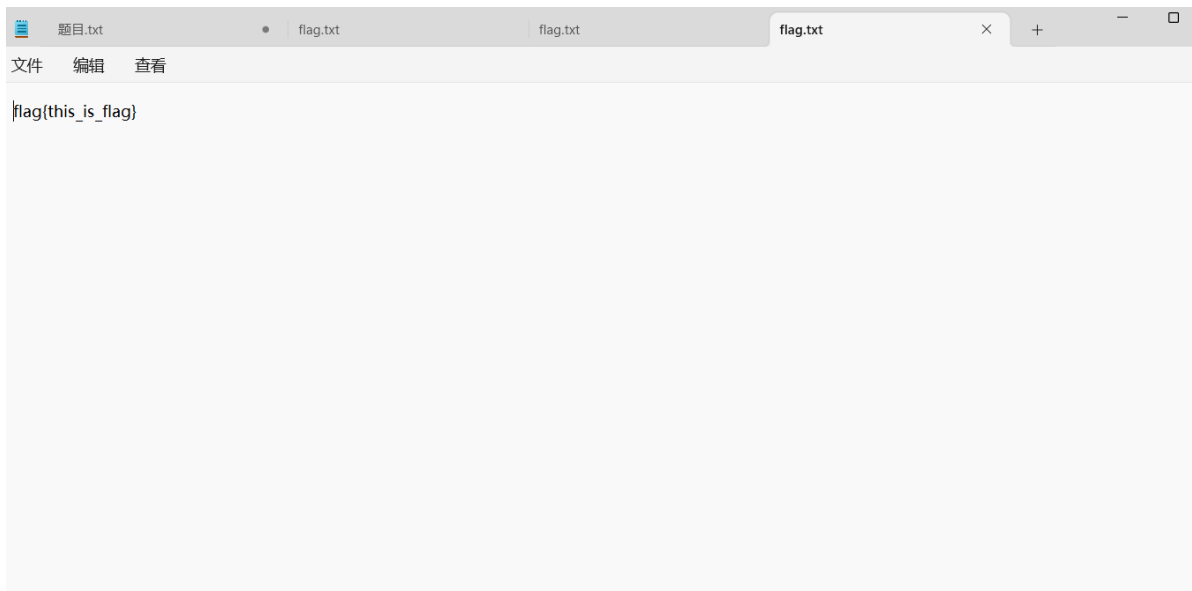
发现依旧打不开文件确定其为真加密，因为其无描述随后使用archpr暴力打开



第一次试验没有记住一些必要的点，不能有开始的口令，且在描述的情况下先全数字再前三个全开

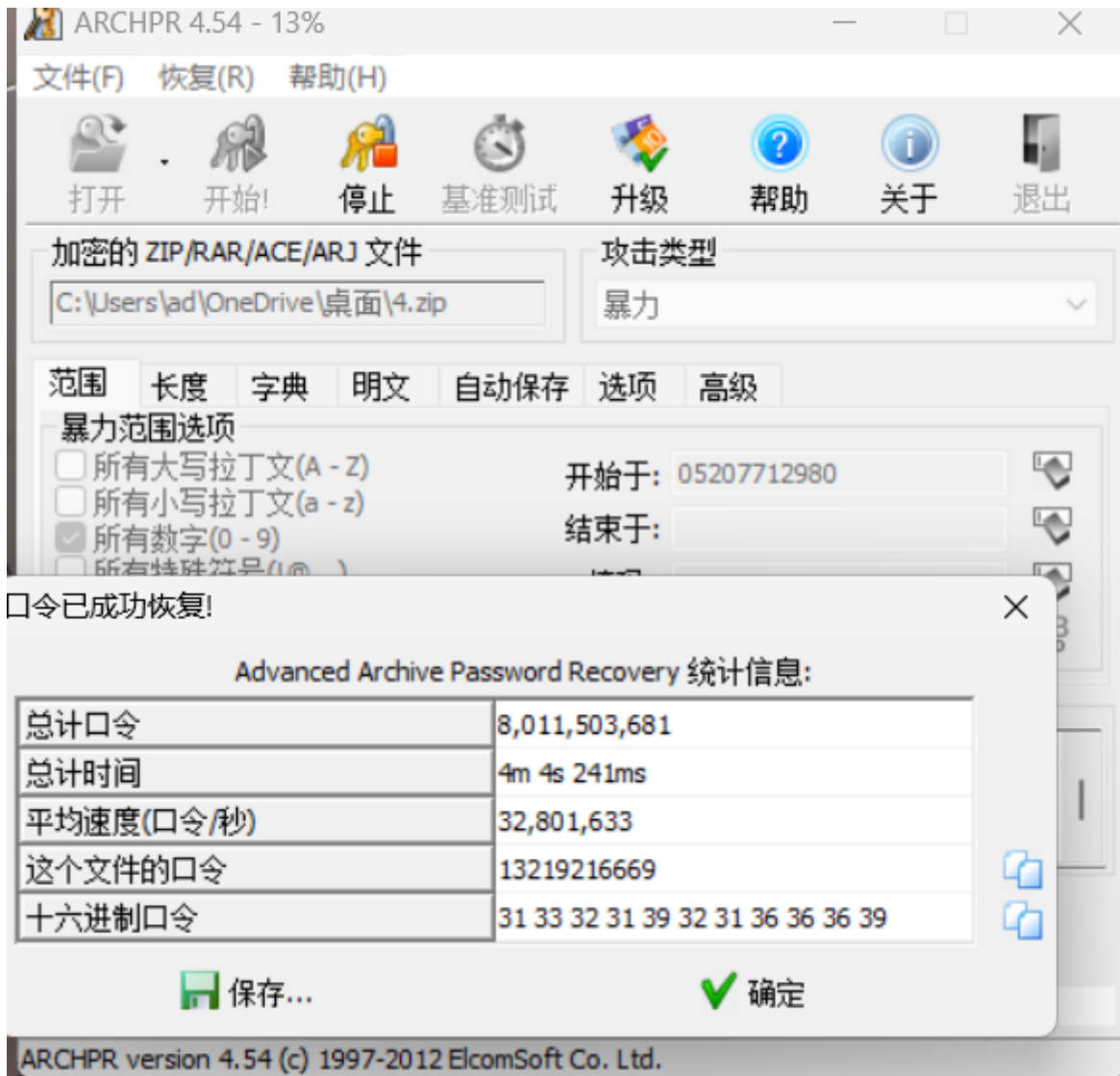


成功暴力打开

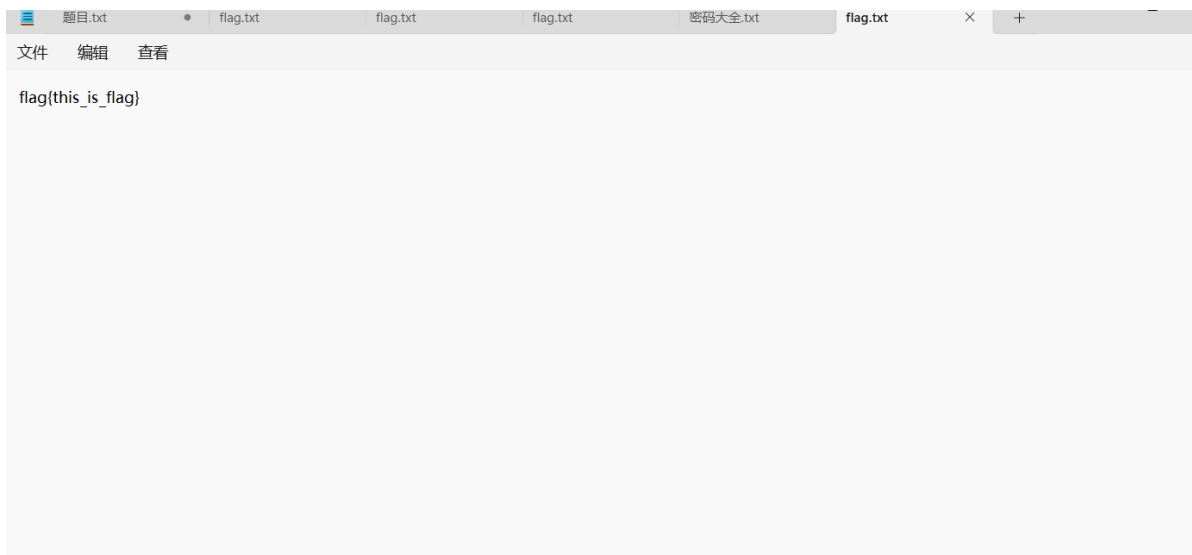


4.看到关键信息为手机号,便把暴力范围圈定了数字并且长度锁定在十一位

随后在一段时间后便成功破解

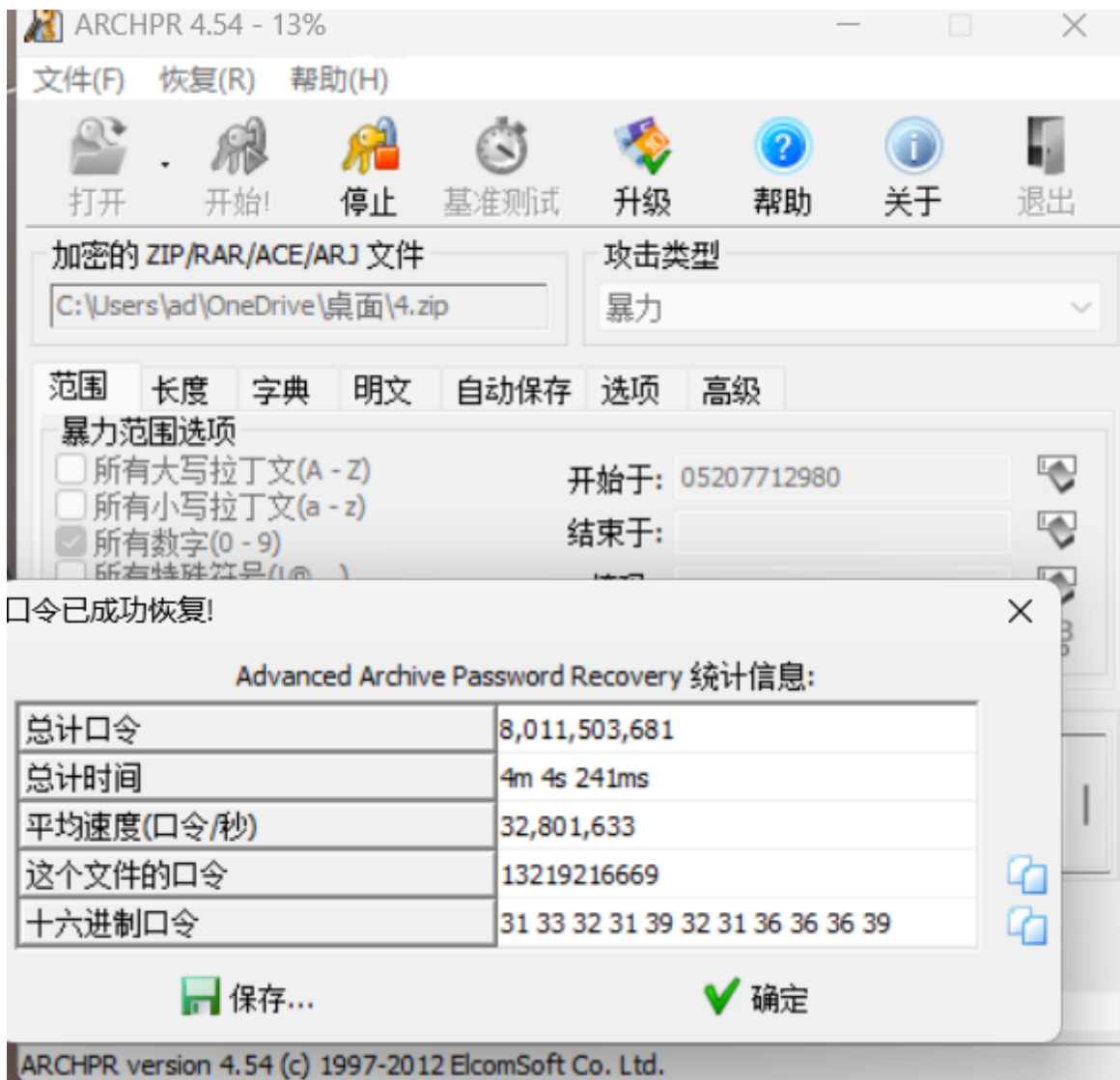


那个开始于哪里是我中途停止了一会然后连接上的

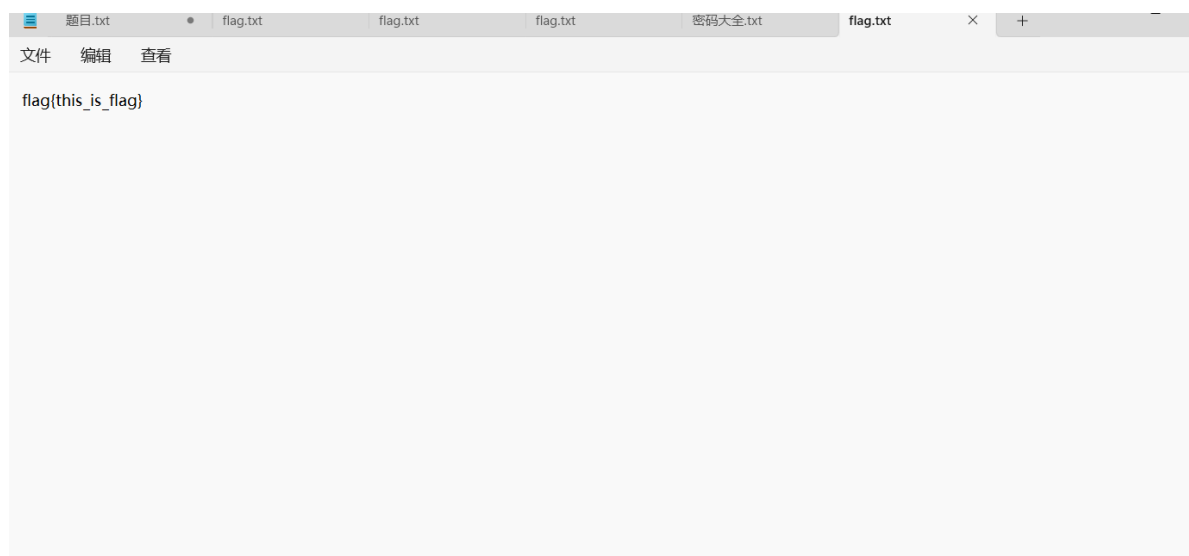


5.

读题发现是在手机号码间加入了名字缩写，所有便使用了工具的掩码破解，并且在暴力范围勾选了只数字



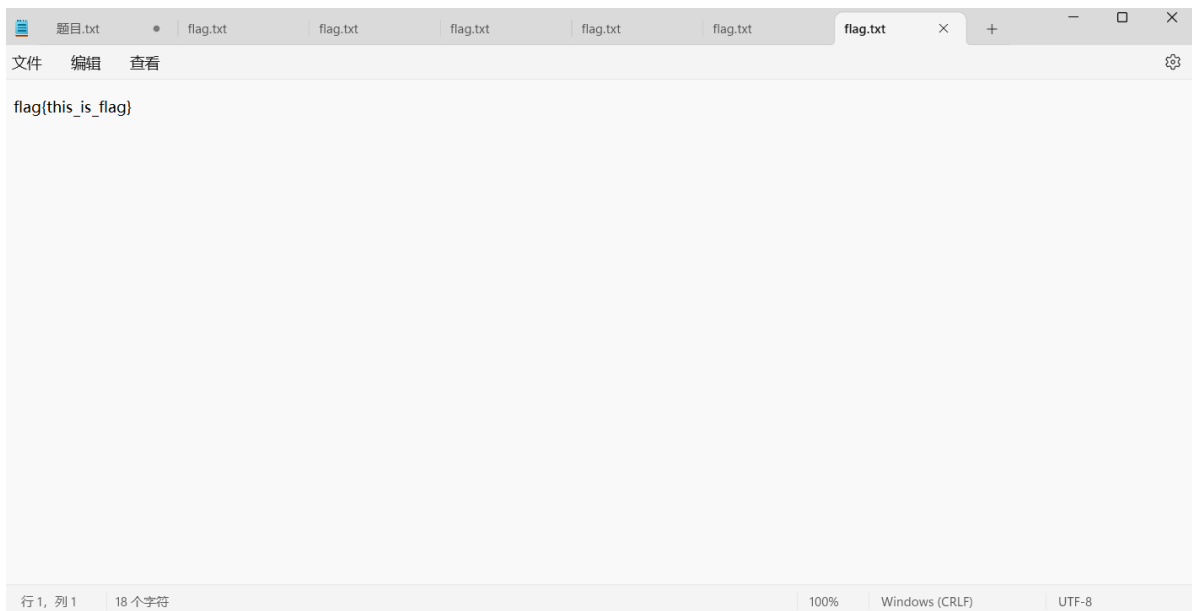
成功得到flag



6.

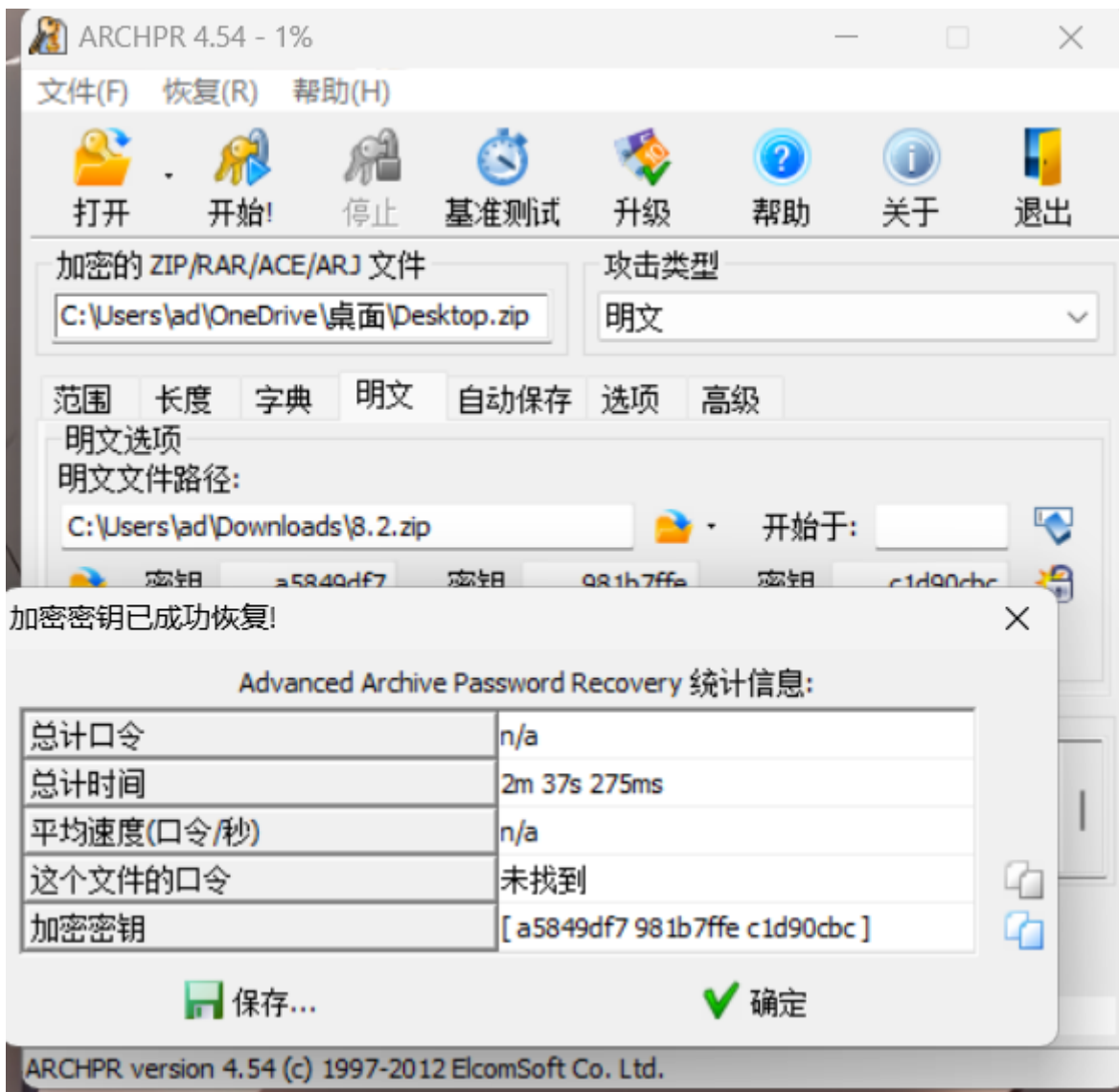
题目信息为在密码大全里找了个当密码，于是确定为字典破解，并把密码大全打开

得吃flag



7.

题目信息为将自己的信息打包放在压缩包里，确定为明文破解



保存为无密码的文件包后打开得到flag



```
flag{this_is_flag}
```