一、加密

1、DFD

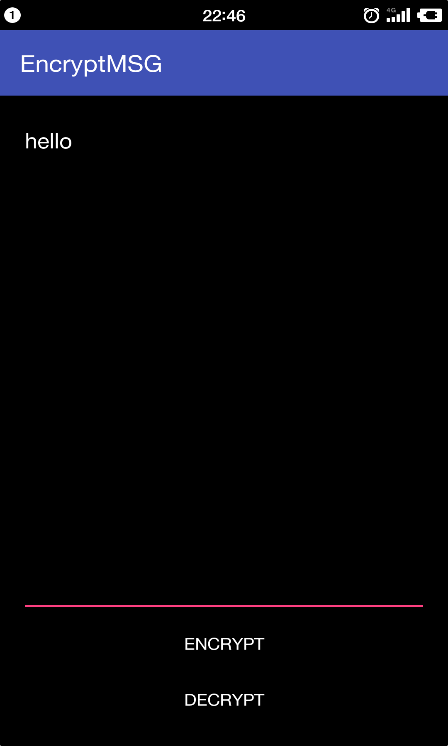


2、类图

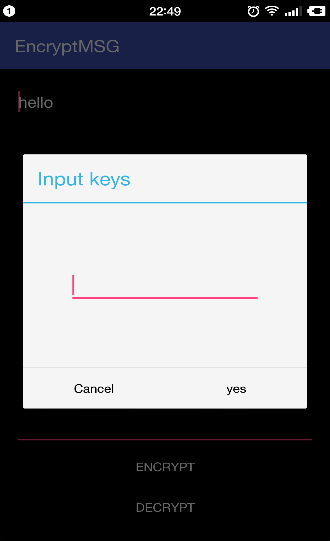


加密者（发送者流程）

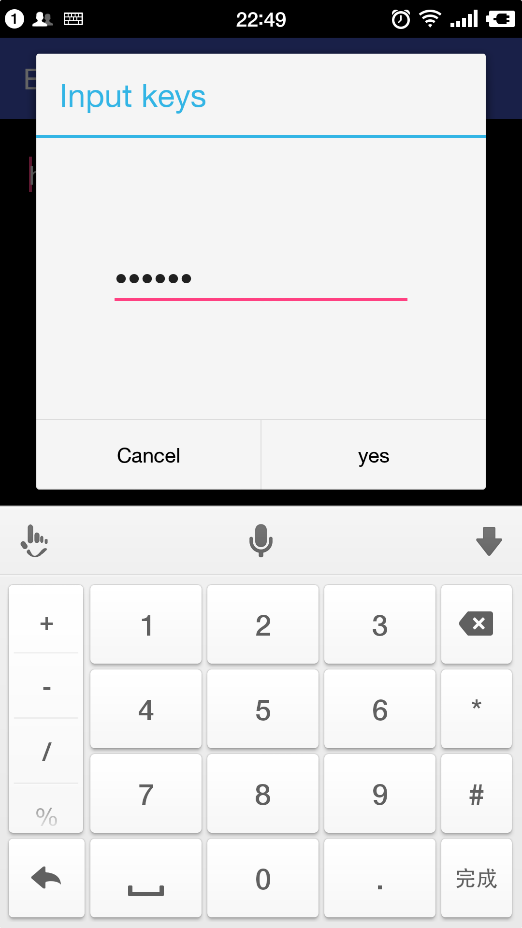
选中要发送的文字后添加到系统剪贴板（一般android设备以长按屏幕呼出粘贴菜单），打开程序后程序会自动响应系统粘贴板的内容并添加到程序自身的TextField中↓



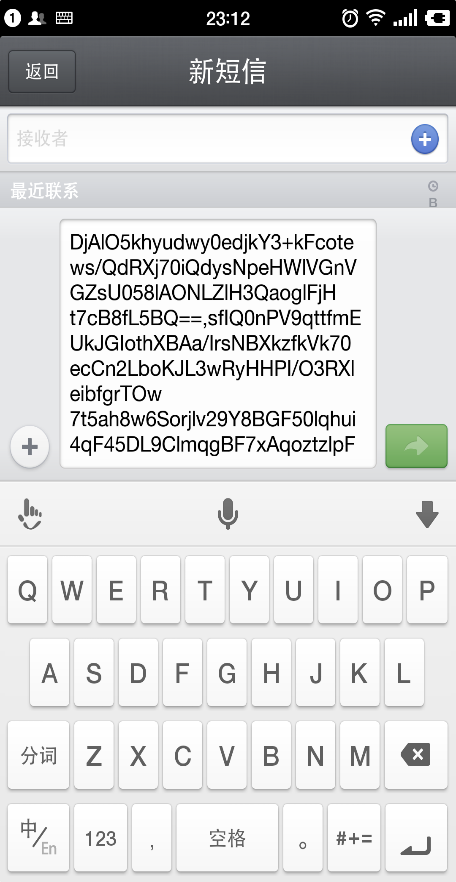
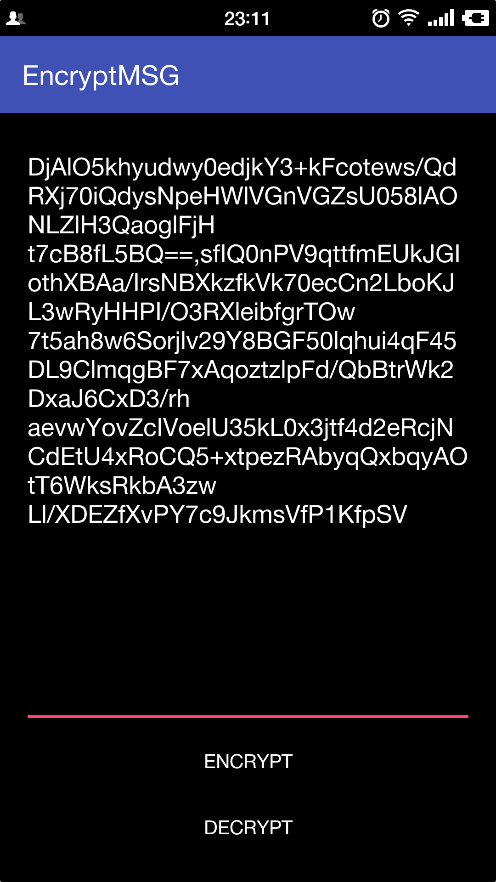
随后点击ENCRYPT按钮，然后呼出对话框，填写会话秘钥（SessionKey）↓



选用123456作为会话秘钥↓



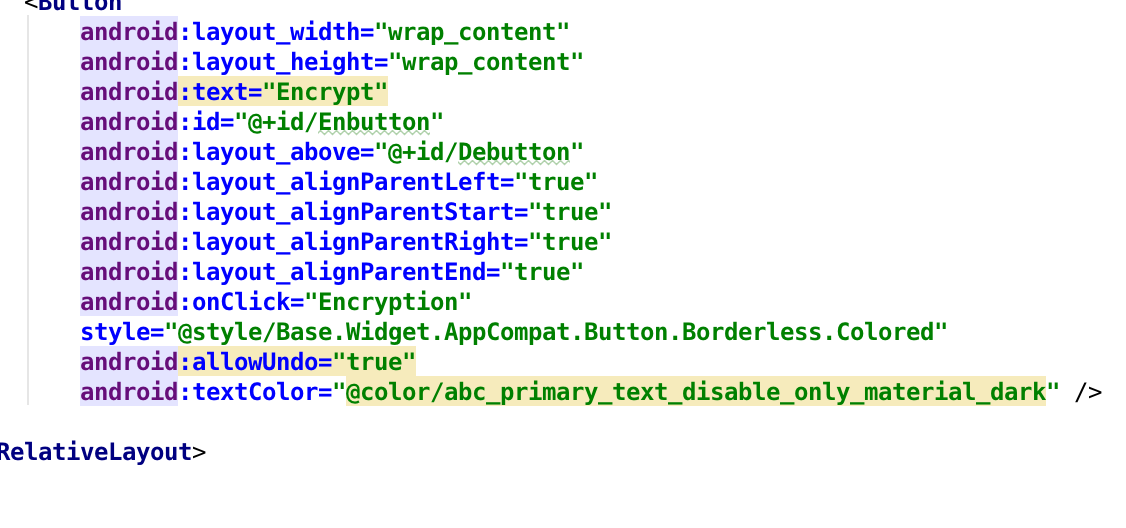
点击yes后获得加密内容并自动添加到系统剪贴板上↓

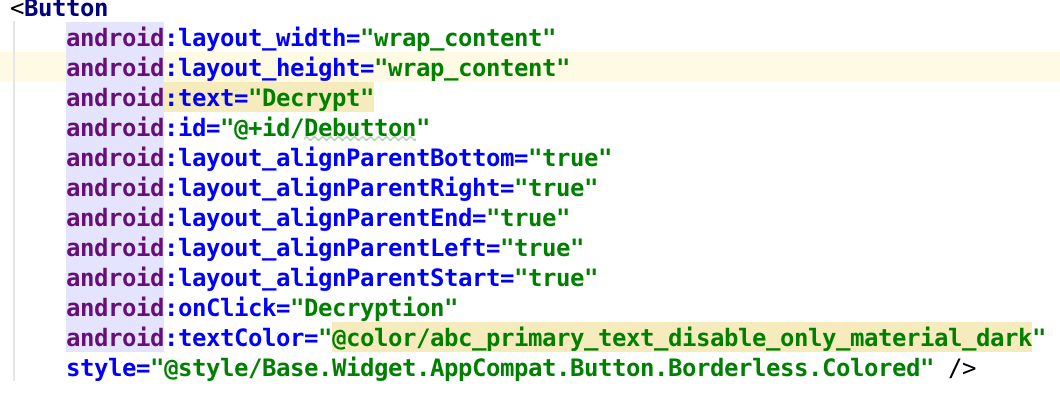


程序内流程

Mainactivity中定义了承接输入内容（Content）的TextField，以及加密（ENCRYPT）解密(DECRYPT)按钮

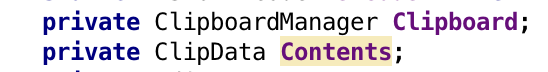


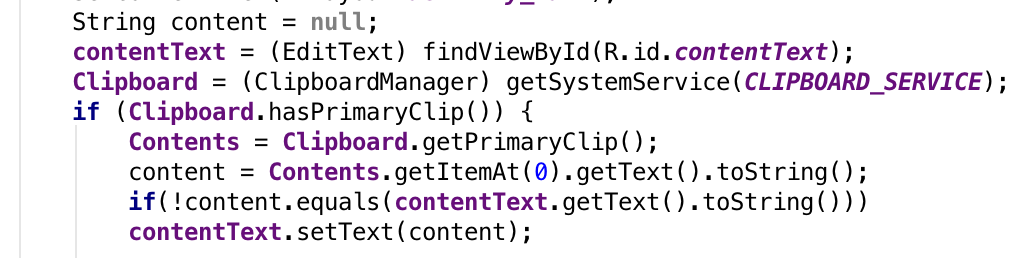




Mainactivity中创建两个私有域Clipboard以及CilpData承接系统剪贴板里面的内容

并将Textfield里的内容置为剪贴板中的内容↓





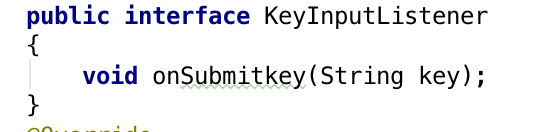
得到内容后点击ENCRYPT按钮，通过绑定onClick动作接入Encryption方法

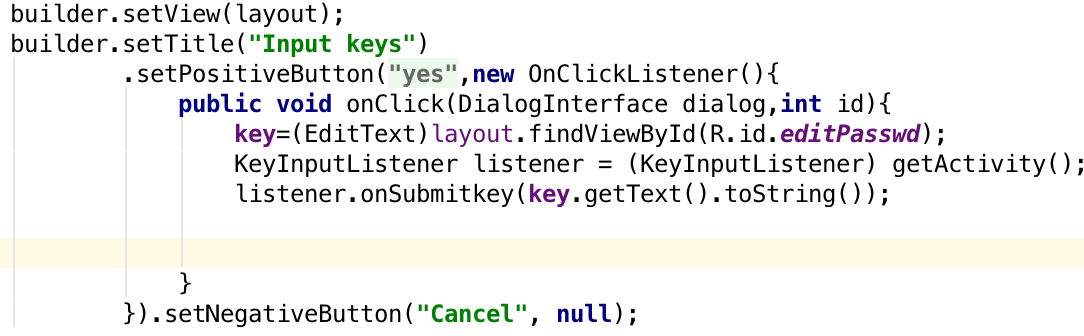
\\Mac\Home\Desktop\屏幕快照 2016-05-12 下午11.19.28.png

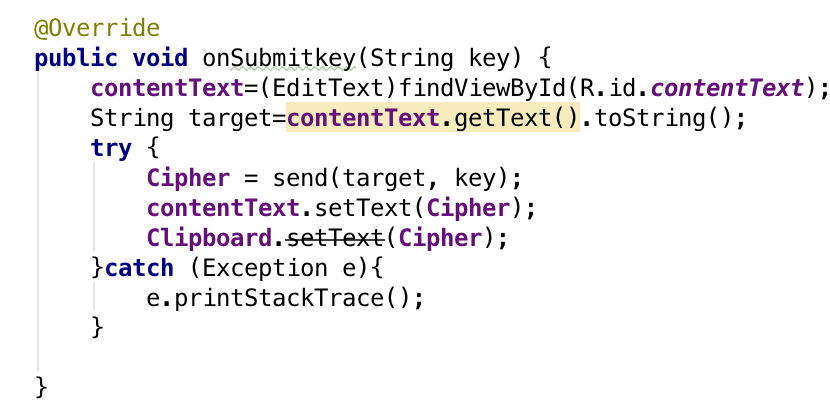
Encryption方法中通过创建DialogFragment呼出dialog收集用户输入的String作为会话秘钥Sessionkey

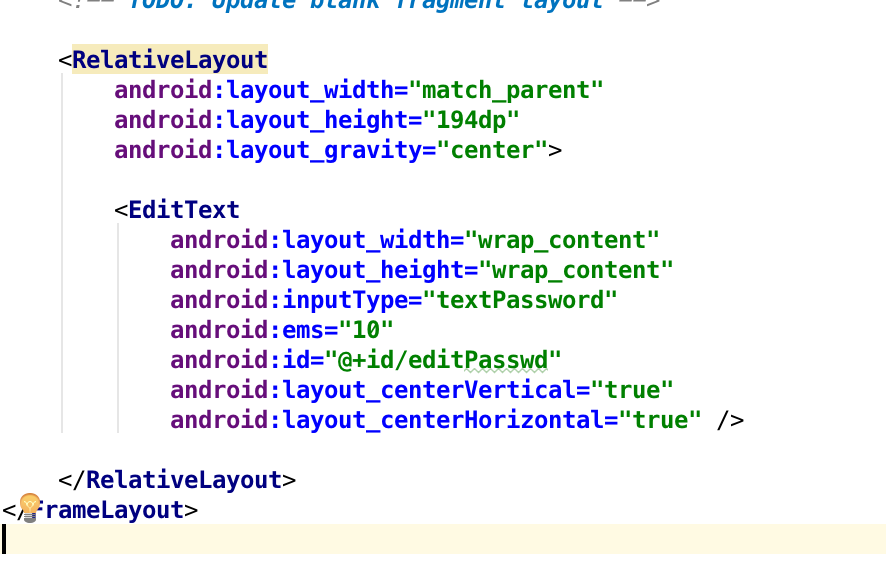


因为要实现dialog与Mainactivity直接的数据传输，所以DialogFragment要定义一个接口模式，并在Mainactivity中重写相应的接口方法↓





此外还要在dialog实现textField输入



在接口方法中调用了加密方法Send，其接受用户输入的会话秘钥Key及想要加密的信息为参数，返回值为带签名的密文以及用接受者的公钥解密了的会话密钥组合成的综合密文

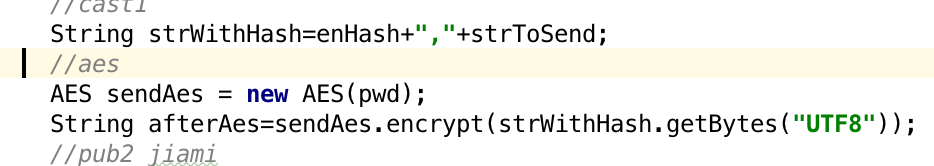
\\Mac\Home\Desktop\屏幕快照 2016-05-12 下午11.46.40.png

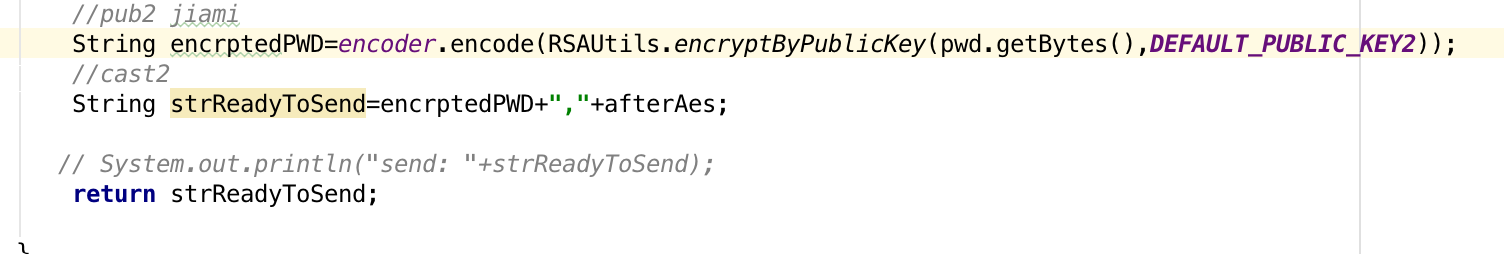
具体流程如下：

首先将需要加密的信息做hash运算，然后将得到的hash值以自己的私钥加密进行签名↓

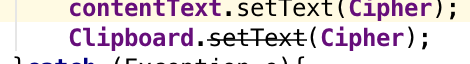


然后将待加密的信息以及签名用用户输入的会话密钥进行AES加密

  
最后将会话秘钥用对方的公钥进行加密，然后与上面AES加密后的内容组合在一起发送



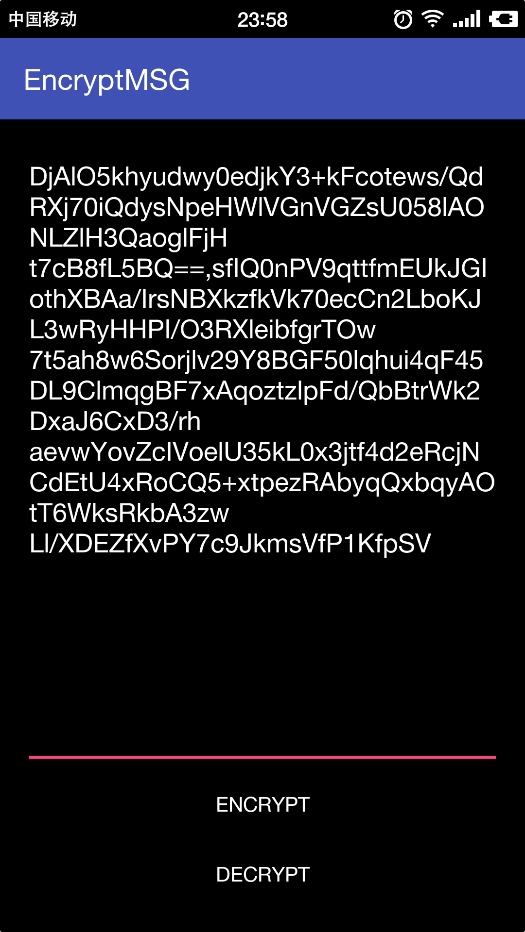
最后将加密后的所有内容显示在Mainactivity的TextField中，并自动加入系统的剪贴板



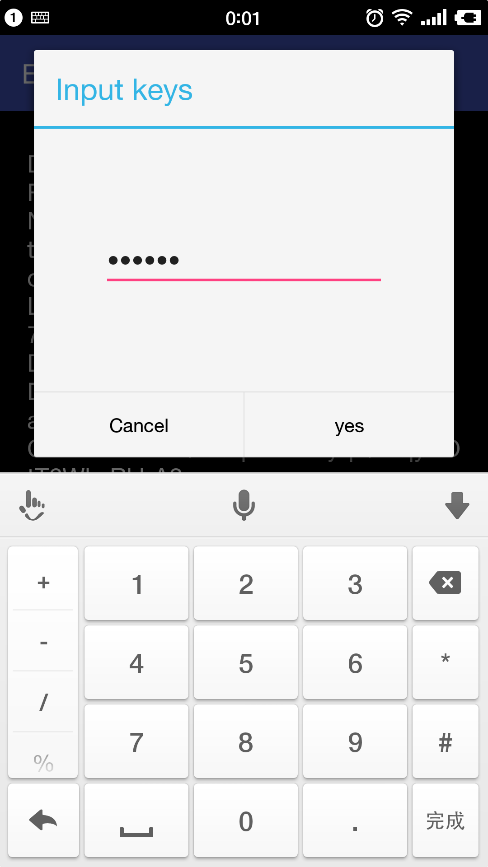
二、解密

解密流程与加密类似，具体演示如下：

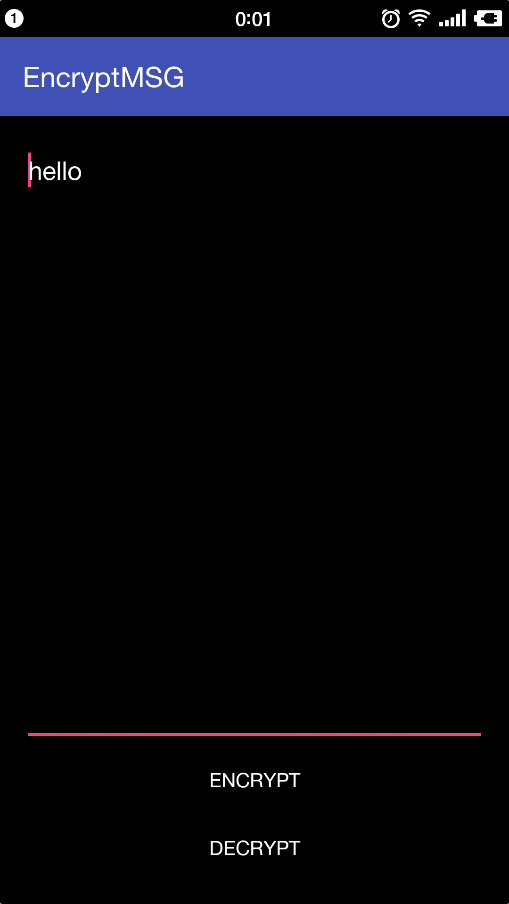
打开程序，自动添加系统剪贴板内容到TextField↓



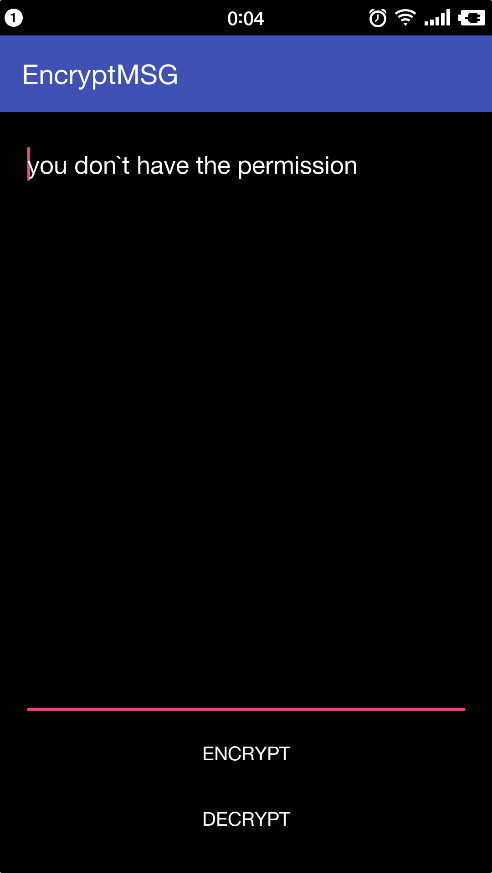
点击DECRYPT，呼出对话框，填写与Sender商定好的会话秘钥



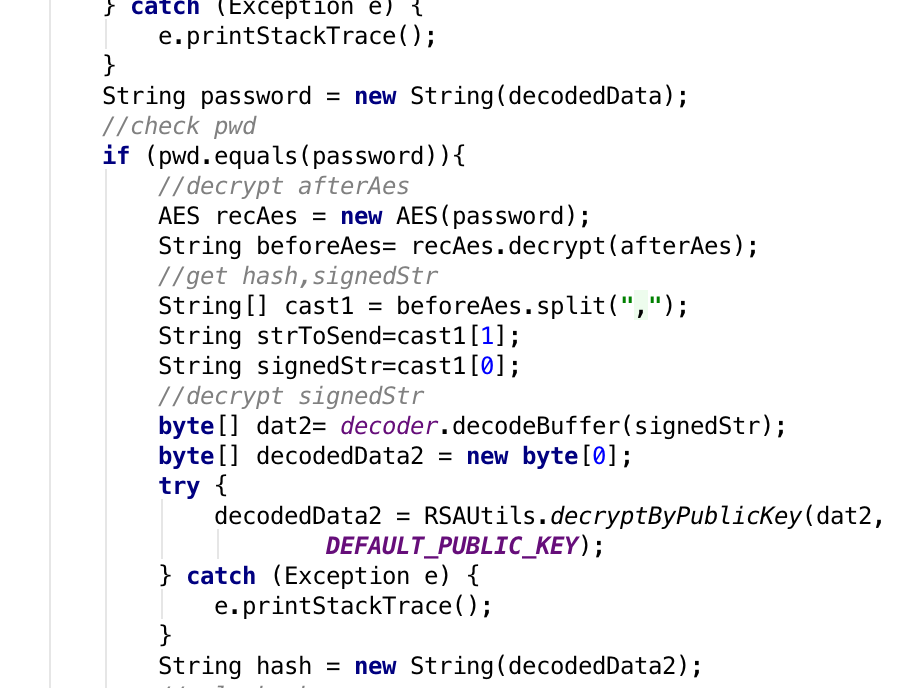
点击yes后解密完成



若输入错误秘钥会得到一下提示



值得注意的是，解密比加密多了一个流程：会话秘钥比对流程，如果用户输入的秘钥不等于用接受者公钥解密出来的会话密钥的话，就会显示如上信息



值得注意的是，本程序采用的是base64编码解码工具包对加密后的密文与解密后的明文以及加密所用的秘钥进行编码和解码操作操作，所采用的对称加密算法是AES，hash算法是MD5，非对称加密算法是RSA

本程序所用额公私钥是与程序绑定的（演示作用），但是是向OpenSSL申请得到，具有效力