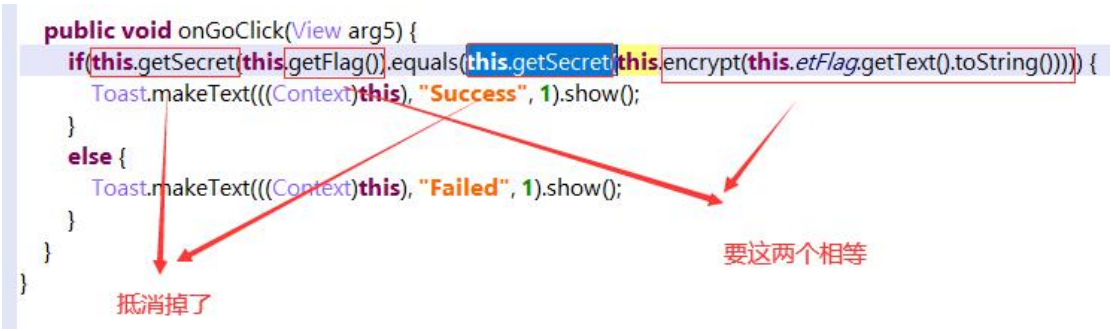
# 反编译




# 查找 so

```
1  // 点击a1，按下y，输入JNIEnv*，就能得到以下的伪代码效果
2  int __fastcall Java_com_ph0en1x_android_1crackme_MainActivity_encrypt(JNIEnv *a1)
3  {
4    JNIEnv *v1; // r6
5    const char *v2; // r4
6    const char *i; // r5
7
8    v1 = a1;
9    v2 = (const char *)((int (*)(void))(*a1)->GetStringUTFChars)();// 传入的参数
10   for ( i = v2; i - v2 < strlen(v2); ++i )      // 对传入字符串的每一位的ascii值减一
11     --*i;
12   return ((int (__fastcall *)(JNIEnv *, const char *))(*v1)->NewStringUTF)(v1, v2);
13 }
```

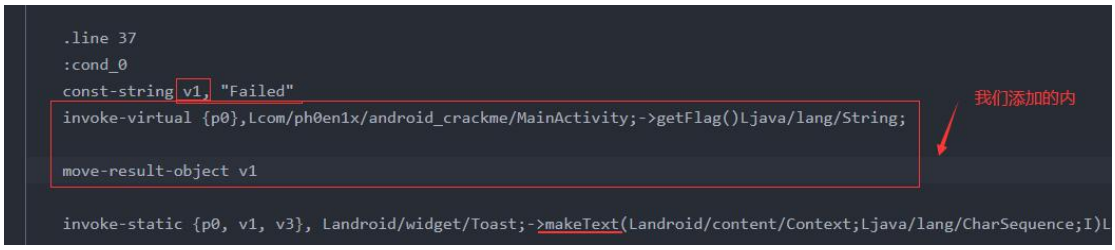
```
int __fastcall Java_com_ph0en1x_android_1crackme_MainActivity_getFlag(int a1)
{
  char *v1; // r4
  int v2; // r7
  char *v3; // r3
  int v4; // r0
  int v5; // r1
  char *v6; // r2
  const char *v7; // r3
  int v8; // r0
  int v9; // r1
  int v10; // r4
  int v11; // r0
  __int16 v12; // r3
  signed int v13; // r8
  signed int v14; // r0
  char *v15; // r9
  char v16; // r3
  char v17; // t1
  int v18; // r1
  char s; // [sp+4h] [bp-5Ch]
  char v21[40]; // [sp+14h] [bp-4Ch]
  char v22; // [sp+40h] [bp-20h]

  v1 = v21;
  v2 = a1;
  v3 = (char *)&dword_2770;
  do
  {
    v4 = *(_DWORD *)v3;
    v3 += 8;
    v5 = *((_DWORD *)v3 - 1);
    *(_DWORD *)v1 = v4;
    *((_DWORD *)v1 + 1) = v5;
    v1 += 8;
  }
  while ( v3 != "Hello Ph0en1x" );
  v6 = &s;
  v7 = "Hello Ph0en1x";
  do
  {
    v8 = *(_DWORD *)v7;
    v7 += 8;
    v9 = *((_DWORD *)v7 - 1);
    *(_DWORD *)v6 = v8;
    *((_DWORD *)v6 + 1) = v9;
    v10 = (int)(v6 + 8);
    v6 += 8;
  }
  while ( v7 != "0en1x" );
  v11 = *( DWORD *)v7;
00000EE0 Java_com_ph0en1x_android_1crackme_MainActivity_getFlag:1 (EE0)
```

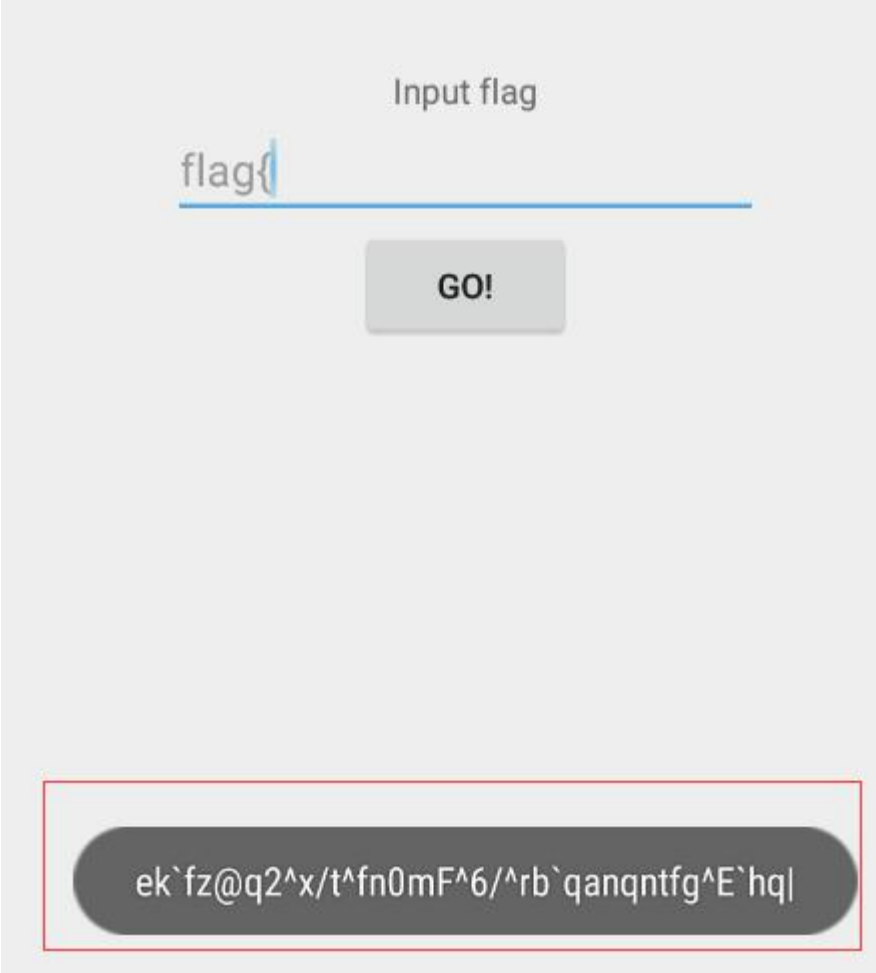
其实这个 getFlag 函数可以不用看，应为这个函数是一个无输入的固定值，我们想办法把他回显出来其实就行了。

# 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

```
flag{Ar3_y0u_go1nG_70_scarborough_Fair}
```