题目名:保护数据

知识点：app反编译、backup备份/还原、sqlcipher加密/解密数据库

解题过程：

文件名backup.ab，根据词意可以猜到是备份文件。

关于备份文件。

【之所以可以得到这个备份文件，是因为AndroidManifest.xml文件中一个属性的设置而我们在创建应用的时候，这项设置默认是true，这可能会带来一定的安全风险。

安全风险源于adb backup允许任何一个能够打开USB 调试开关的人从Android手机中复制应用数据到外设，一旦应用数据被备份之后，所有应用数据都可被用户读取。尤其是通讯录应用，一旦应用程序支持备份和恢复功能，攻击者即可通过adb backup和adb restore进行恢复新安装的同一个应用来查看聊天记录等信息；对于支付金融类应用，攻击者可通过此来进行恶意支付、盗取存款等；因此为了安全起见，开发者务必将allowBackup标志值设置为false来关闭应用程序的备份和恢复功能，以免造成信息泄露和财产损失。】

对于这个备份文件，可以手动提取备份文件中的数据。过程见

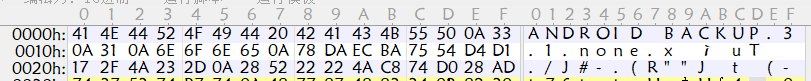
<http://bobao.360.cn/learning/detail/169.html>

也可以通过编译好的工具abe.jar直接转化成tar格式。提供一个下载地址<https://sourceforge.net/projects/adbextractor/files/?source=navbar>

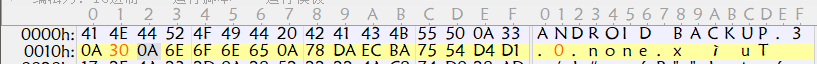
操作指令为



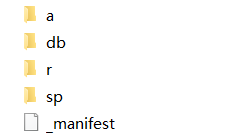
但是得到的tar解压时会提醒压缩包损坏，因为这个backup.ab文件头需要自己修复一下。



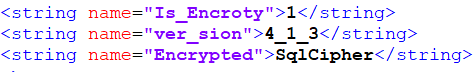
搜索得知常规的backup.ab文件头，最开始是ANDROID BACKUP，然后是版本号（这里是3），然后是Compression位，正常情况是1，因为备份文件经过了压缩。对比发现题目给出的文件头里，这一位被篡改成了0，手动改成1。之后便可正常解压tar。



（要是这个地方没必要的话，就直接提供修好的ab文件）

解压后目录下有这几个文件，这里面保存了该应用程序私有数据目录（/data/data/<Package Name>/）下的所有文件。

a中是源APK，db里是数据库文件，\_manifest是配置文件，sp里是Android中一种轻量级存储方式SharePreferences得到的xml文件，主要用于记录用户的一些偏好设置，而这里的test.xml相当于题目的hint。



提示了数据库经过了4.1.3版本的sqlcipher的加密。

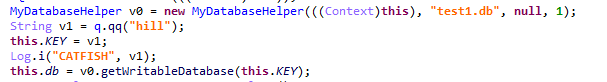
另外的r文件夹存放剩下的其它所有文件和目录。

此题中的r目录下还有一个名为Encrypted.db的数据库文件，具体用处后面再看。但是尝试后得知这个数据库文件和db目录下的test1.db都是经过加密的，需要找到他们的密钥。

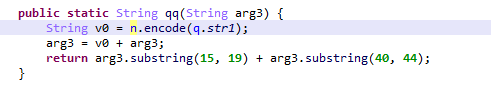
当前只得到这些信息，但是我们还有源apk可以反编译。

没有任何加固，直接拖进JEB查看。

逻辑比较简单，其中看到了SharedPreferences的插入记录和sqlite数据库的插入记录，其中明文SKCTF{hereistherealkey}，不过显然这并不是真的答案，尝试失败后继续寻找。

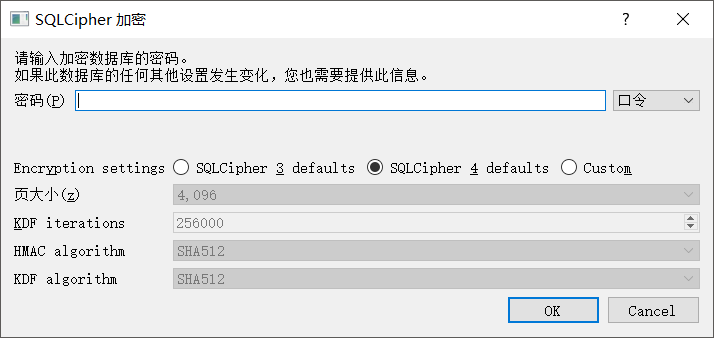


这里的getWritableDatabase写入数据库时使用了密钥KEY ，而KEY经过了q.qq()的处理。

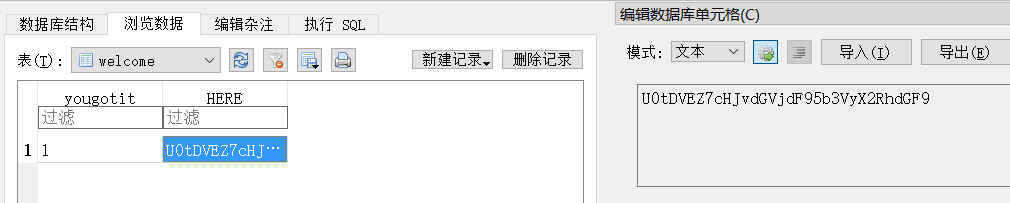


就是一个简单的SHA-1加密后取其中的八位字符，即数据库的密钥。

直接使用可视化工具DB Browser for SQLite可以解密。



test1.db里存的是假flag，真正的答案在Encrypted.db中



解一下base64得到最后答案。

flag：SKCTF{protect\_your\_data}