lab5 实验文档

程茜　19302010084

首先安装 apktool：

```
cx418y@ubuntu:~/Desktop/lab5/tools$ sudo mv apktool /bin
[sudo] password for cx418y:
cx418y@ubuntu:~/Desktop/lab5/tools$ sudo mv apktool.jar /bin
```

```
cx418y@ubuntu:/bin$ sudo chmod +x apktool
[sudo] password for cx418y:
cx418y@ubuntu:/bin$ sudo chmod +x apktool.jar
cx418y@ubuntu:/bin$
```

```
cx418y@ubuntu:~/Desktop/lab5$ apktool d ics_lab_smali.apk
I: Using Apktool 2.3.4 on ics_lab_smali.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
S: WARNING: Could not write to (/home/cx418y/.local/share/apktool/framework), us
ing /tmp instead...
S: Please be aware this is a volatile directory and frameworks could go missing,
 please utilize --frame-path if the default storage directory is unavailable
I: Loading resource table from file: /tmp/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Baksmaling classes2.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
cx418y@ubuntu:~/Desktop/lab5$
```

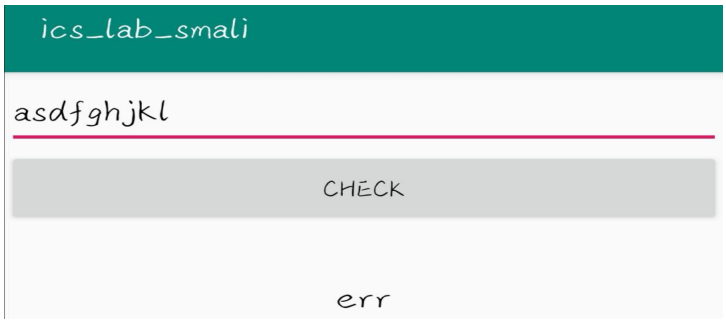
1. check 方法对应的 java 代码：

```java
public static String check(String in){
    int k1 = 5; //寄存器v0;
    int k2 = 9;  //寄存器v1;
    int len = in.length(); //寄存器v2的值为方法返回值;
    String out = ""; //寄存器v3的值为"";

    char []b = new char[]{'a','A'};//char数组v4，array_0的内容由后面得到

    try{
        int d = 1/(len-9);  //v5 = v6/v5 = 1/(v2-9) = 1/(len-9)
        for(int i = 0;i<len;i++){
            int enc = in.toLowerCase().toCharArray()[i] - b[0];
            out = new StringBuilder().append(out).append(String.valueOf((char)((k1*enc+k2)%26+b[1]))).toString();
        }
    }catch (Exception e){
        char[]c = new char[]{'e','r','r'};
        return String.valueOf(c);
    }
    return out;
}
```

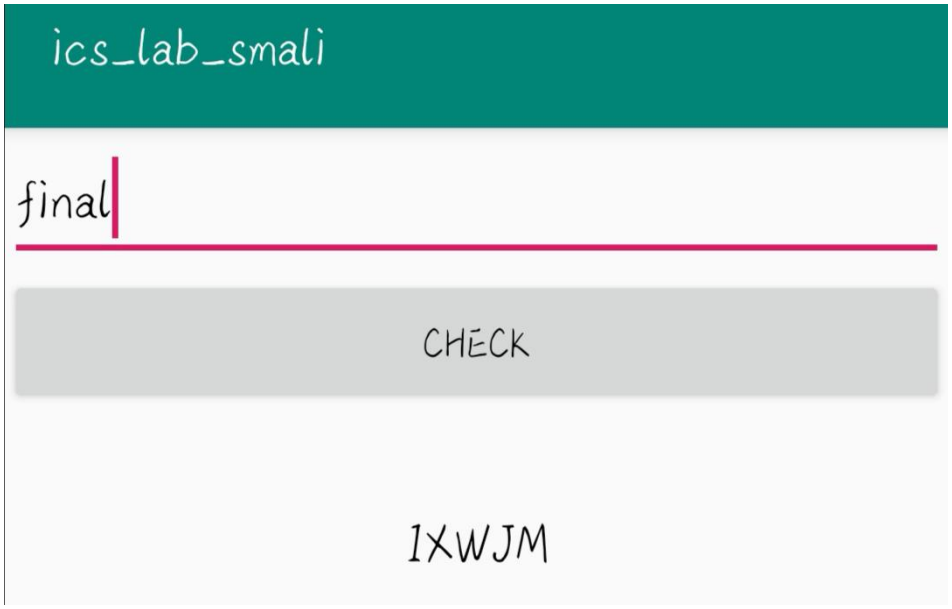
2. 可以发现当输入的字符串长度为 9 时程序会捕获异常，输出”err”：



故只要输入长度为 9 的任意字符串，均可以输出”err”；

3. 由以下代码反推回去可以得到输出为”IXWJM”的输入可以是”final”:

```
int enc = in.toLowerCase().toCharArray()[i] - b[0];
out = new StringBuilder().append(out).append(String.valueOf((char)((k1*enc+k2)%26+b[1]))).toString();
```



同时可以发现输入的大小写并不会影响输出的结果，所以任意转换为小写之后为”final”的字符串均可以得到输出”IXWJM”