2014 年全国大学生信息安全竞赛

作品报告

作品名称：基于蓝牙系统的随身密钥

电子邮箱：yangyankai_Mr@outlook.com

提交日期：2014 年 5 月 30 日

填写说明

1. 所有参赛项目必须为一个基本完整的设计。作品报告书旨在能够清晰准确地阐述（或图示）该参赛队的参赛项目（或方案）。

2. 作品报告采用A4纸撰写。除标题外，所有内容必需为宋体、小四号字、1.5倍行距。

3. 作品报告中各项目说明文字部分仅供参考，作品报告书撰写完毕后，请删除所有说明文字。(本页不删除)

4. 作品报告模板里已经列的内容仅供参考，作者也可以多加内容。

目　　录

摘要

如今，人们都拥有多组用户名与密码。同时，很多人由于遗忘密码或被他人盗取密钥，而对他们的生活工作带来极大的麻烦，甚至威胁到国家安全与社会稳定。

本作品设计并实现一种基于蓝牙系统的随身密钥，利用蓝牙通信技术连接手机和PC机，由手机向PC机中的加密软件提供复杂且安全的密码管理。应用所设计的随身密钥系统，用户在实施文件加密或打开加密文件时，无需记忆密钥或手动输入任何密码，从而避免因忘记密码而带来的麻烦。该系统可以大大增加密钥的复杂性和安全性，进而提高抗攻击力。同时，使用蓝牙方式传输密码还可以杜绝因偷窥而造成的密码泄露问题。该作品适用于Windows操作系统的计算机与安卓手机之间的蓝牙通讯，具有数据加解密方便、密钥安全性高等特色，并且能够广泛应用于个人、团队、企业、政府、军队等机密文件的保护，严格保证机密数据的安全性。

本作品的创新点包括：①基于蓝牙系统的身份认证模式，并将密钥存储在手机移动端，提高安全性与便捷性；②程序隐蔽性强，在系统任务栏、系统托盘中均无法查看，防止被拥有管理员权限的非法用户强行终止；③将程序完全嵌入操作系统，操作只需点击右键菜单；④定期更换密钥，防止固定密钥的短板；⑤硬件绑定，屏蔽虚假消息及请求。下一步工作包括：（1）将本系统嵌入到账号登陆时的密码输入环节中。（2）与电子锁系统配套生产蓝牙电子钥匙。（3）制作其他有关身份认证的软件等。

第 1 章　作品介绍

1.1背景分析

随着计算机的蓬勃发展，越来越多的人不喜欢使用纸质资料，纸质资料逐渐被电子版取代。相比纸质材料，电子文档具有易于修改、存储、携带、传送等诸多优点，但是，事物都是有两面性的，有优点的同时也必定存在缺点，电子文档在信息安全防护的脆弱性，使得所存储的涉及私密的信息面临严重的安全问题。

因此，对电子文件的安全防护变得至关重要。对文件进行加密，并设置一个密码是传统的保护措施，可是这样的措施在密码验证模块存在严重的安全隐患，主要包括以下几个方面：

（1）用户自己忘记密码。现实生活中需要用到密码的地方实在太多了，忘记密码也是很正常的事情，同时也是非常麻烦的事，人们迫切需要更好的身份验证方式来取代传统的密码验证。

（2）由于各种情况而产生的密码泄露。直接从键盘读入密码的方式很容易被木马程序获取密码，即使用软键盘，由于可以手动输入的密码都不会太长，所以通过电脑屏幕截屏以及鼠标动作记录，再人工破解密码也不是问题。

用户因忘记密码导致文件无法打开，最多就是该文件报废，文件中的数据仍是安全的，不会泄密。但是，如果是密码泄露了，文件又同时被窃取，那将直接导致该文件中的数据泄密，对个人来说，这样的泄密可能影响没那么大，但是对于一个企业，重要信息的泄露很可能导致大量财产损失，甚至是破产，对一个国家来说，危害就更大了。

1.2相关工作

随着信息化的高速发展，人们对信息安全的需求接踵而至，人才竞争、市场竞争、金融危机、敌特机构等都给企事业单位的发展带来巨大风险，内部窃密、黑客攻击、无意识泄密等窃密手段成为了人与人之间、企业与企业之间、国与国之间的安全隐患。

1.2.1 当今身份认证的三种基本方法

1、根据你所知道的信息来证明你的身份(what you know，你知道什么)；

2、根据你所拥有的东西来证明你的身份(what you have，你有什么)；

3、直接根据独一无二的身体特征来证明你的身份(who you are，你是谁)，比如指纹、面貌等。

1.2.2 当今几种常见的认证形式

1、静态密码：用户的密码是由用户自己设定的。在网络登录时输入正确的密码，计算机就认为操作者就是合法用户。如果密码是静态的数据，在验证过程中需要在计算机内存中传输，可能会被木马程序或网络中截获。因此，静态密码机制无论是使用还是部署都非常简单，且从安全性上讲，用户名/密码方式也不是一种安全的身份认证方式。 它利用what you know方法。

2、智能卡（IC卡）：一种内置集成电路的芯片，芯片中存有与用户身份相关的数据，智能卡由专门的厂商通过专门的设备生产，是不可复制的硬件。智能卡由合法用户随身携带，登录时必须将智能卡插入专用的读卡器读取其中的信息，以验证用户的身份。智能卡认证是通过智能卡硬件不可复制来保证用户身份不会被仿冒。然而由于每次从智能卡中读取的数据是静态的，通过内存扫描或网络监听等技术还是很容易截取到用户的身份验证信息，因此还是存在安全隐患。它利用what you have方法。

3、短信密码：短信密码以手机短信形式请求包含6位随机数的动态密码，身份认证系统以短信形式发送随机的6位密码到客户的手机上。客户在登录或者交易认证时候输入此动态密码，从而确保系统身份认证的安全性。它利用what you have方法。

4、动态口令：目前最为安全的身份认证方式，也利用what you have方法，也是一种动态密码。

动态口令牌是客户手持用来生成动态密码的终端，主流的是基于时间同步方式的，每 60 秒变换一次动态口令，口令一次有效，它产生 6 位动态数字进行一次一密的方式认证。但是由于基于时间同步方式的动态口令牌存在 60 秒的时间窗口，导致该密码在这 60 秒内存在风险，现在已有基于事件同步的，双向认证的动态口令牌。基于事件同步的动态口令，是以用户动作触发的同步原则，真正做到了一次一密，并

且由于是双向认证，即：服务器验证客户端，并且客户端也需要验证服务器，从而达到了彻底杜绝木马网站的目的。

5、数字签名：数字签名又称电子加密，可以区分真实数据与伪造、被篡改过的数据。这对于网络数据传输，特别是电子商务是极其重要的，一般要采用一种称为摘要的技术，摘要技术主要是采用 HASH 函数（HASH(哈希)函数提供了这样一种计算过程：输入一个长度不固定的字符串，返回一串定长度的字符串，又称HASH值）将一段长的报文通过函数变换，转换为一段定长的报文，即摘要。身份识别是指用户向系统出示自己身份证明的过程，主要使用约定口令、智能卡和用户指纹、视网膜和声音等生理特征。数字证明机制提供利用公开密钥进行验证的方法。

6、生物识别：运用who you are方法， 通过可测量的身体或行为等生物特征进行身份认证的一种技术。生物特征是指唯一的可以测量或可自动识别和验证的生理特征或行为方式。生物特征分为身体特征和行为特征两类。身体特征包括：指纹、掌型、视网膜、虹膜、人体气味、脸型、手的血管和DNA等；行为特征包括：签名、语音、行走步态等。[1-4]

1.3系统功能描述

基于蓝牙的随身密钥系统主要功能包括：密钥初始化生成、加密文件、解密文件、密码验证读取文件四部分：

1、密钥生成及管理：由PC端生成密钥，加密后传输到手机并存储；

2、加密文件：从手机获取密钥后调用AES加密算法对文件进行加密；

3、解密文件：身份认证通过后从手机获取密钥并调用AES解密算法解密文件；

4、读取文件：身份认证通过后对文件进行解密，用户关闭文件后自动对文件重新进行加密。

1.4应用前景分析

本系统能实现各种身份验证式管理，基于预期的访问控制策略保证了用户身份的唯一性，理论上可以应用于大部分需要身份认证的场景，具有广阔的市场前景，例如以下几个场景：

1、对电子文件的保护：文件加密后，读取需要解密，解密时则需要进行身份认

证，这个过程中便可以使用本作品，并且相对现有产品在访问控制的安全性与便捷性上得到很大的提升。这里对个人、企业、政府、军队、银行等各种需要保护机密文件的地方均适用；

2、适用于绝大多数账号登陆：账号登陆时需要输入密码，而这个密码是越复杂越好，但是目前很多人不愿意使用长且复杂的密码，原因是输入麻烦，又容易忘记，本作品正好解决了这两个问题。在保护账号安全方面得到了极大的提升；

3、适用于电子锁系统：目前很多人都拥有多把钥匙（如自己家大门钥匙、办公室钥匙、车钥匙等），一大串钥匙挂在腰间实在不方便，使用本产品可以将这些钥匙换成超长密钥全部“装”入你的手机，用一部手机代替所有的钥匙，同时实现了安全与便捷。当然，在这方面还需要电子锁技术的发展与支持，在不久的将来还是可以实现的。

第 2 章　作品的设计与实现

2.1系统总体方案

鉴于当前手动输入密码的繁琐性与不安全性，本系统采用将超长密码存储在手机端，并在需要密码的时候通过蓝牙密文传输，具体实现方案如下：

首先，开发组搭建了一个需要进行密码验证的场景——读取加密后的文件。在读取过程中，需要对用户进行身份认证，认证通过才开始对文件进行解密、读取，关闭文件后又自动对文件进行加密。流程图如图2-1所示（该过程需要蓝牙始终处于开启并可用状态）：

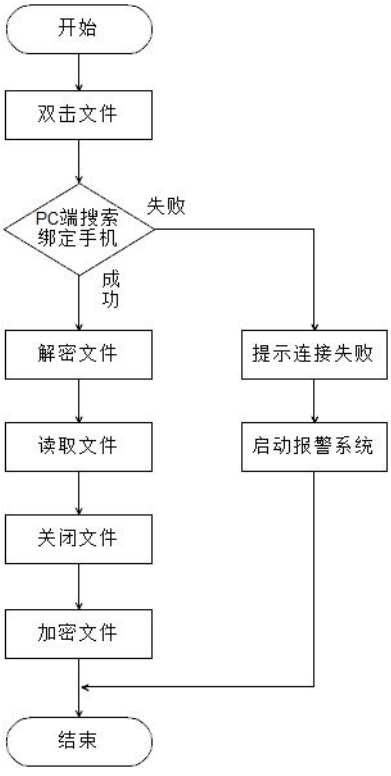

图 2-1 读取文件流程图

2.2 软件流程

2.2.1 软件整体流程

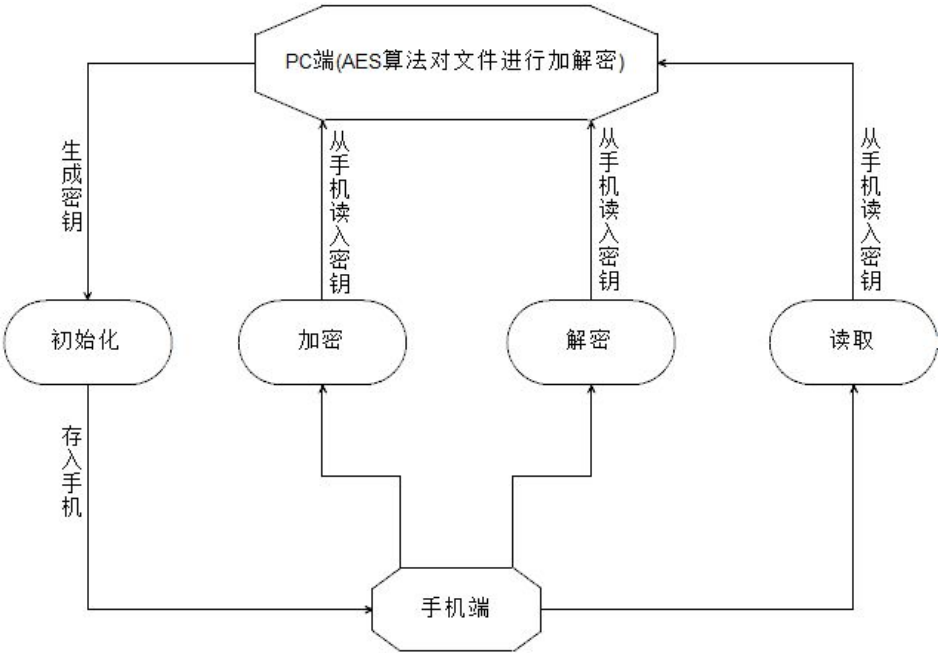

图 2- 2 软件整体流程图

软件主要分为初始化、加密、解密、读取4个模块完成，如图2-2所示。其中读取是核心模块，初始化是重要模块。

2.2.2 软件详细流程

（1）初始化模块

这个模块主要完成了计算机与手机一对一绑定，生成第一次使用需要的密钥并存入手机。绑定手机时，计算机与手机均记录了彼此的蓝牙地址，并且在今后使用本系统时，该计算机只会与该手机进行通信，该手机也只会与该计算机进行通信。计算机首次生成128位随机密钥后立即对该密钥进行加密（AES算法），然后发送到手机端，并存储在手机中。流程图如图2-3所示：

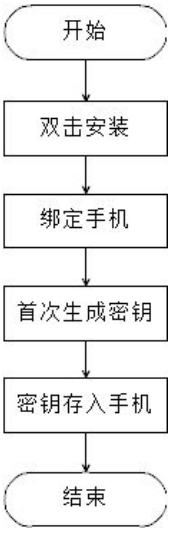

图 2-3 初始化模块流程图

（2）加密模块

鼠标右键点击加密后，PC端会通过蓝牙地址直接寻找出首次设定的手机并与其连接，向其请求发送密钥用于加密，若无法找到该手机则会提示连接失败并结束程序，若连接成功，手机端确认是初始化时的PC机发送的请求后便会将密钥以密文的形式发送到PC端，PC端接受密文后，对其进行解密，调用加密算法（AES算法）并使用该密钥对文件进行加密，加密完成后直接将密钥销毁并结束程序。流程图如图2-4所示：

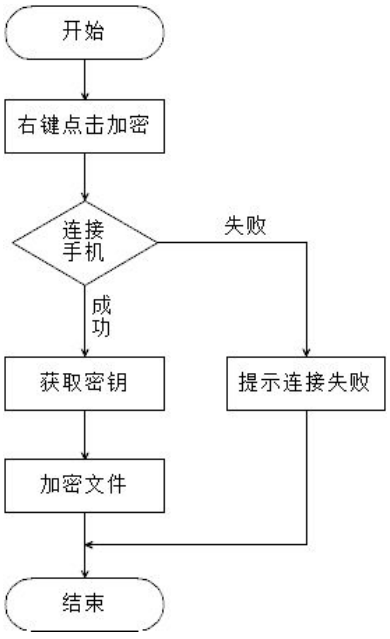

图 2-4 加密模块流程图

（3）解密模块

解密过程与加密过程类似。鼠标右键点击解密后，PC端会直接寻找出首次设定的手机并与其连接，向其请求发送密钥用于解密，若无法找到该手机则会提示连接失败并启动报警系统，若连接成功，手机端确认是初始化时的PC机发送的请求后便会将密钥以密文的形式发送到PC端，PC端接受密文后，对其进行解密，调用解密算法（AES算法）并使用该密钥对文件进行解密，解密完成后直接将密钥销毁并结束程序。流程图如图2-5所示：

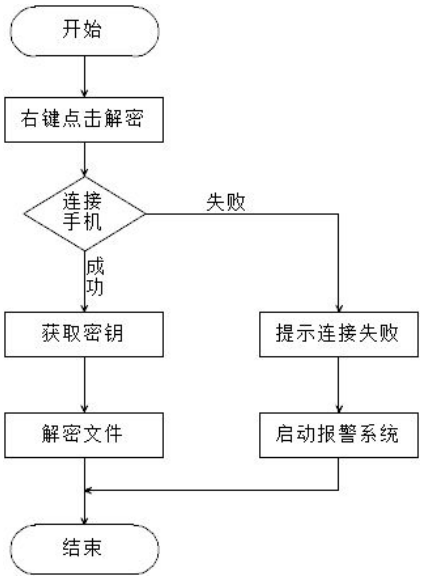

图 2-5 解密模块流程图

（4）读取模块

该模块作为密码验证的载体，在验证通过时调用解密与加密模块的功能来观察密码验证是否成功。

双击已加密的文件，PC端则向绑定手机请求发送密钥，验证失败会提示失败并启动报警系统，验证通过则调用解密算法对文件进行解密，解密完成后即打开文件，用户关闭文件后，系统自动对文件重新加密。整个过程中，密钥只有在验证的时候才处于明文状态，其余时间均处于密文状态，即使被人恶意截取，对方也无法立即使用密钥，并且系统还会提示定期更换密钥，就算黑客破解了密钥的密文，系统也早已不用那个已被破解的密钥了。读取模块流程图如图2-1所示：

2.3实现原理

2.3.1 AES 算法介绍

严格地说，AES和Rijndael加密法并不完全一样（虽然在实际应用中二者可以互换），因为Rijndael加密法可以支持更大范围的区块和密钥长度：AES的区块长度固定为128比特，密钥长度则可以是128，192或256比特；而Rijndael使用的密钥和区块长度可以是32位的整数倍，以128位为下限，256比特为上限。加密过程中使用的密钥是由Rijndael密钥生成方案产生[5]。

截至2006年，针对AES唯一的成功攻击是旁道攻击。美国国家安全局审核了所有的参与竞选AES的最终入围者（包括Rijndael），认为他们均能够满足美国政府传递非机密文件的安全需要。

至2006年为止，最著名的攻击是针对AES7次加密循环的128位密钥版本，8次加密循环的192比特密钥版本，和9次加密循环的256比特密钥版本所作的攻击[6]。

由于已遭破解的弱版的AES，其加密循环数和原本的加密循环数相差无几，有些密码学家开始担心AES的安全性：要是有人能将该著名的攻击加以改进，这个区块加密系统就会被破解。在密码学的意义上，只要存在一个方法，比穷举法还要更有效率，就能被视为一种“破解”。故一个针对AES128位密钥的攻击若“只”需要2^{120}计算复杂度（少于穷举法2^{128}），128位密钥的AES就算被破解了；即便该方法在目前还不实用。从应用的角度来看，这种程度的破解依然太不切实际。最著名的暴力攻击法是distributed.net针对64位密钥RC5所作的攻击。（该攻击在2002年完成，根据摩尔定律，到2005年12月可以破解66比特密钥的RC5加密。）

其他的争议则着重于AES的数学结构。不像其他区块加密系统，AES具有相当井然有序的代数结构。虽然相关的代数攻击尚未出现，但有许多学者认为，把安全性创建于未经透彻研究过的结构上是有风险的。Ferguson，Schroeppel和Whiting因此写道：“我们很担心Rijndael[AES]算法应用在机密系统上的安全性。”[7]

2002年，Nicolas Courtois和Josef Pieprzyk发表名为XSL攻击的理论性攻击，试图展示AES一个潜在的弱点。但几位密码学专家发现该攻击的数学分析有点问题，推测应是作者的计算有误。因此，这种攻击法是否对AES奏效，仍是未解之谜。就现阶段

而言，XSL攻击AES的效果并不显著，故将之应用于实际情况的可能性不高。

关于旁道攻击。旁道攻击不攻击密码本身，而是攻击那些基于不安全系统（会在不经意间泄漏信息）上的加密系统。

2005年4月，D.J.Bernstein公布了一种缓存时序攻击法，他以此破解了一个装载OpenSSL AES加密系统的客户服务器[8]。为了设计使该服务器公布所有的时序信息，攻击算法使用了2亿多条筛选过的明码。对于需要多个跳跃的国际互联网而言，这样的攻击方法并不实用[9]。Bruce Schneier称此攻击为「好的时序攻击法」[10]。

2005年10月，Eran Tromer和另外两个研究员发表了一篇论文，展示了数种针对AES的缓存时序攻击法[11]。其中一种攻击法只需要800个写入动作，费时65毫秒，就能得到一把完整的AES密钥。但攻击者必须在执行加密的系统上拥有执行程序的权限，方能以此法破解该密码系统。

AES算法流程图如图2-7所示：

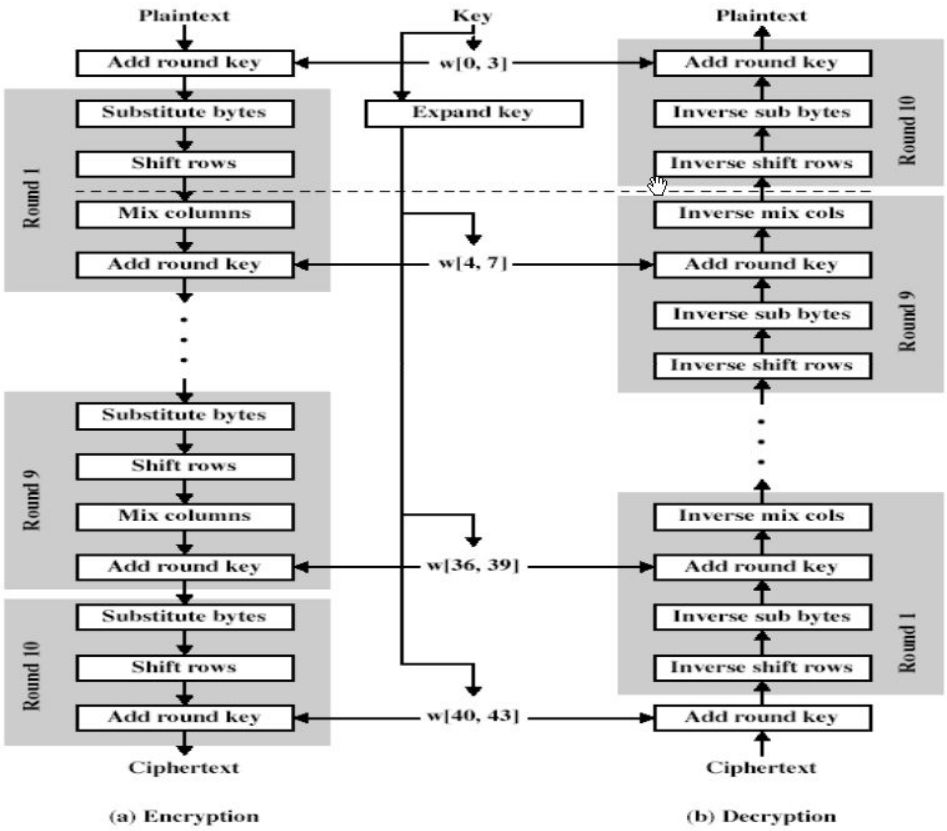

图 2-7 AES 算法流程图

2.3.2 密钥管理

密钥采用RNGCryptoServiceProvider()真随机数发生函数生成，随机性高，破解难度大，安全性强。

密钥在首次生成的时候就是以密文的形式存储在手机端，每次需要验证的时候从手机端将密文发送到PC端，解密后在进行验证，验证完后密钥不会保存在计算机上。并且密钥在整个过程中只有在验证那一瞬间是处于明文状态，其余时间均是处于密文状态。

为了安全起见，系统每隔15天就会提示用户重新生成一次密钥，以覆盖之前的密钥，防止密钥密文被人获取并通过各种方法破解后，使本作品失去安全性。

第 3 章　作品测试与分析

3.1测试方案

开发组对整个系统进行了完备的测试，主要分为功能测试、安全性测试、通讯测试以及密钥随机性测试四个方面。其中：

功能性测试，主要对作品的 4 个模块（初始化模块、加密模块、读取模块、解密模块）的功能设计进行验证，测试系统的运行结果是否达到预期效果。

安全性测试，本项测试主要针对加密后的文件是否可以通过解密以外的方式打开，为确保加密后的文件在理论上是安全的。

通讯测试，该项测试主要包括有效通讯距离测试、通讯效率测试两项。

密钥随机性测试，该项测试主要通过重复调用随机函数，生成大量随机数，并比较随机数是否有重复。

3.2测试环境搭建

PC 端：找一台未安装过本软件的正常的计算机，若未安装蓝牙模块，则先安装好所需的蓝牙模块的程序；若已安装蓝牙模块，只需检测蓝牙是否可用即可。确保该计算机能支持本软件的运行。

手机端：找一部功能正常的安卓手机，且蓝牙通信功能还能正常运行即可。确保手机能与 PC 端通过蓝牙正常连接。

Visual Studio 2010，用于编写随机性测试的控制台应用程序。

3.3测试设备

一台具备完整蓝牙功能的计算机，且可正常运行蓝牙程序（事先未安装过本软件）；

一部支持蓝牙通信的安卓手机（事先未安装过本软件）。

一台装有 Visual Studio 2010 的计算机。

3.4测试过程

3.4.1 功能性测试

测试全程需要 PC 端与手机端均处于蓝牙开启并正常工作状态。

(1)初始化模块

双击安装包中的“双击安装”应用程序，系统则会自动进行安装，安装完成后，进入手机绑定模块，选择好手机后，开始选择手机进行绑定，手机端确认通过后，同时也在手机端存入了密码，即完成了初始化模块。结果如图 3-1 所示：

图 3- 1 手机端保存密码

(2)加密模块

创建一个测试文件，如图 3-2 所示（理论上可对其他格式文件进行加密，这里采用 txt 格式进行测试）

图 3- 2 测试文件

右击加密文件菜单项对文件进行加密，结果如图 3-3 以及图 3-4 所示：

图 3- 3 加密成功后的测试文件

图 3- 4 加密成功提示

加密后的文件图标也对其进行了更换，以便让用户能清楚的分辨出是否为加密文件（如图 3-3 所示）。

(3)读取模块

当绑定手机手机在有效范围内且已成功连接时，双击加密后的文件，手机端通过验证后（图 3-5）便可直接读取其内容。

图 3- 5 手机端通过验证并发送密码

若系统无法找到绑定手机，则会出现如图 3-6 的提示框，点击“确定”后会会触发报警系统（图 3-7）。

图 3-6 未找到解锁手机

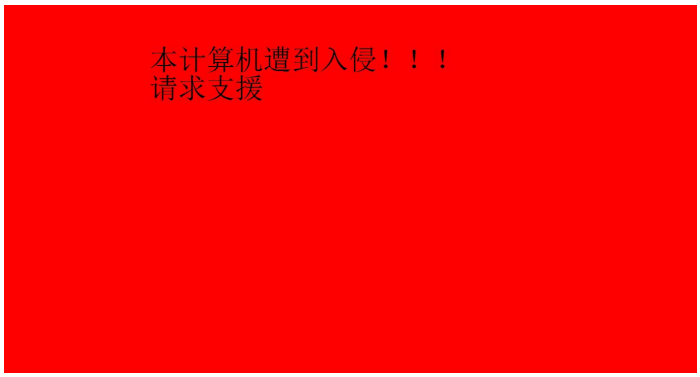

图 3-7 报警系统界面

(4)解密模块

解密过程与读取类似，绑定手机手机在有效范围内且已成功连接时，可以成功解密（图 3-8）；否则仍会弹出如图 3-6 的提示框，并触发报警系统（图 3-7）。

图 3-8 解密成功

3.4.2 安全性测试

该测试主要采用两种方式试图强制打开加密后的文件。

1、修改打开方式强制将加密后的文件改为txt文件进行打开，文件打开后处于乱码状态（图3-9）。

图 3-9 乱码文件 1

2、将文件后缀名修改为txt，打开后仍是乱码状态（图3-10）。

图 3-10 乱码文件 2

3.4.3 通讯测试

(1)有效距离测试

将处于与计算机正常连接状态的手机从距离计算机 100cm 的距离开始，每隔 100cm 观察一次手机是否还是与计算机保持连接状态，共测试 3 次，测试结果如表 3-1 所示：

表 3-1 有效距离测试结果表

手机与计算机之间的距离/cm	100	200	300	400	500	600	700	800	900	1000	1100
是否正常运行1	是	是	是	是	是	是	是	是	否	否	否
是否正常运行2	是	是	是	是	是	是	是	否	否	否	否
是否正常运行3	是	是	是	是	是	是	是	否	是	否	否

(2)通讯效率测试

本项测试是为了获取从计算机向手机请求发送密钥至计算机接收到密钥这一段时间，共进行 3 次测试，结果如表 3-2 所示：

表 3-2 通讯效率测试结果表

手机与计算机之间的距离/cm	60	120	180	240	300	360	420	480
花费时间1/ms	39	61	66	65	44	70	42	43
花费时间2/ms	64	41	40	43	45	47	56	45
花费时间3/ms	49	62	41	35	45	45	103	46

3.4.4 随机性测试

通过大量数据的测试，可以在很大程度上体现数据的随机性，测试结果如图 3-11 所示：

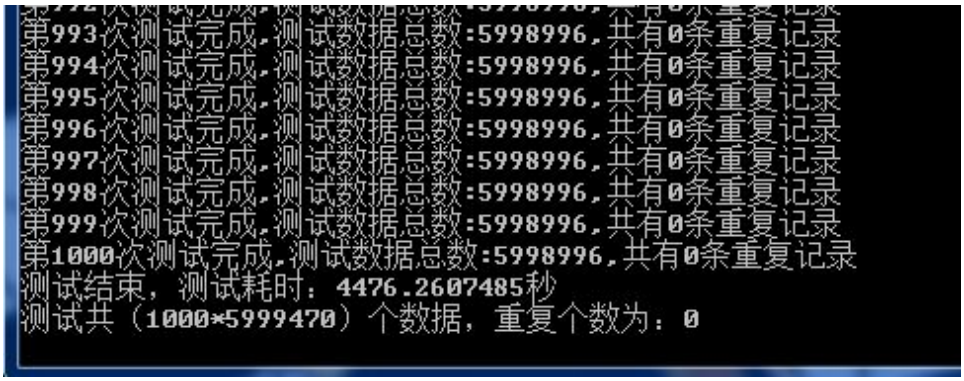

图 3-11 随机性测试结果图

3.5 结果分析

本次测试结果如表 3-3 所示：

表 3-3 功能测试结果表

分类	测试项目	是否达到预期效果
功能测试	初始化	是
	加密	是
	读取	是
	解密	是
安全性测试	修改打开方式	是
	修改后缀名	是

从表 3-1 中可以看出：手机与计算机的距离在 7 米以内时，手机与计算机可以稳定连接，7 米—10 米不稳定连接，大于 10 米后无法连接。

从表 3-2 中可以看出，手机与计算机的距离对通讯效率的影响很小，主要还是跟设备的稳定性有关。

从图 3-10 可以看出，在大量数据的测试后，仍没有出现重复的数据，说明该算法的随机性还是相对较高的。

第 4 章　创新性说明

该系统克服了用户在输入密码时容易被木马病毒获取密码的缺点，使用文件加密技术对文件进行自动加密，并配备了基于蓝牙的身份验证解密模式，在用户和操作系统上实现对文件的双重立体保护。整个系统是一个不可分割的整体，各个模块分工明细，合作完善，构成一个严密的保护体系。

具体来说，该系统具有以下创新点：

1. 基于蓝牙系统的身份认证模式

传统的身份验证仅为单纯的密码验证，这样的验证方式极其容易被木马程序窃取密码并获得访问权限。本系统采用蓝牙的方式，将一段 128 位超长密码存储在手机端，在需要验证的时候，与 PC 端进行蓝牙对接，并通过蓝牙的方式传输密码进行验证，保证的密码的安全性，且用户不需要手动输入密码，也不需要记住密码，从而避免了因密码泄露、遗忘而带来的不必要的损失。

2. 程序隐蔽性强

当不怀好意的人已经发现计算机在运行本程序，可能会强行中断本程序，遗憾的是，在任务栏、系统托盘中根本看不到该程序，但它确确实实是在运行的。

3. 将程序完全嵌入操作系统

为保证系统不被恶意软件破解，开发组将其完全嵌入操作系统。本程序运行时用户几乎看不到任何界面，用户操作就与压缩/解压文件一般简便。

4. 采用非静态密钥解密

每隔 15 天就对密码进行一次更新，万一密码的密文被人恶意截取，并且在一定时间后被破解成明文，也可以确保对方拿到的是失效后的密码。

5. 硬件绑定

在初始化时PC端与手机端便记录了彼此的蓝牙地址，程序运行过程中只会与具有该蓝牙地址的设备进行通信，从而确保了不会被伪造的请求迷惑而发送密钥给非法用户。

第 5 章　总结

针对当前密码管理所面临的严重安全问题，本系统从密码的构成、储存，验证等角度实现了对密码的安全输入与管理，可以用来防止他人偷窥密码，密码密文不慎被窃取时，对方也无法在短时间内将其破解，从被窃前与被窃后两个环节保证了密码的安全性。并且具有以下创新性：①基于蓝牙系统的身份认证模式，并将密钥存储在手机移动端，提高安全性与便捷性；②程序隐蔽性强，在系统任务栏、系统托盘中均无法查看，防止被拥有管理员权限的非法用户强行终止；③将程序完全嵌入操作系统，操作只需点击右键菜单；④定期更换密钥，防止固定密钥的短板；⑤硬件绑定，屏蔽虚假消息及请求。

在本作品已取得的成果的基础上，下一步工作包括：（1）将本系统嵌入到账号登陆时的密码输入环节中。（2）与电子锁系统配套生产蓝牙电子钥匙。（3）制作其他有关身份认证的软件等。

参考文献

[1] 岳峰,左旺孟,张大鹏. 掌纹识别算法综述[J]. 自动化学报,2010,(3).

[2] 贲晛烨,徐森,王科俊. 行人步态的特征表达及识别综述[J]. 模式识别与人工智能,2012,(1).

[3] 田启川,张润生. 生物特征识别综述[J]. 计算机应用研究,2009,(12).

[4] 王科俊,侯本博. 步态识别综述[J]. 中国图象图形学报,2007,(7).

[5] Vincent, Rijmen, Joan, Daemen. 高级加密标准[EB/OL]. http://zh.wikipedia.org/wiki/%E9%AB%98%E7%BA%A7%E5%8A%A0%E5%AF%86%E6%A0%87%E5%87%86, 2014-05-19

[6] Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Mike Stay, David Wagner, and Doug Whiting, Improved Cryptanalysis of Rijndael, Fast Software Encryption, 2000 pp213–230.

[7] Niels Ferguson, Richard Schroeppel, Doug Whiting. A simple algebraic representation of Rijndael. Proceedings of Selected Areas in Cryptography, 2001, Lecture Notes in Computer Science (PDF/PostScript). Springer Verlag. 2001: pp. pp. 103–111 [2006-10-06].

[8] Daniel J. Bernstei. Cache-timing attacks on AES. Citeseer. 2005.04.

[9] Lou Scheffer. Successful remote AES key extraction. 2005-04-17 [2011-05-16].

[10] Bruce Schneier. AES Timing Attack. 2005-05-17 [2011-05-16].

[11] Eran Tromer , Dag Arne Osvik and Adi Shamir. Efficient Cache Attacks on AES, and Countermeasures. Journal of cryptology. 2010, 23 (1): 37–71.