Lab2

16302010039\_崔帅帅

**Challenge1**

在看过smali代码之后发现该challenge主要在于一个check(string input)函数

这段是函数签名，即public int check（String input）

定义a，b两个字符串变量

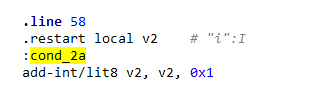
String a = “qwerfdsazxcvbgtyhjuioplkmnb”；

String b = “czgstdubqvz”;

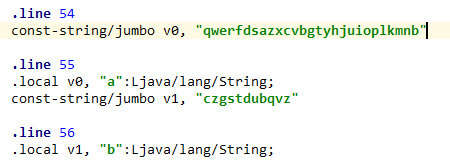
先对输入的input长度做初步判断，如果长度不合适，就直接返回0。

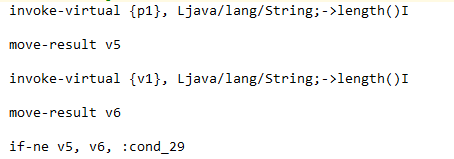
从此处可以看出，该函数有一个for循环，循环长度为input的length

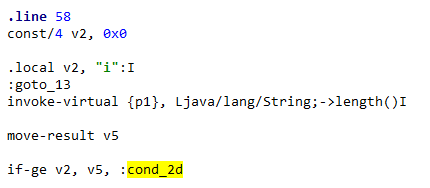
将input字符串做处理判断，如果不符合input的输入要求，则返回0，符合则继续循环

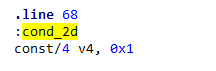


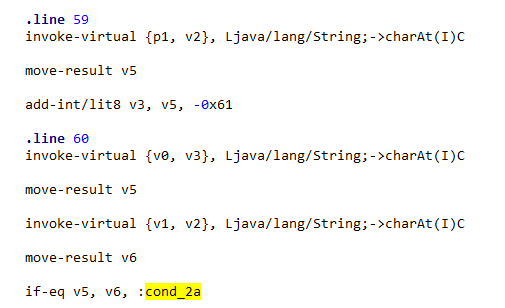












然后整理之后得到如下check函数：

**public int** check(String input){  
 String a = **"qwerfdsazxcvbgtyhjuioplkmnb"**;  
 String b = **"czgstdubqvz"**;  
 **int** j = 0;  
 **if** (input.length() == b.length()){  
 **for** (**int** i = 0; i < input.length(); i++) {  
 **if** (a.charAt(input.charAt(i) - **'a'**) != b.charAt(i))  
 **return** 0;  
 }  
 **return** 1;  
 }  
 **return** 0;  
}

如果input输入正确则返回1，否则返回0。

通过解密得到input为“kingofsmali”

不知道是手误还是什么那个字符串a好像多了一个字母b，然后我发现字符串“kingofs{ali”也是正确的。

**Challenge2**

通过challenge2的smali代码发现主要逻辑就是verify函数，大致如下：

这是函数签名，private boolean verify（String key）

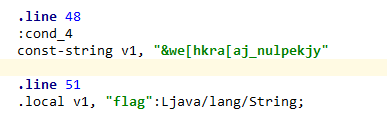
声明定义字符串变量flag

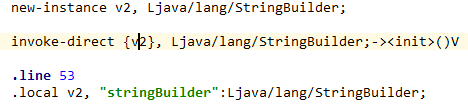
String flag = “&we[hkra[aj\_nulpekjy”

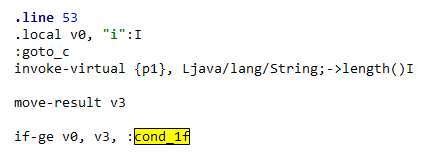
声明定义一个StringBuilder

一个以key长度的for循环



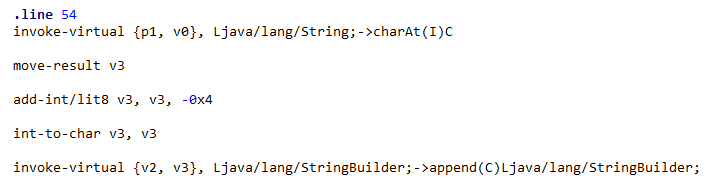








将输入字符串减少4



整理之后得到如下verify函数

**private boolean** verify(String key){  
 **if** (key.length() == 0) {  
 **return false**;  
 }  
 String flag = **"&we[hkra[aj\_nulpekjy"**;  
 StringBuilder stringBuilder = **new** StringBuilder();  
 **for** (**int** i = 0; i < key.length(); i++) {  
 stringBuilder.append((**char**)(key.charAt(i) - 4));  
 }  
 **return** stringBuilder.toString().equals(**"&we[hkra[aj\_nulpekjy"**);  
}

如果输入值正确会返回true，否则返回false

不知道是我解读的问题还是什么，他的flag变量好像没有用到。

不过最终解密还是没有任何影响，

我得到的结果是\*{i\_love\_encryption}最后验证结果正确