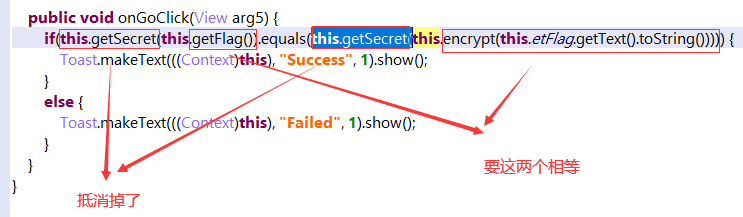
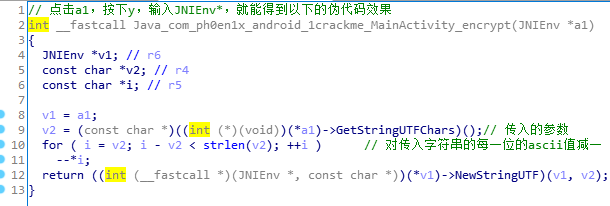
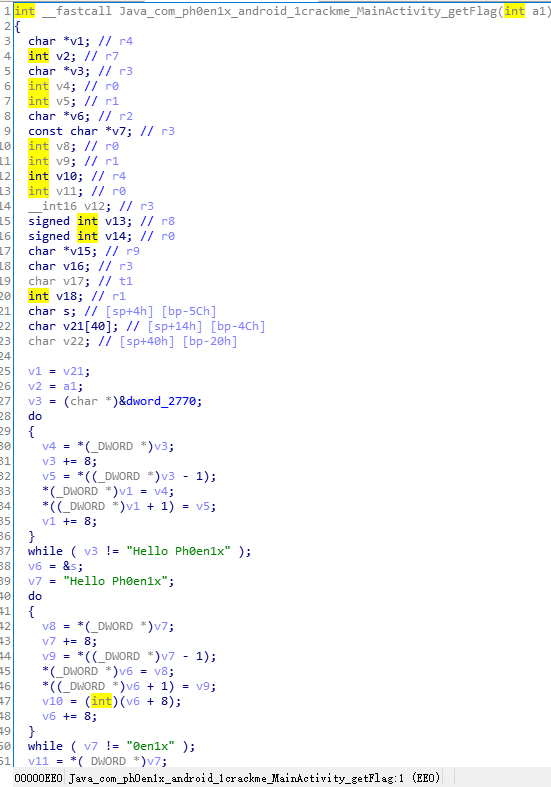
# 反编译



# 查找so





其实这个getFlag函数可以不用看，应为这个函数是一个无输入的固定值，我们想办法把他回显出来其实就行了。

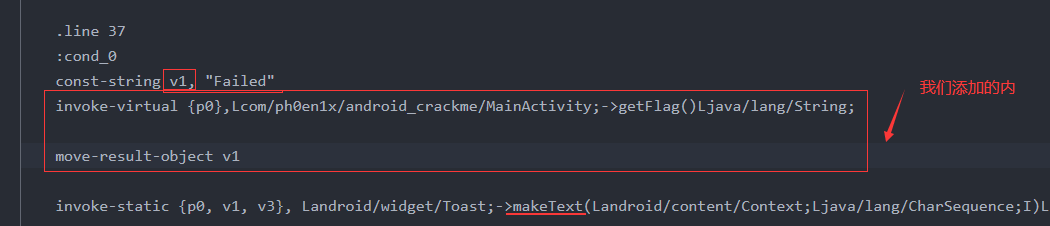
# 拿getFlag的值

这里有两种方法。

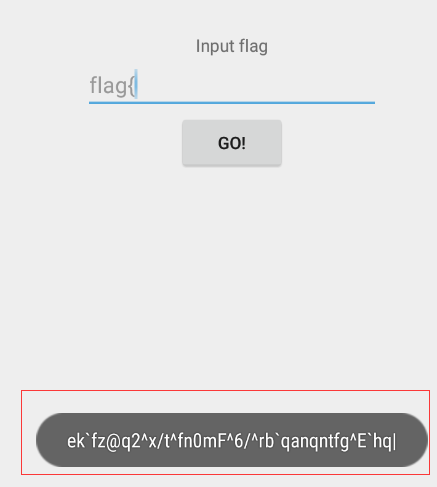
第一种是动态调试，

第二种是修改smail文件然后回编译

运行该程序时我们知道，如果我们的值时错误的会回显一个Failed，我们在MainActive.smail中查找到Failed的位置，我们要用getFlag的返回值替代掉Failed的值。



然后回编译，签名



# 最终结果和脚本

我们已经知道encrypt函数的作用是将string中的每一个字符的ascii值减一。所以我们可以编写脚本

|  |
| --- |
| str1 = "ek`fz@q2^x/t^fn0mF^6/^rb`qanqntfg^E`hq|"  flag = ''  for i in str1:      flag += chr(ord(i)+1)  print(flag) |

结果

