基于 Android 的私密短信系统设计与实现

刘安战，贾晓辉
（中原工学院，河南 郑州 450007）

摘 要： 通过对 Android 短信库的研究，开发了基于 Android 的私密短信系统，实现了点到点的短信加密通信，重点阐述了系统的主要功能，短信收发流程和实现中的关键问题，本系统通过了真机运行测试。

关键词： Android；私密短信；加密
中图分类号： TN929.5 **文献标识码：** A **文章编号：** 1674-7720(2012)17-0051-02

Design and implementation of private message system based on Android

Liu Anzhan, Jia Xiaohui
(Zhongyuan University of Technology, Zhengzhou 450007, China)

Abstract: Based on the research of Android message library, the paper develops the private message system, realizes the point-to-point encryption communication through message. This paper expounds the main function of the system, message transceiver procedures and key issues in the implementation. The system passed the test on the real mobile equipment.

Key words: Android; private message; encryption

2007 年 11 月 Google 公司推出 Android[1]智能手机平台，接着推出的面向 Android 应用开发的 SDK[2]为开发者开发 Android 平台上各种应用提供了方便。随着时间的推移，各种应用层出不穷，目前国内已经出现了很多汇集 Android 应用的网站，如 AppChina 应用汇和安智市场等。

Android 有活动(Activity)、服务(Service)、广播接收器(Broadcast Receiver)和内容提供者(Content Provider)4 大组件[3]。

活动主要用来进行应用界面的开发，一个活动往往占据当前的窗口，对于开发者而言，就需要派生一个 Activity 的子类。服务有点像后台程序，通常都是后台长时间运行，接受上层调用指令，完成相关功能。广播接收器用来接收一种或若干种意图(Intent)的触发事件，当事件发生时，系统会传递消息给广播接收器，进而由广播接收器进行进一步处理。广播接收器一般用来监听一些事件，如：监听来电、邮件和短信等。内容提供者是 Android 提供的第三方应用数据的访问方案。每个 Content Provider 都用一个 URI 作为独立的标识，如：content://sms/inbox 表示短信收件箱。Content Provider 在屏蔽了内部数据的存储细节基础上向外提供了统一的接口，这样大大简化了上层应用的访问。

除了 4 大组件外，Android 还提供了意图(Intent)机制，它能在程序运行的过程中连接 2 个不同的组件。活动、服务和广播接收器都是通过意图机制激活的，意图在组件之间传递数据。

1 Android 短信库

1.1 短信息表结构

Android 系统中采用的 SQLite[4]嵌入式数据库，其短息库为 mmssms.db，在 adb shell 中可以通过 sqlite3 mmssms.db 连接该数据库。通过.tables 命令可以发现 mmssms.db 共有 13 个表，其中的 sms 表是用来存储所有短息数据的，通过.schema sms 命令查看表 sms 的表结构，其表结构如表 1 所示。

1.2 短信库的访问

系统数据库的访问需要授权，在编写程序时需要在 AndroidManifest.xml 文件中添加权限使用说明。如：<uses-permission android:name="android.permission.READ_SMS"/>表示可以读短信，若是要使得应用可以发送短信则还需要加入<uses-permission android:name="android.permission.

表 1 短信息表结构

字段	类型	说明
_id	INTEGER	主键,短信编号
thread_id	INTEGER	thread 表中的 id,表示对话编号
address	TEXT	发短信人地址,即手机号
person	INTEGER	发短信人在通信录中编号
date	INTEGER	日期时间,整数格式表示的时间
protocol	INTEGER	协议,0 为短信,1 为彩信
read	INTEGER	0 为未读,1 为已读
status	INTEGER	默认值为 1,表示短信状态,如接收失败等
type	INTEGER	短信类型,1 为收到的,2 为已发出等
reply_path_persent	INTEGER	应答路径
subject	TEXT	短信标题
body	TEXT	短息内容
service_center	TEXT	服务中心号码
locked	INTEGER	默认值为 0

SEND_SMS"/>。

Android 通过内容提供者向应用提供访问底层数据库,应用程序可以通过一个 URL 访问对应的数据,如:content://sms/inbox 表示短信收件箱,而 content://sms/outbox 表示短信发件箱。

数据表的访问在 Android 采用游标方式,通过 Activity 类的 manageQuery 方法获得一个数据集游标,managedQuery 方法的声明为:public final Cursor managedQuery(Uri uri,String[] projection,String selection,String[] selectionArgs, String sortOrder)。

2 系统设计

2.1 系统功能

私密短信系统的功能主要包括:(1)建立短信,加密短信,发送短信;(2)私密短信列表;(3)查收私密短信,解密查看;(4)联系人选择;(5)私密短信会话。

2.2 私密短信收发过程

私密短信系统通过在应用层加密/解密短信数据达到点对点的密码通信。发送短信方通过输入明文短信、加密短信及发送密文短信实现发送短信功能;接收短信方通过查询短信库和解密短信来阅读短信,考虑到短信传输过程中的编码问题,还要进行编码转换工作。具体的收发短信流程如图 1 所示。

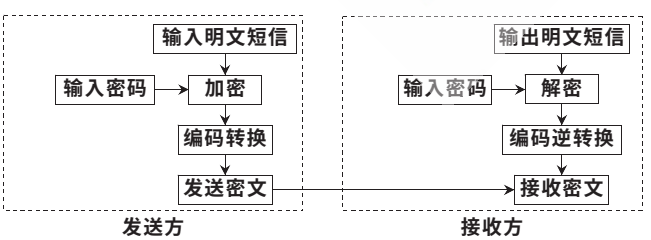

图 1 私密短信收发流程

(1)输入明文:输入与发送的短信明文内容。

(2)输入密码:输入加密使用的密码。

(3)加密:根据输入明文和密码进行加密产生密文,通过 javax.crypto 中 Cipher 类提供的功能对密文采用用 DES[5]加密。

(4)编码转换:加密后的密文以字节码的形式存在,在发送短信前需要进行进一步的编码,将其转换成 Base64 编码格式以便能够正常发送短信。

(5)发送短信:通过调用 Android 提供的 API 来实现发送短信,在系统中 SmsManager 类提供的 sendTextMessage 方法可以实现发送短信功能。

(6)接收短信:通过访问系统短信库中的信息查看接收的短信,检索可以查看所有私密短信。

(7)编码逆转换:编码转换的逆过程。

(8)解密:加密逆过程。

2.3 关键问题

(1)菜单的实现

Android 系统支持选项菜单、子菜单和快捷菜单 3 种菜单。系统采用选项菜单,实现选项菜单需要重载 Activity 的 onCreateOptionsMenu(Menu menu)方法,通过 Menu 的 add 方法添加菜单项,对于菜单的响应则是通过重载 onOptionsItemSelected(MenuItem item)方法实现。

(2)加密转码

加密采用的是 Cipher 类实现的,其中的 getInstance 方法可以获得相应的实例,通过 init 方法初始化加密模式和密码,通过 doFinal 方法进行加密并返回加密后的字节数组。

加密后的字节数组并不能直接用于短信内容发送,因此还要进行进一步的转码。系统将加密后的字节数组密文转换成 Base64 编码组成的字符串后作为短信内容进行传输。

(3)密信标志

加密转码后的短信和普通短信一样借助于移动网络传输,接收方收到的就是一个短信,只不过短信内容是没有意义的密而已。系统为了区分加密短信和未加密的短信,在发送私密短信时在密信内容中加入了供系统识别的密信标志。通过密信标志,接收方可以过滤接收的所有密信。

(4)短信发送

在 Android 系统中,SmsManager 类提供 sendTextMessage 方法发送短信,具体代码为:smsManager.sendTextMessage(mobile,null,text,null,null)。其中,mobile 为目标手机号码,text 为发送的短信内容。对于长度较小的短信系统采用直接发送的方式实现,对于长度超过 70 B 的短信,系统通过分割成多个短信的方式进行发送,以便用户能够接收到完整的短信内容。

3 系统测试

系统测试采用的摩托罗拉 XT502 机型,图 2 为系统主界面,默认列出系统收到的所有密信,可以通过相应

的菜单执行相应的功能。

发送密信菜单可以打开加密和解密界面，如图3所示。图中显示的是明文为“你好”，密码为“123”的加密和解密界面。

图2 系统主界面

图3 加密、解密界面

随着3G手机不断普及，用户可以越来越多地定制自己的应用，信息安全传输的重要性更是不可忽视。私密短信系统为用户提供点对点的私密通信，信息在网络的传输过程中采用的密码形式，即使信息被拦击或被通信公司泄露，解密也会大大地提高成本，从而提高用户传输信息的安全性。下一步的研究开发将侧重于私密通话研究，防止电话窃听。

参考文献

[1] http://www.android.com/, 2012-03-01.

[2] http://developer.android.com/sdk/index.html, 2012-03-01.

[3] 杨丰盛.Android应用开发揭秘[M].北京：机械工业出版社，2010.

[4] http://www.sqlite.org, 2012-03-01.

[5] 顾超. 动态DES算法. 计算机应用与软件[J].2007, 7: 164-166.

（收稿日期：2012-03-08）

作者简介：

刘安战，男，1980年生，硕士，讲师，主要研究方向：移动通信安全，网络安全。