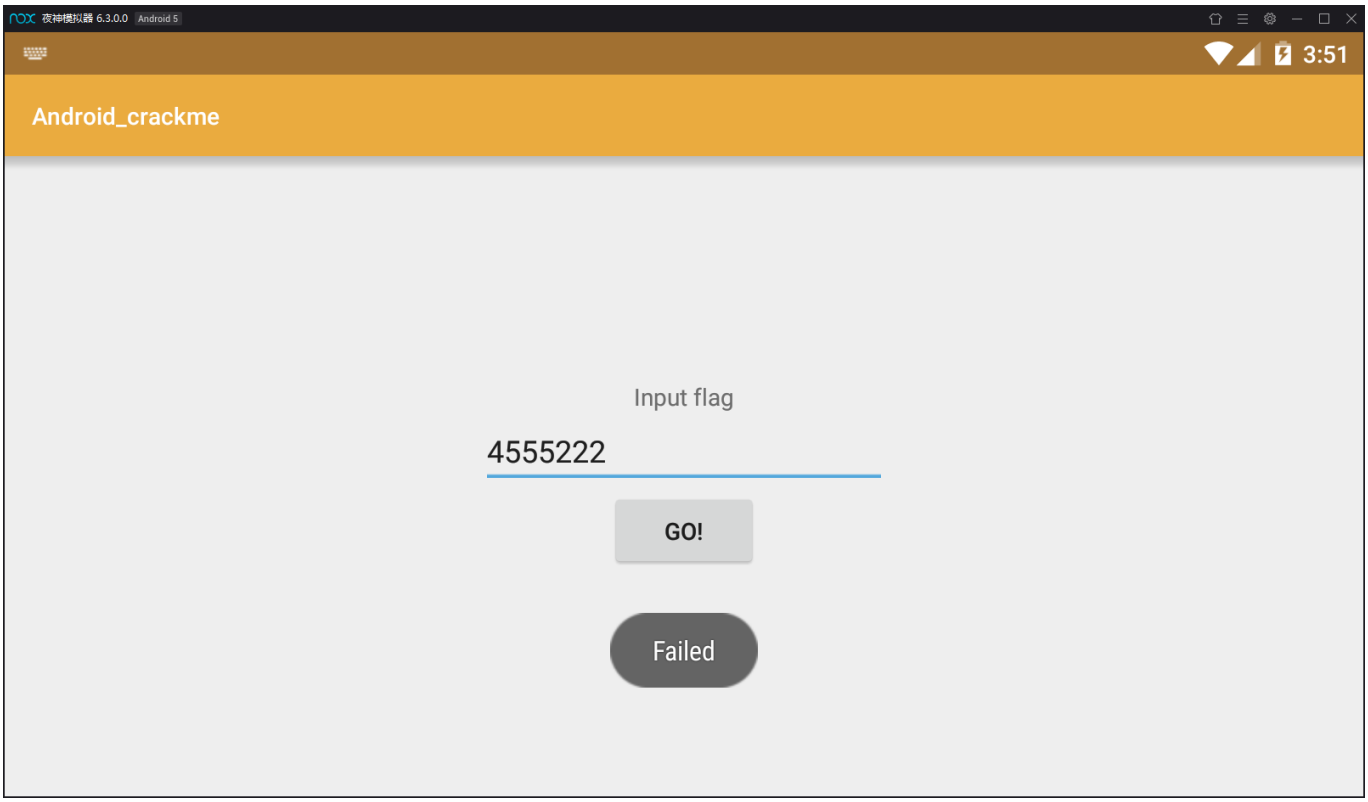
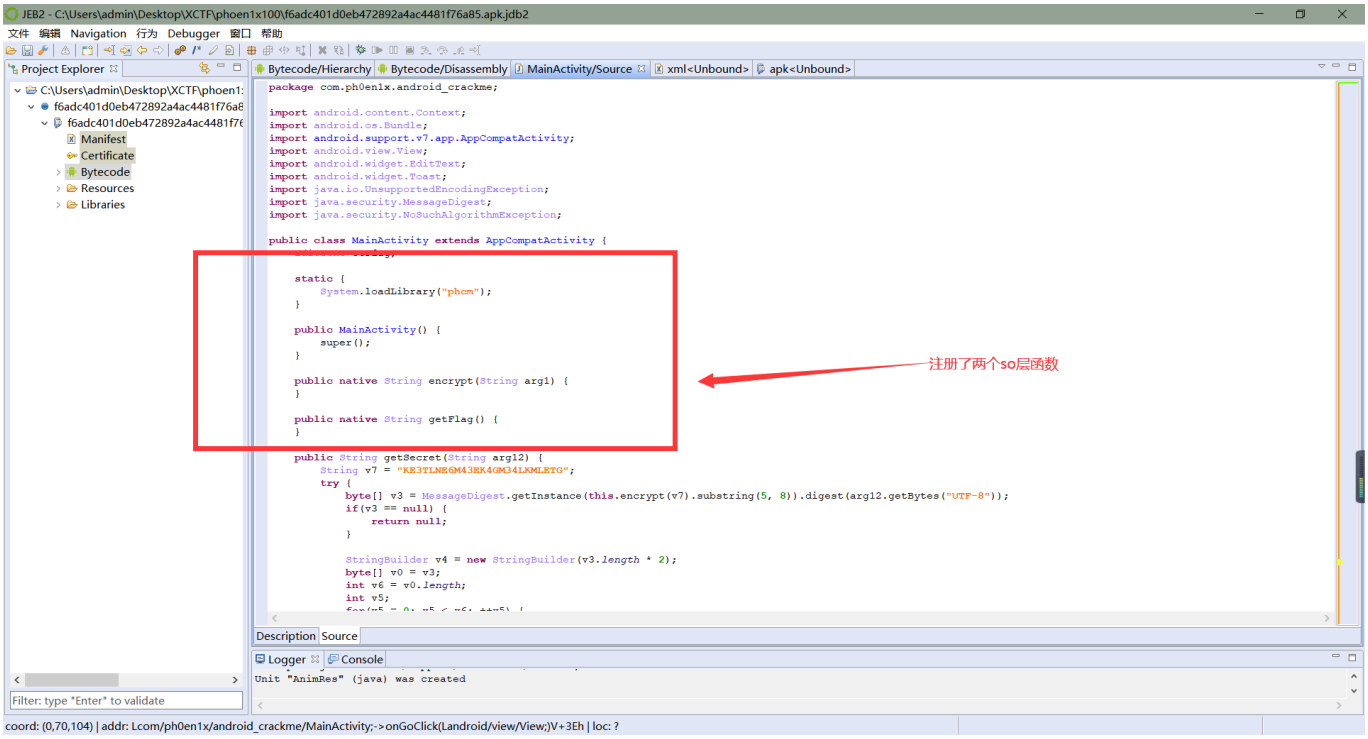
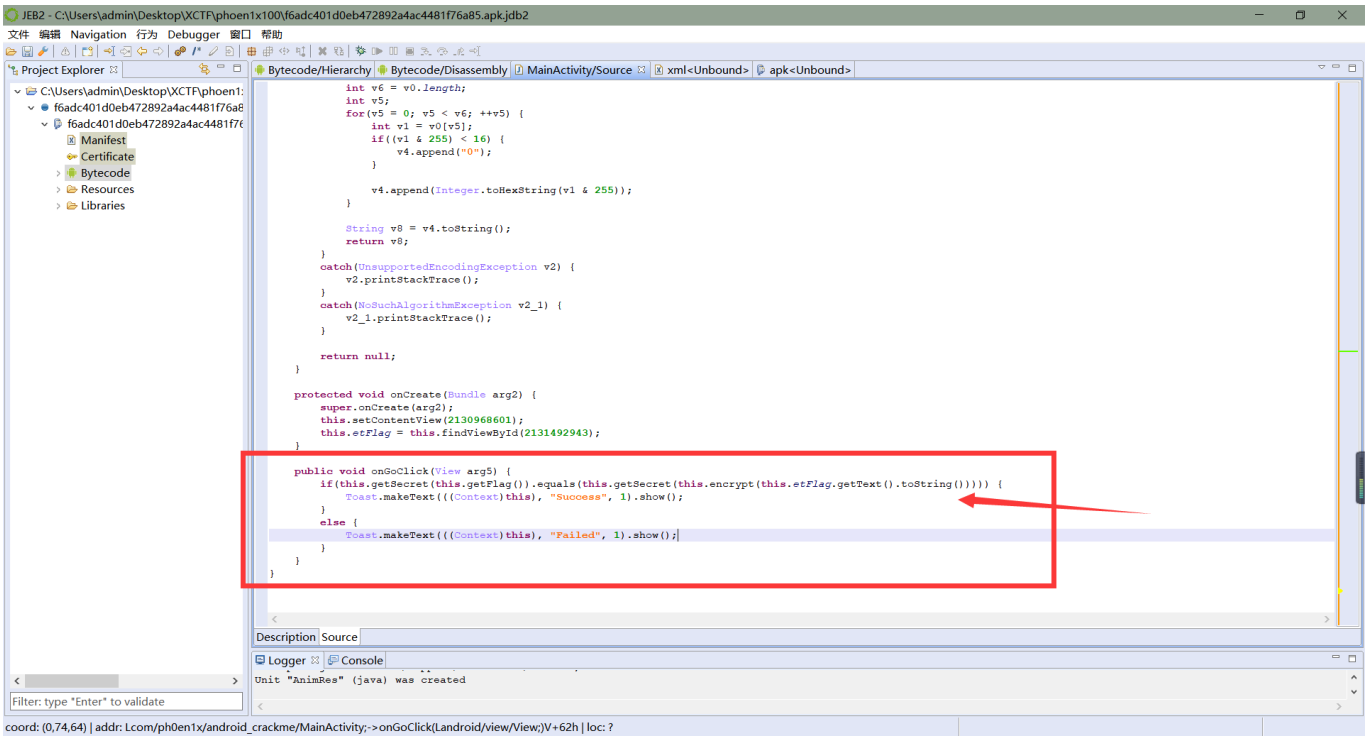
1、拖进夜神中安装运行，主界面只有一个输入框和一个按钮，随便输入信息，点击按钮后，弹出信息`Failed!`，如下图所示：

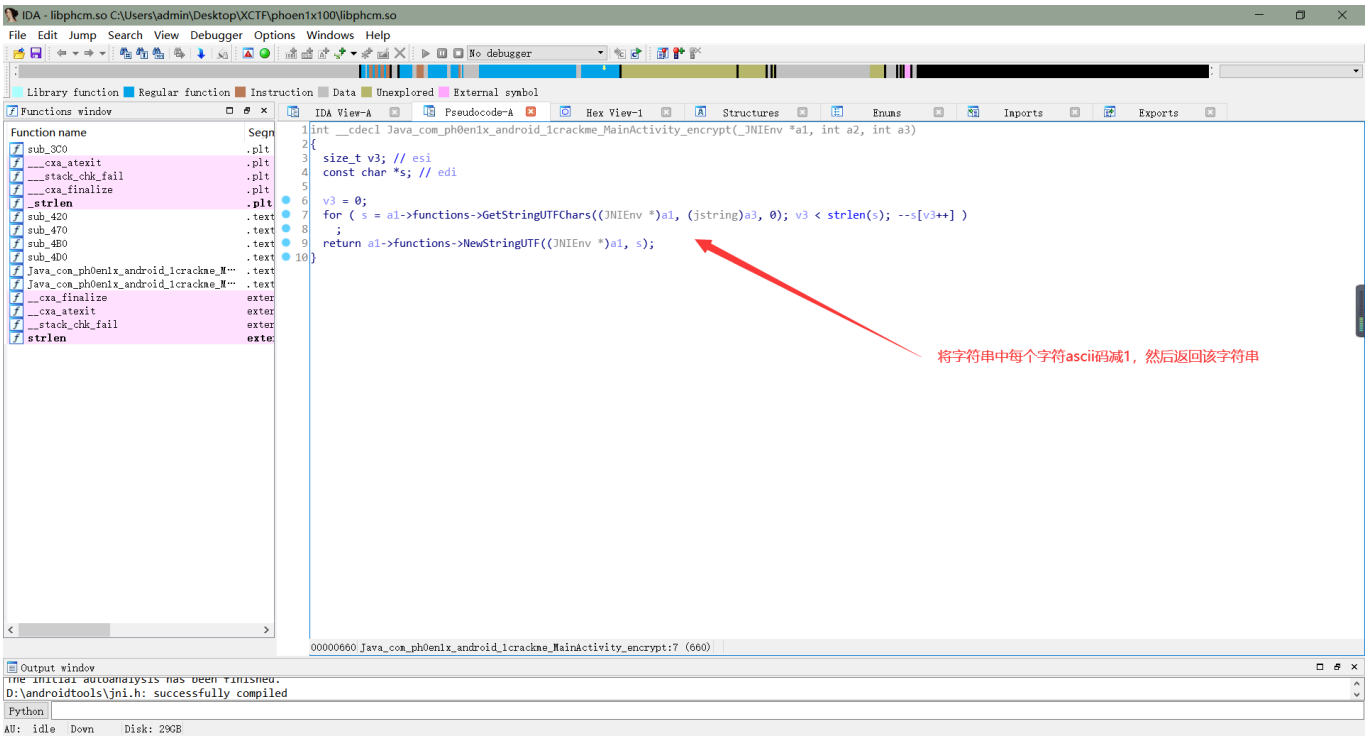


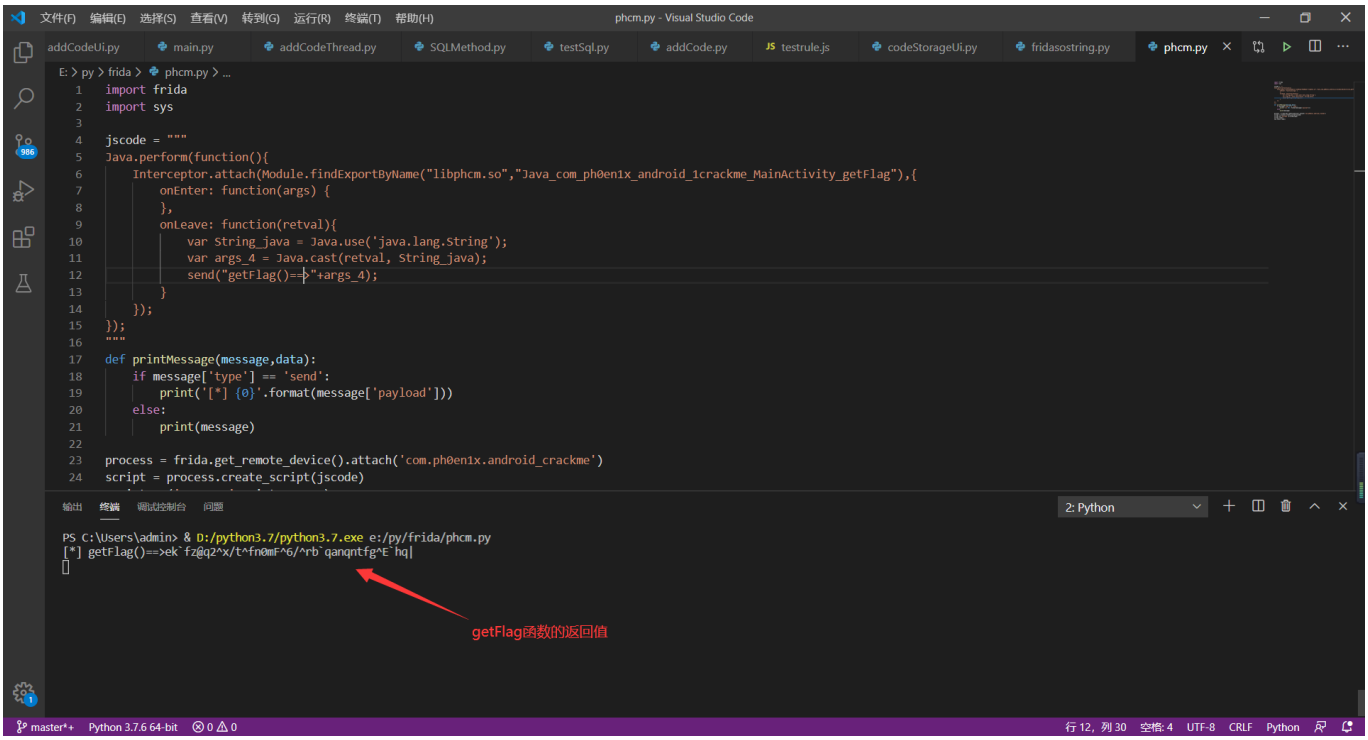
2、查壳后无壳直接使用**JEB**反编译，查看**MainActivity.java**文件，发现要弹出信息`Success`逻辑如下：首先在**so**层注册了两个静态函数--`encrypt(String)`、`getFlag()`函数，然后在**java**层有个函数`getSecret(String)`，将**so**层函数`getFlag`返回值经过`getSecret`函数加密后与我们在输入框中输入的字符串经过`encrypt`函数后在经过`getSecret`函数加密比较，如果一致，则返回`Success`，由于比较的两个字符串最外层都经过`getSecret`函数加密，所有我们不需要在管`getSecret`函数，直接让内部两个字符串一直一致即可得到**flag**！！！





3、使用**IDA**打开**so**文件，静态分析一下`encrypt`函数，发现逻辑很简单，就是将传进来的字符串的每个字符的**ASCII**码减一；对于`getFlag`函数，由于该函数没有输入只有输出，直接用**frida Hook**该函数得到返回值即可，如下图所示：

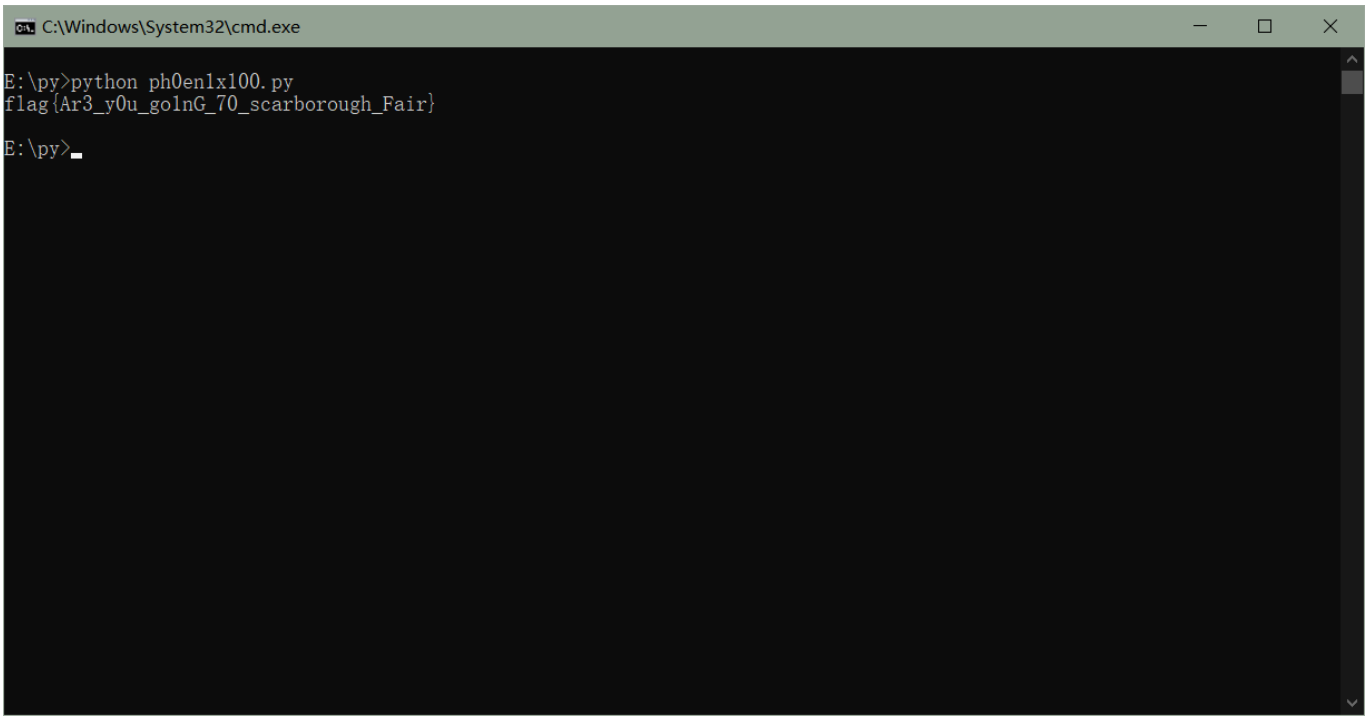


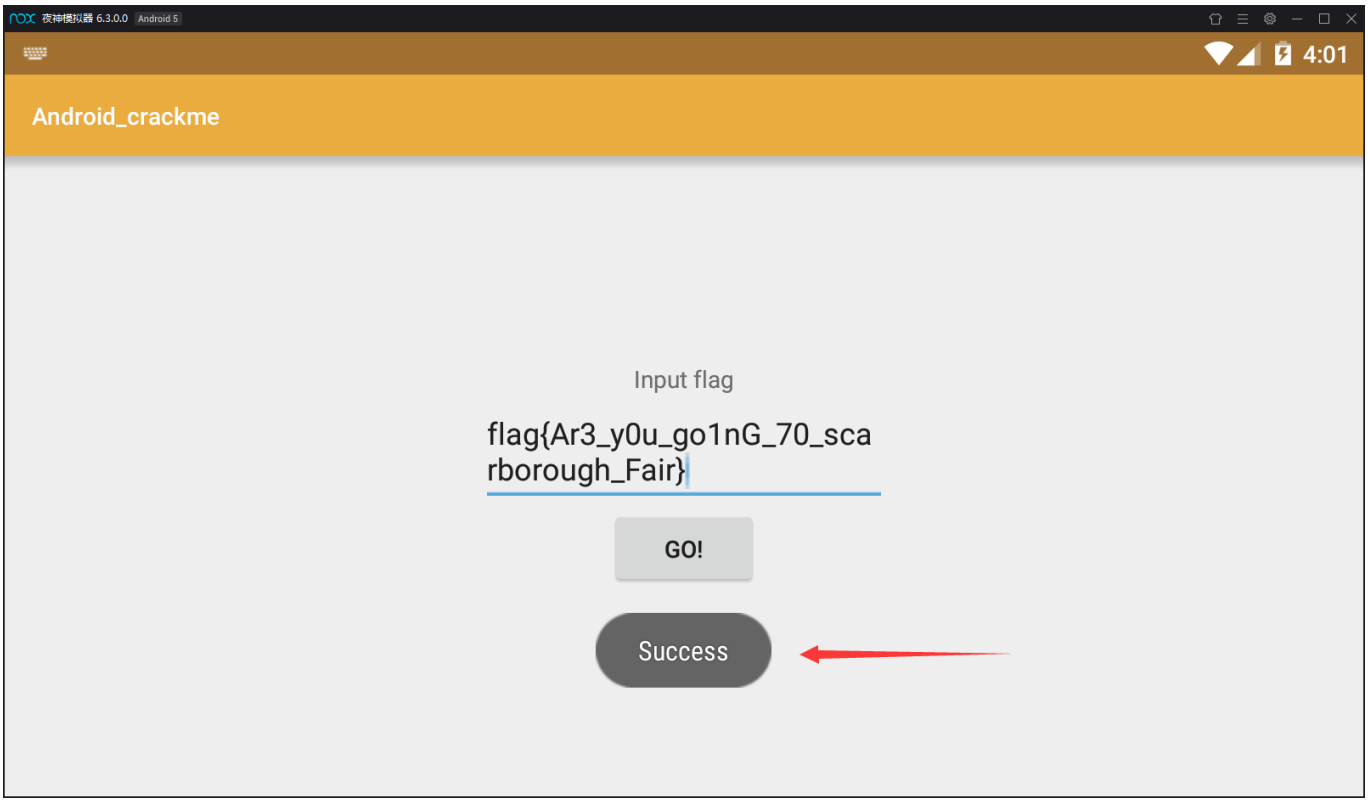


Frida代码：

```
import frida
import sys

jscode = """
Java.perform(function(){

Interceptor.attach(Module.findExportByName("libphcm.so","Java_com_ph0en1x_android_
1crackme_MainActivity_getFlag"),{
        onEnter: function(args) {
        },
        onLeave: function(retval){
            var String_java = Java.use('java.lang.String');
            var args_4 = Java.cast(retval, String_java);
            send("getFlag()==>"+args_4);
        }
    });
});
"""
def printMessage(message,data):
    if message['type'] == 'send':
        print('[*] {0}'.format(message['payload']))
    else:
        print(message)

process = frida.get_remote_device().attach('com.ph0en1x.android_crackme')
script = process.create_script(jscode)
script.on('message',printMessage)
script.load()
sys.stdin.read()
```

4、得到以上信息后，使用**python**脚本跑出**falg**即可，如下所示：





python脚本：

```
Flag = 'ek`fz@q2^x/t^fn0mF^6/^rb`qanqntfg^E`hq|'

flaglist = list(Flag)

stringlist = []
```

```
for ch in flaglist:
    stringlist.append(chr(ord(ch) + 1))

print(''.join(stringlist))
```