基于DES的安卓系统安全通讯的设计与实现

姓 名 陈伟桐（S201407001）

姓 名 刘 岩（S201407077）

指导教师 蔡永泉

2015 年 3 月

一、 安卓系统平台简介

Android 是一种由 Google 公司领导及开发的基于 Linux 的自由及开放源代码的操作系统，主要使用于移动设备，如智能手机和平板电脑。

Android 一词的本义指“机器人”，同时也是 Google 于 2007 年 11 月 5 日宣布的基于 Linux 平台的开源手机操作系统的名称，该平台由操作系统、中间件、用户界面和应用软件组成。

2012 年 7 月美国科技博客网站 BusinessInsider 评选出二十一世纪十款最重要电子产品，Android 操作系统和 iPhone 等榜上有名。

二、 Des 加密算法原理说明

数据加密标准（DES，Data Encryption Standard）是一种使用密钥加密的块密码，1976 年被美国联邦政府的国家标准局确定为联邦资料处理标准（FIPS），随后在国际上广泛流传开来。它基于使用 56 位密钥的对称算法。这个算法因为包含一些机密设计元素，相对短的密钥长度以及怀疑内含美国国家安全局（NSA）的后门而在开始时有争议，DES 因此受到了强烈的学院派式的审查，并以此推动了现代的块密码及其密码分析的发展。

DES 算法加密过程主要分为以下几个步骤：

1. 初始置换

将输入的明文，根据初始换位表进行置换，获得初始置换结

果

2. 逐层置换

1) 将初始置换后的数据分为左右各 32 位

2) 将 32 位数据扩展为 48 位

3) 对 Key 进行压缩换位，获得 K

4) 将右数据 R 与 K 进行异或

5) 左右交叉换位

6) 将左右合并成新的 massage

7) 重复 1-6 过程 16 次，获得逐层置换结果

3. 最后换位

将上一步的置换结果，根据最终换位表进行置换，获得密文，加密完成

其中涉及的置换表如下：

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

初始换位表

IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

最终换位表

E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

32-48 扩展表

PC-1

左						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
右						
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

压缩型换位 1 表

PC-2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

压缩型换位 2 表

以下为 S 位置置换表

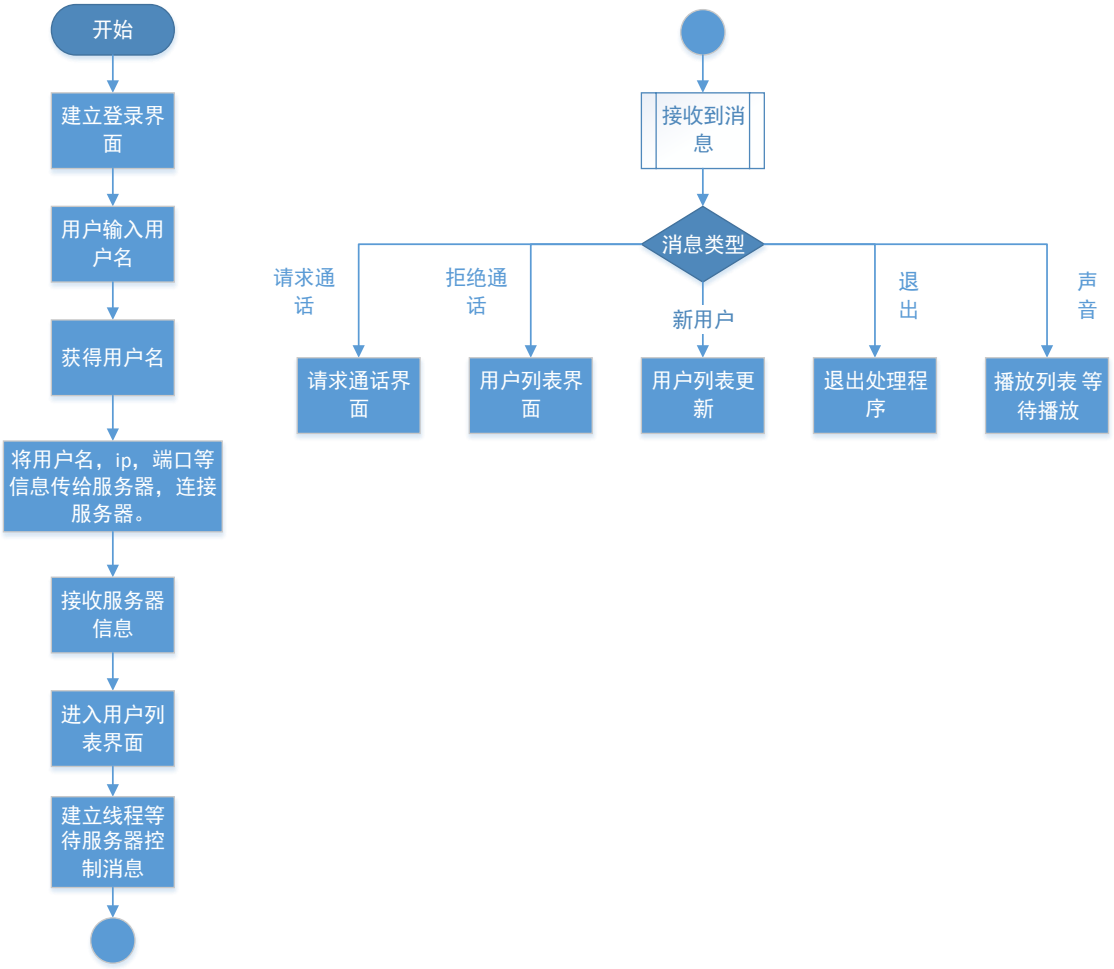
```
S1Form = new byte[]
{
    14,4,13,1,2,15,11,8,9,10,6,12,5,9,0,7,
    0,15,7,4,14,2,13,1,10,6,12,11,9,5,3,8,
    4,1,14,8,13,6,2,11,15,12,9,7,3,10,5,0,
    15,12,8,2,4,9,1,7,5,11,3,14,10,0,6,13
};

S2Form = new byte[]
{
    15,1,8,14,6,11,3,4,9,7,2,13,12,0,5,10,
    3,13,4,7,15,2,8,14,12,0,1,10,6,9,11,5,
    0,14,7,11,10,4,13,1,5,8,12,6,9,3,2,15,
    13,8,10,1,3,15,4,2,11,6,7,12,0,5,14,9
};

S3Form = new byte[]
{
    10,0,9,14,6,3,15,5,1,13,12,7,11,4,2,8,
    13,7,0,9,3,4,6,10,2,8,5,14,12,11,15,1,
    13,6,4,9,8,15,3,0,11,1,2,12,5,10,14,7,
    1,10,13,0,6,9,8,7,4,15,14,3,11,5,2,12
};
```

```
S4Form = new byte[]
{
    7,13,14,3,0,6,9,10,1,2,8,5,11,12,4,15,
    13,8,11,5,6,15,0,3,4,7,2,12,1,10,14,9,
    10,6,9,0,12,11,7,13,15,1,3,14,5,2,8,4,
    3,15,0,6,10,1,13,8,9,4,5,11,12,7,2,14
};

S5Form = new byte[]
{
    2,12,4,1,7,10,11,6,8,5,3,15,13,0,14,9,
    3,13,4,7,15,2,8,14,12,0,1,10,6,9,11,5,
    0,14,7,11,10,4,13,1,5,8,12,6,9,3,2,15,
    13,8,10,1,3,15,4,2,11,6,7,12,0,5,14,9
};

S6Form = new byte[]
{
    12,1,10,15,9,2,6,8,0,13,3,4,14,7,5,11,
    10,15,4,2,7,12,9,5,6,1,13,14,0,11,3,8,
    9,14,15,5,2,8,12,3,7,0,4,10,1,13,11,6,
    4,3,2,12,9,5,15,10,11,14,1,7,12,0,8,13
};

S7Form = new byte[]
{
    4,11,2,14,15,0,8,13,3,12,9,7,5,10,6,1,
    13,0,11,7,4,9,1,10,14,3,5,12,2,15,8,6,
    1,4,11,13,12,3,7,14,10,15,6,8,0,5,9,2,
    6,11,13,8,1,4,10,7,9,5,0,15,13,2,3,12
};

S8Form = new byte[]
{
    13,2,8,4,6,15,11,1,10,9,3,14,5,0,12,7,
    1,15,13,8,10,3,7,4,12,5,6,11,0,14,9,2,
    7,11,4,1,9,12,14,2,0,6,10,13,15,3,5,8,
    2,1,14,7,4,10,8,13,15,12,9,0,3,5,6,11
};
```

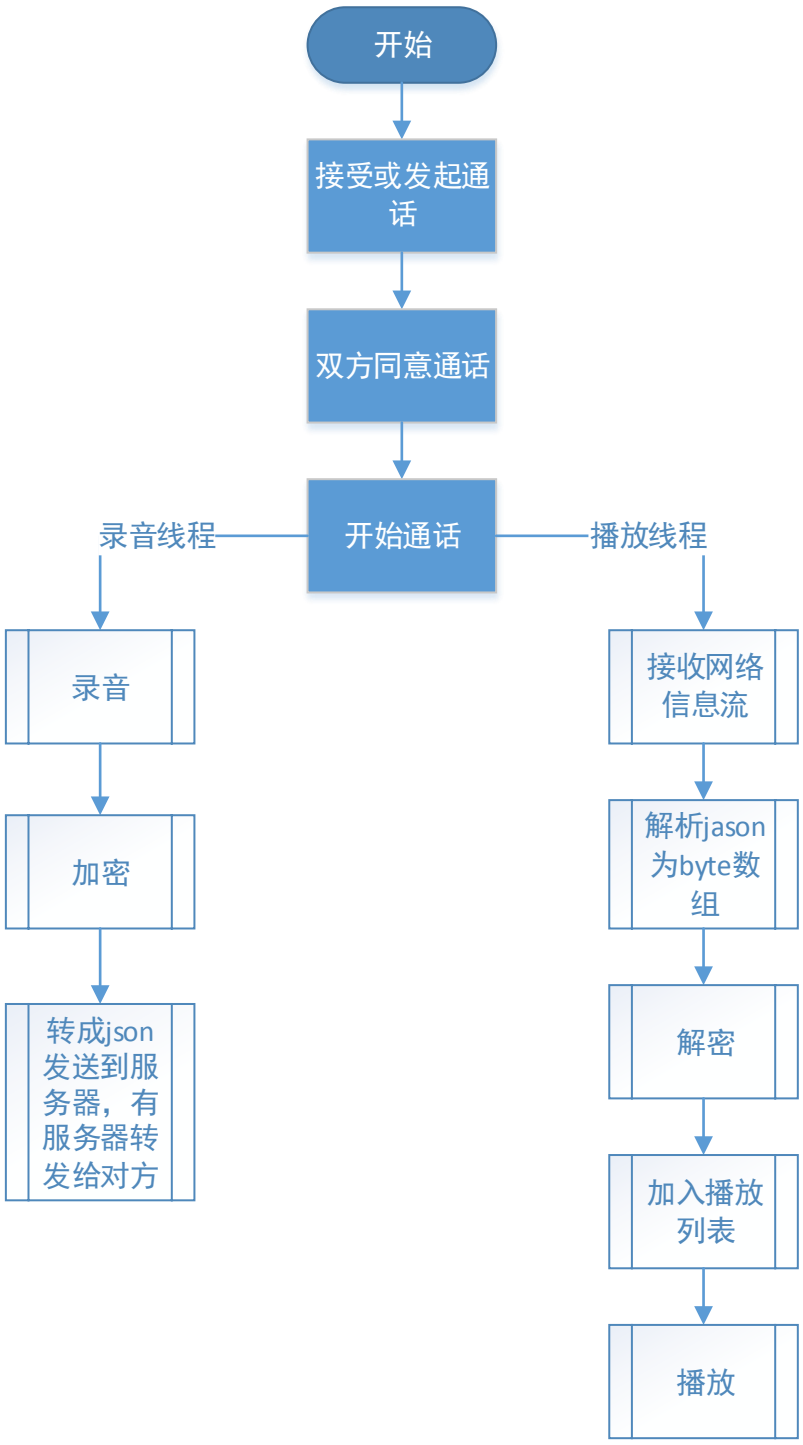
三、 安全通讯程序架构设计

程序主要分为客户端和服务器两部分，客户端负责将用户的语音存储起来，加密后发送给服务器，以及接收服务器发来的信息，进行解密；服务器负责接收用户发来的消息并进行转发。

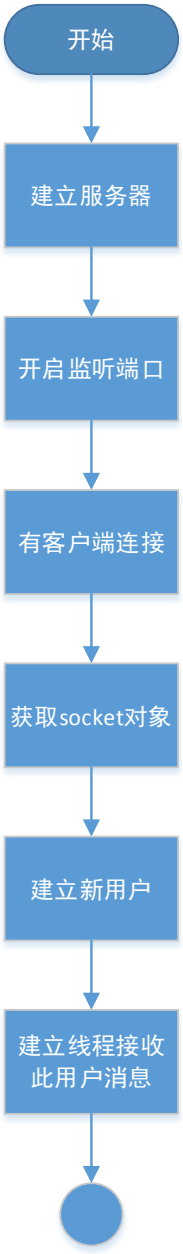
客户端主要流程：

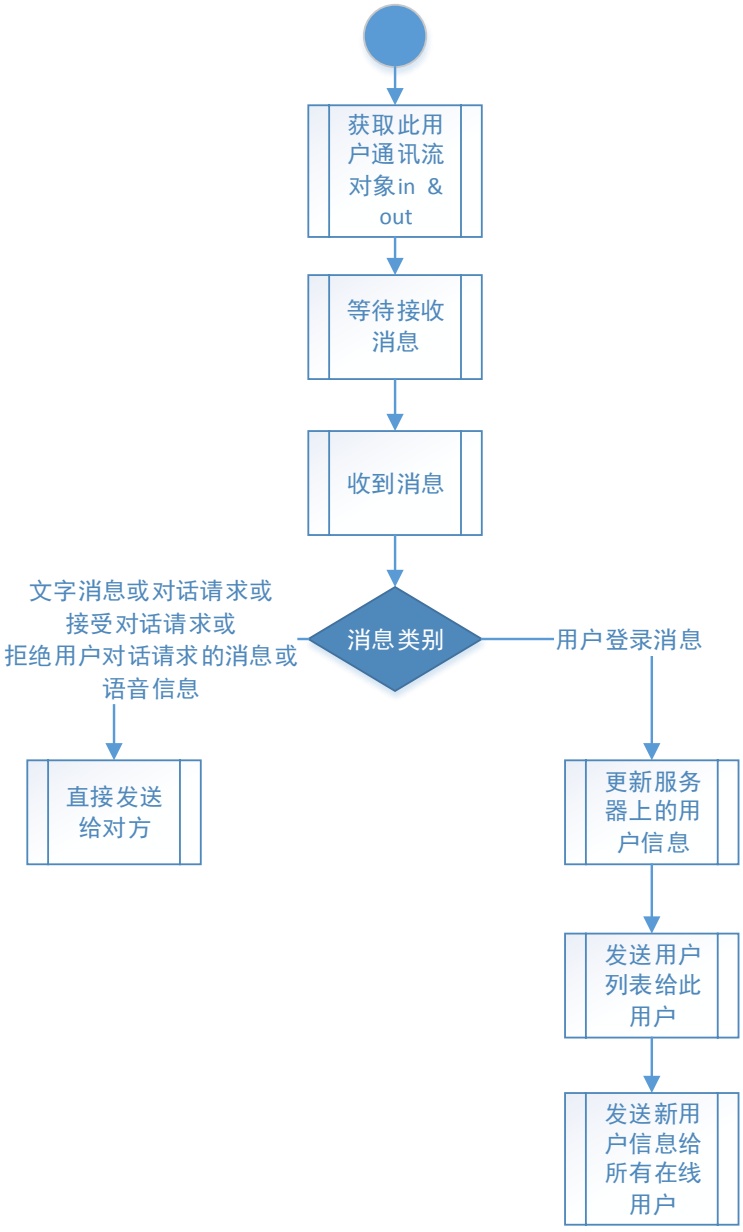


通话流程：


开始
接受或发起通话
双方同意通话
开始通话
录音线程
播放线程
录音
加密
转成json发送到服务器，有服务器转发给对方
接收网络信息流
解析jason为byte数组
解密
加入播放列表
播放

服务器主要流程：

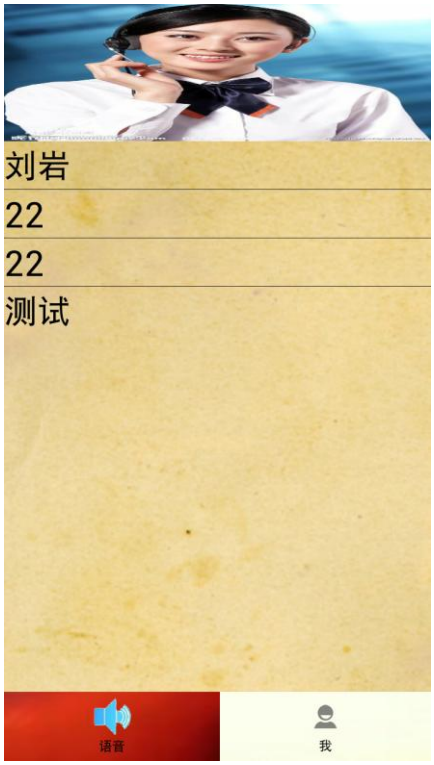

开始
建立服务器
开启监听端口
有客户端连接
获取socket对象
建立新用户
建立线程接收此用户消息


获取此用户通讯流对象in &out
等待接收消息
收到消息
消息类别
文字消息或对话请求或接受对话请求或拒绝用户对话请求的消息或语音信息
用户登录消息
直接发送给对方
更新服务器上的用户信息
发送用户列表给此用户
发送新用户信息给所有在线用户

四、 安全通讯程序实现模块

登录界面：

用户列表界面：



等待通话界面：

通话界面：

五、 项目简介及使用说明

本项目在 Android 系统上实现了“DES 加密”通话功能，使用 TCP 传送数据。由于是为了学习 DES 加密，所以做的比较简单，语音通话的降噪和回音消除都没有实现。项目中的两个文件夹分别是服务器项目和 Android 应用项目。两者都是 Eclipse 项目，基于 jdk1.6。Android 项目 sdk 版本是 Android4.2。使用时需要修改服务器项目及 android 项目下的“Const.java”文件中的 ServerIP 为你服务器的 ip，才能运行。

源码结构如下：

ChuanYinServer/ src	服务器
|- com/yichang/chuanyin/server	服务器包

Qianlichuanyin/src	客户端
|- com/yichang/qianlichuanyin/main	客户端主类包
|- com/yichang/qianlichuanyin/net	客户端网络包
|- com/yichang/qianlichuanyin/view	客户端界面包