

专业课程设计报告

（ 2022/ 2023学年 第 一 学期）

题 目： U盘加密系统

|  |  |
| --- | --- |
| **专 业** | **信息安全** |
| **学 生 姓 名** | **陈瑾瑜** |
| **班 级 学 号** | **B190307** |
| **指 导 教 师** | **张洁** |
| **指 导 单 位** | **计算机学院、软件学院、网络空间安全学院** |
| **日 期** | **2022.10.24-2022.11.06** |

|  |  |  |
| --- | --- | --- |
| **课程目标** | **评价准则** | **计分（每项10分）** |
| 课程目标1：通过课程设计，培养学生综合应用信息安全、计算机技术等领域专业知识的技能。（20分） | 1、能够掌握信息安全的相关基础知识，并能够针对求解的工程问题，收集资料进行合理的分析与设计。 |  |
| 2、从软件的分析、设计到编制调试，结合计算机网络理论知识、编程语言以及程序设计的方法，能够解决一个和信息安全相关的问题。 |  |
| 课程目标2：解决信息安全领域复杂工程问题的实践创新能力。（20分） | 3、通过调研，能够选择合适的程序设计语言与编程开发平台，对求解的工程问题进行编程实现。 |  |
| 4、具备一定的人机交互设计意识，人机交互设计合理、友好，操作简便。 |  |
| 课程目标3：文献调研与资料收集能力，问题发现、研究、分析与解决能力。（10分） | 5、具备一定自学能力与探索创新意识，能够充分利用教科书及其资源（如网络等）自学新知识与新技能。 |  |
| 课程目标4：培养工程工具运用能力，能够利用仿真软件或实验系统对信息安全系统进行模拟和预测，并理解仿真软件或实验硬件的局限性。（20分） | 6、能够结合计算机软硬件资源，合理选用算法、数据结构、数据存储方式等技术手段，理解相关算法，对求解的工程问题进行有效建模和求解。 |  |
| 7、掌握调试方法与工具，对程序开发过程中出现的问题进行分析、跟踪与调试，并能够进行充分测试。 |  |
| 课程目标5：分组完成一次项目设计与开发的全过程，组内成员通过讨论和交流解决课程设计中的难题，能在实验报告中准确阐述课程设计的内容，能够清晰陈述观点和回答问题。（30分） | 8、组内成员之间有一定的团队合作，互通有无。 |  |
| 9、具备一定的语言表达能力与文字处理能力，能够结合复杂工程问题撰写报告，报告内容和实验数据详实，格式规范。 |
| 10、能够正确、完整地回答指导教师关于课题的问询，反映其对课题内容，以及相关的工程基础知识具有较好的理解和掌握。 |
| 专业课程设计能力测评总分 | |  |
| **指导教师： 年 月 日** | | |
| **备注：加上平时成绩之后换算的总评成绩及等级（优、良、中、及格等）：** | | |

**具体课题题目**

**U盘加密系统**

**一、课题内容和要求**

**（一）课题内容**

实现一个对u盘进行完全加密或者部分加密的系统。

1.对u盘进行部分或者全部加密；

2.采用对称加密算法进行u盘数据加密；

3.对称加密算法的密钥要用口令或者公钥加密；

4.可以将部分加密的u盘文件加载为一个新的虚拟磁盘。

**二、需求分析和总体设计**

2.1本课题的主要功能包括：

1.对u盘进行加密；

2.采用对称加密算法进行u盘数据加密；

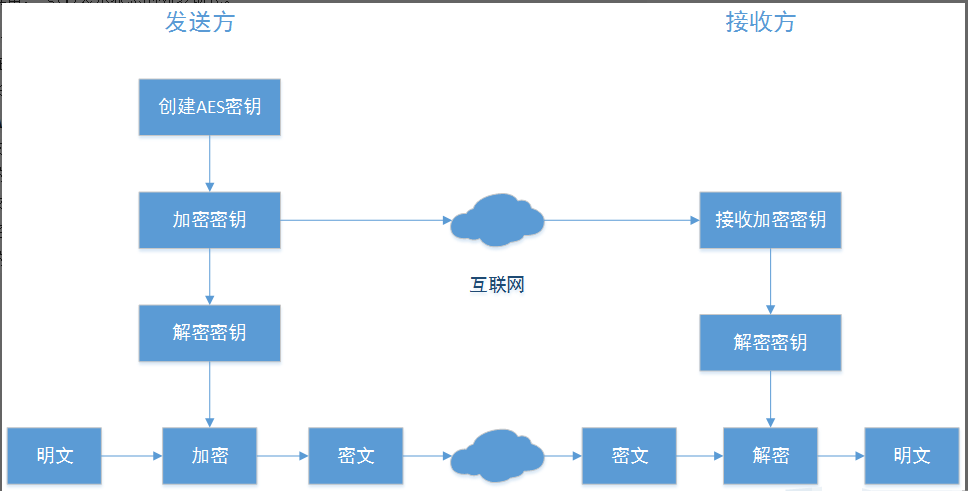
3.用口令或者公钥加密对称加密算法的密钥；

4.可以将部分加密的u盘文件加载为一个新的虚拟磁盘。

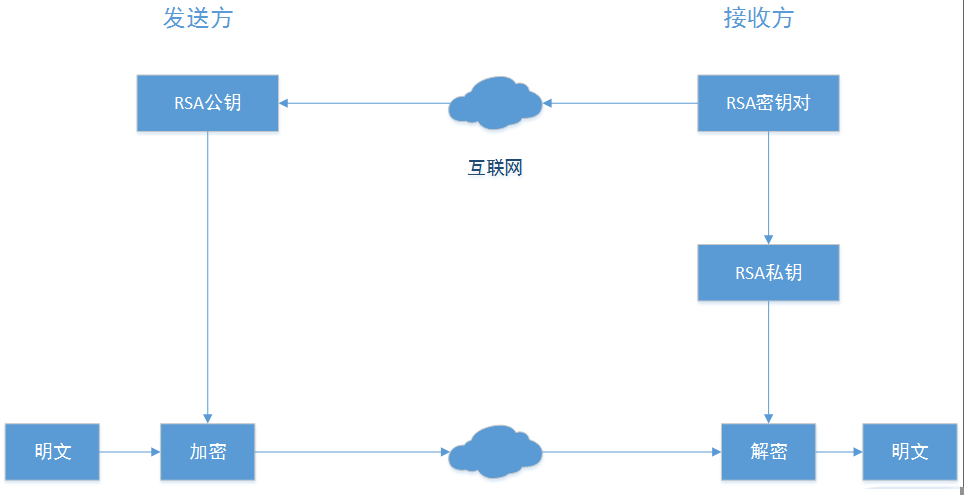
**三、相关功能模块详细设计**

1 模块内的数据结构设计

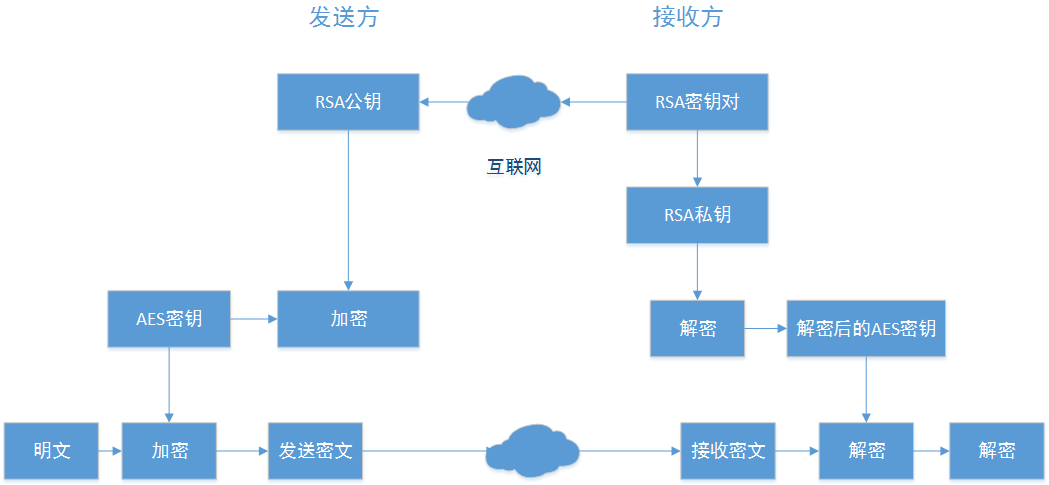
2 模块程序流程图设计



图（1） AES算法流程



图（2） RSA算法流程



图（3） AES与RSA相结合加密流程

1. **部分核心代码**

1.生成RSA公钥私钥（部分）

1.随机取两个不相等的质数pq;我们取两个大质数:

2.取两个数的乘积

3.根据欧拉函数算出φ(n):

φ(n) = φ(pq) = φ(p)φ(q)

4.随机取一个整数,要求1<e<φ(n),并且与φ(n)互质;

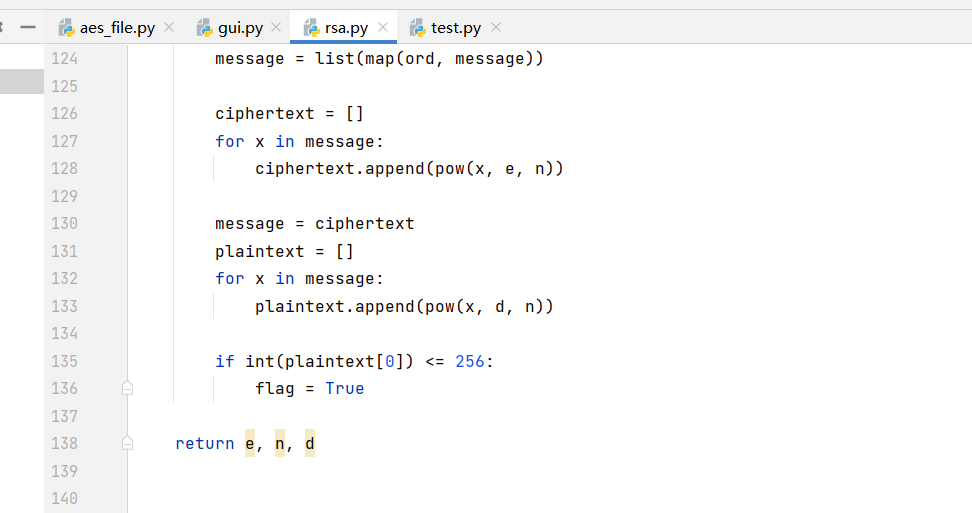
我们在此区间取一个质数,根据质数性质得知,质数与其他数互质;

5.我们计算对e 的φ(n)模反元素d;

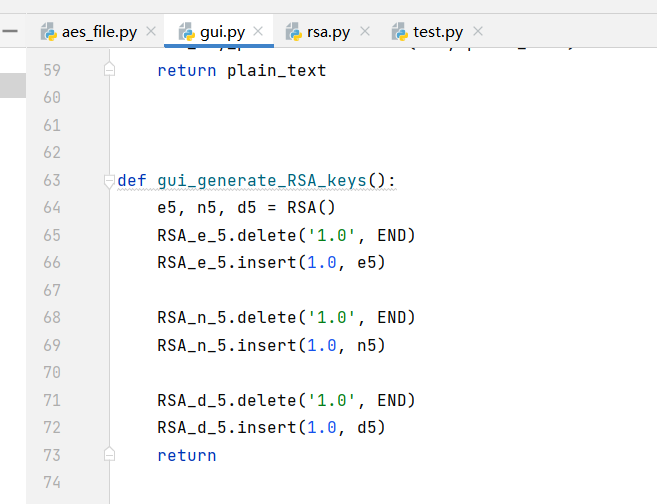
6.我们对公钥、私钥进行封装

****

图（4） RSA公钥私钥生成（1）

****

图（5） RSA公钥私钥生成（2）

****

图（6） RSA公钥私钥生成（3）

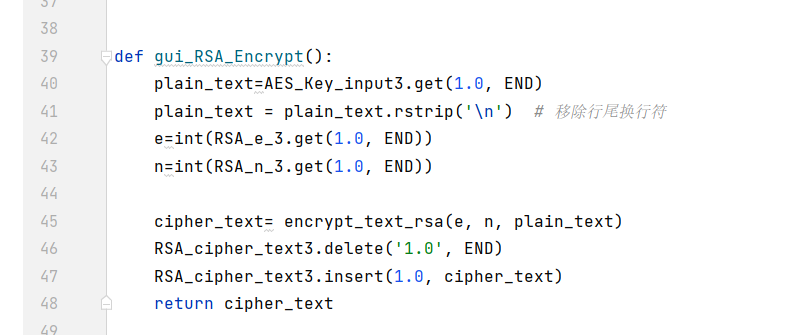
1. 利用RSA生成的公钥私钥对AES进行加密

我们都知道在通信传输中只能传输0和1，取值过程中:所以m=为数字，m必须是整数（字符串可以取ascii值或unicode值），且m必须小于n。如果偏大,可以分段加密:

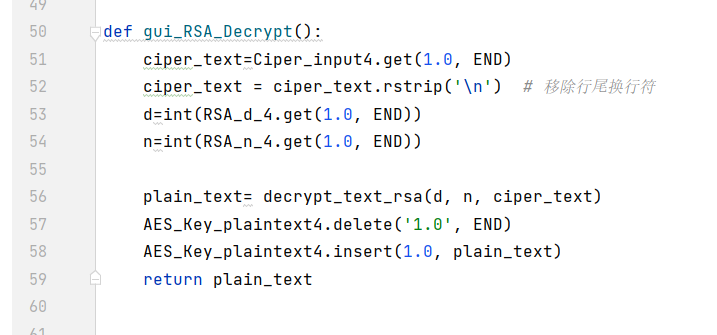
所谓”加密”，就是使用下面的加密公式算出下式的密文c：

M^e≡c(modn)

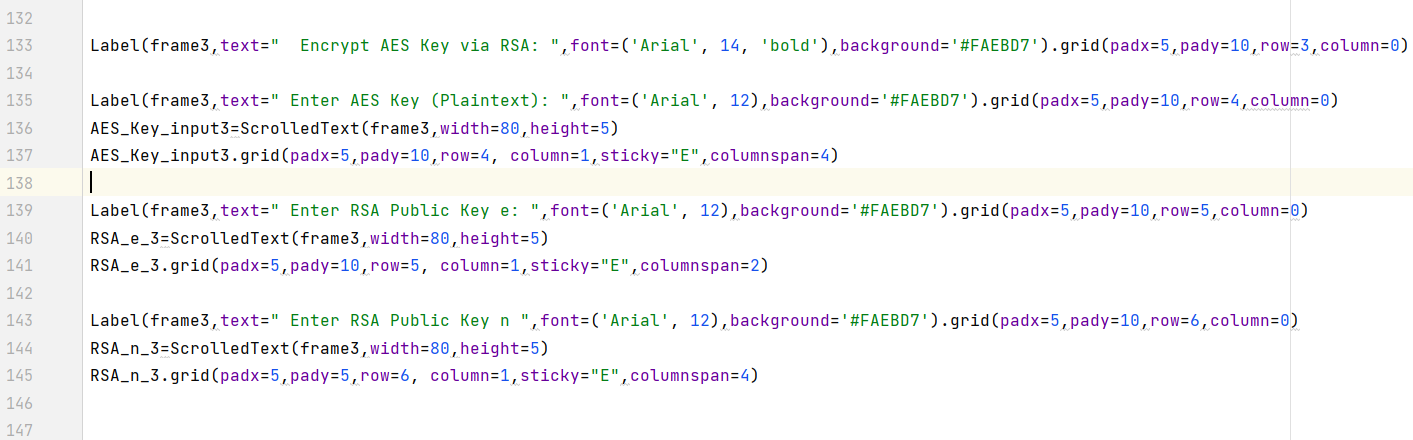
即将m,e,n代入进去，求解算出c，c即为密文



图（7） RSA 算法加密



图（8） RSA算法解密



图（9） 用RSA公钥加密AES密钥（1）



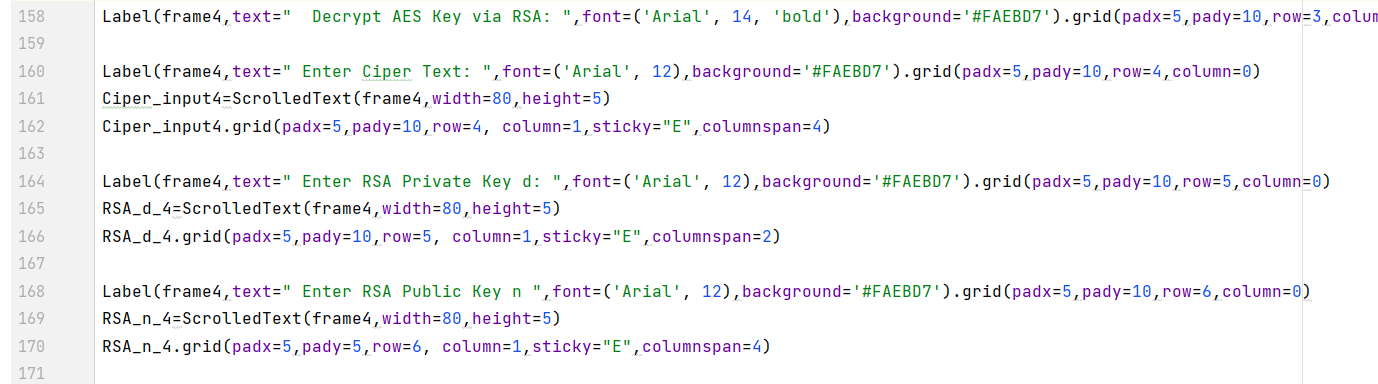
图（10） 用RSA公钥加密AES密钥（2）

解密实现过程:

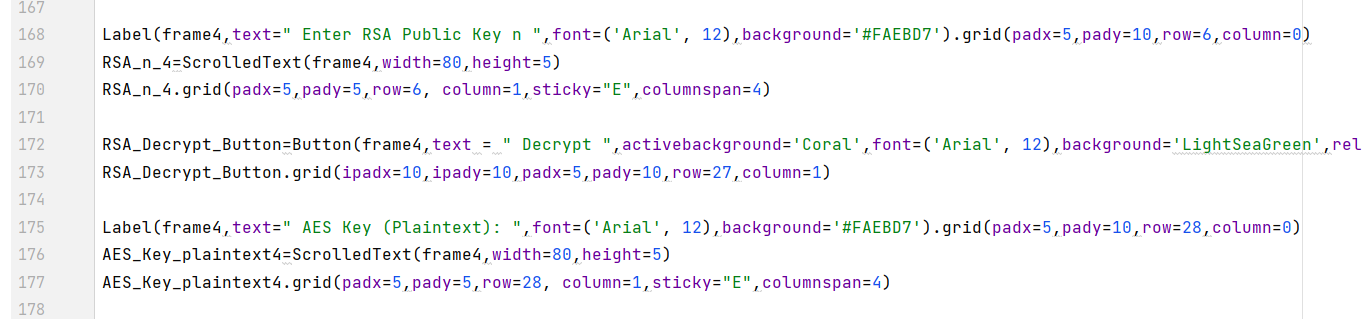
你拿到我发过来的密文C，就用下面的欧拉定理公式进行解密出明文m：

C^d=m(mod n)使用自己的私钥,将d,c,n代入求解m,m即为明文

通过计算得到m;与原明文一样,则解密成功;



图（11） 用RSA私钥解密AES密钥（1）

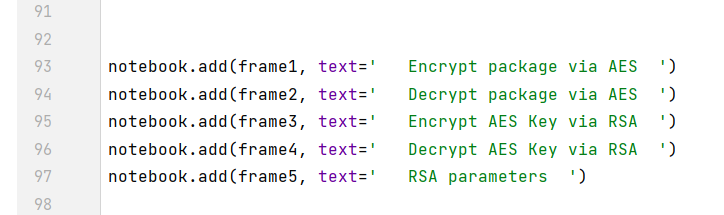


图（12） 用RSA私钥解密AES密钥（2）

至此RSA密钥的生成,加密解密的过程全部运算完毕，RSA算法实现成功;



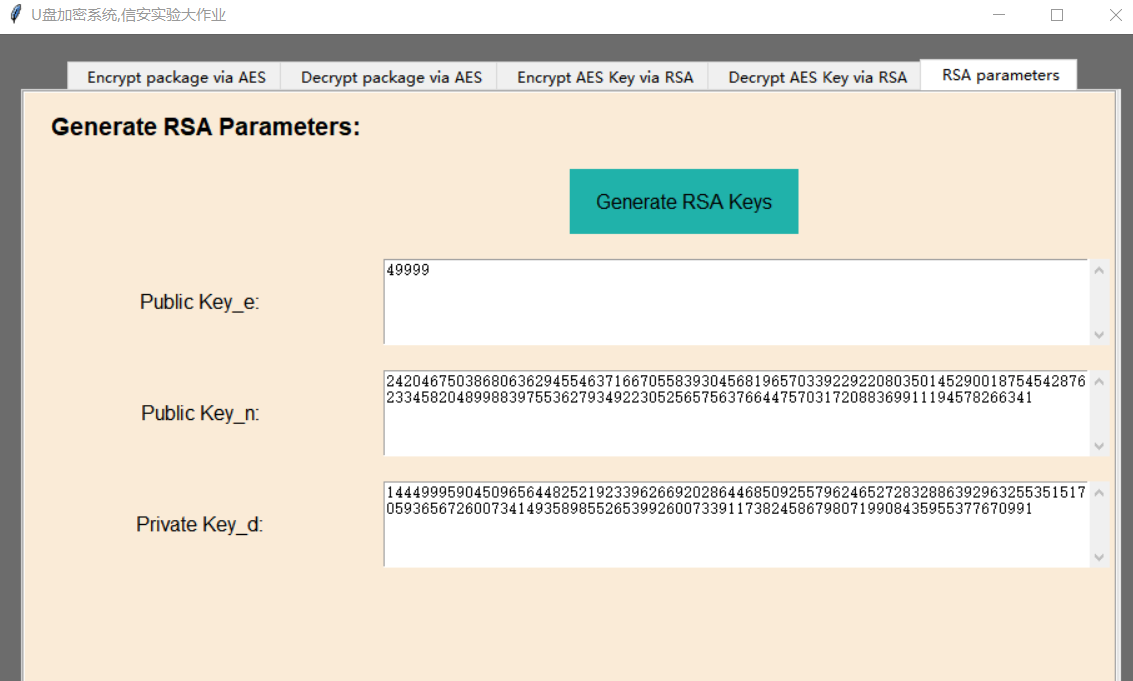
图（13） 界面搭建



图（14）界面搭建

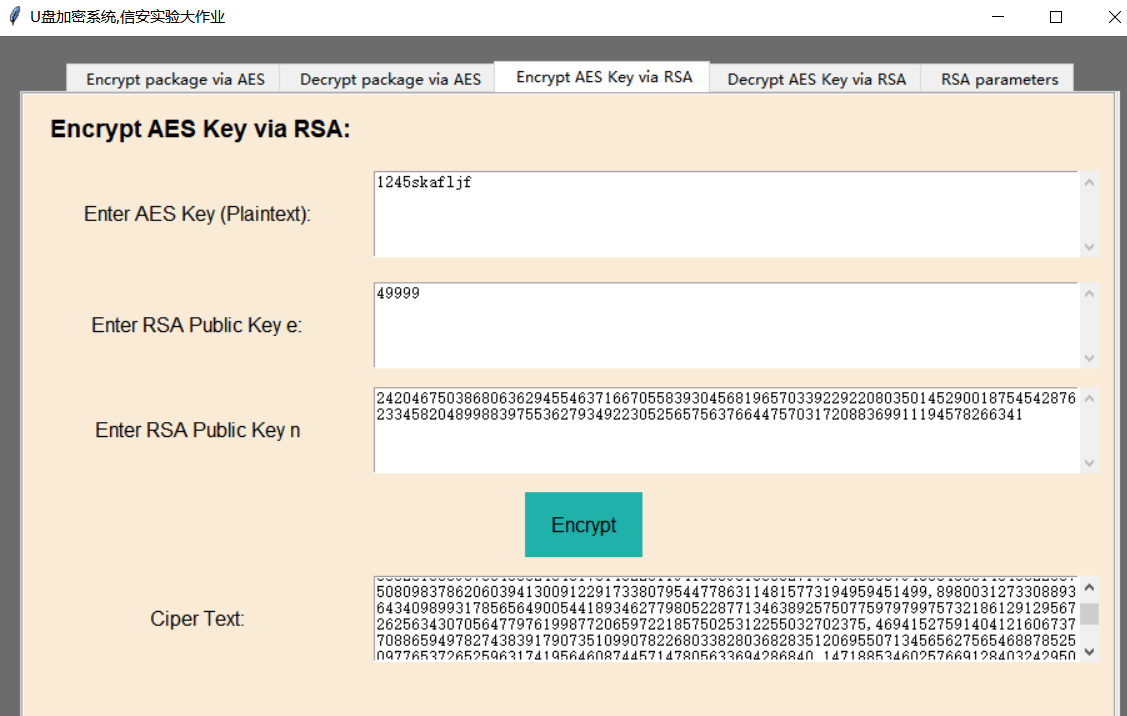
**五、软件测试及其结果分析**

我们对RSA加解密AES的密钥进行测试，首先随机生成RSA的公钥私钥



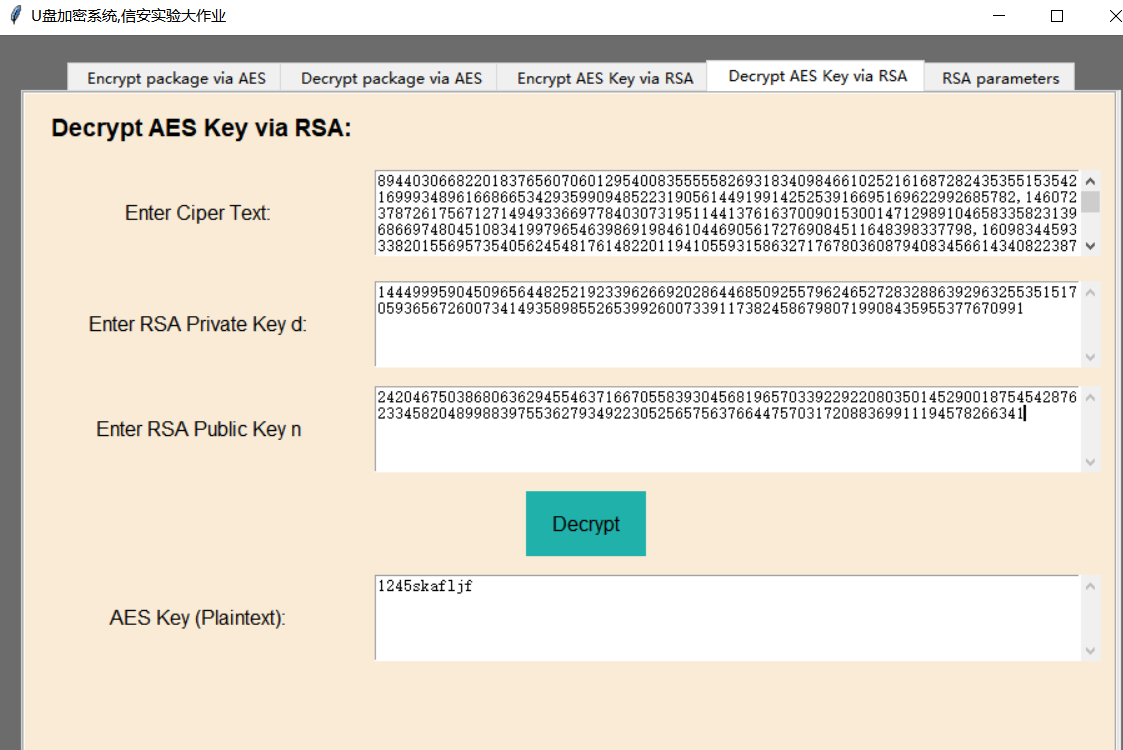
图（13） 随机生成RSA公钥私钥

然后再利用随机生成的公钥对AES密钥进行加密

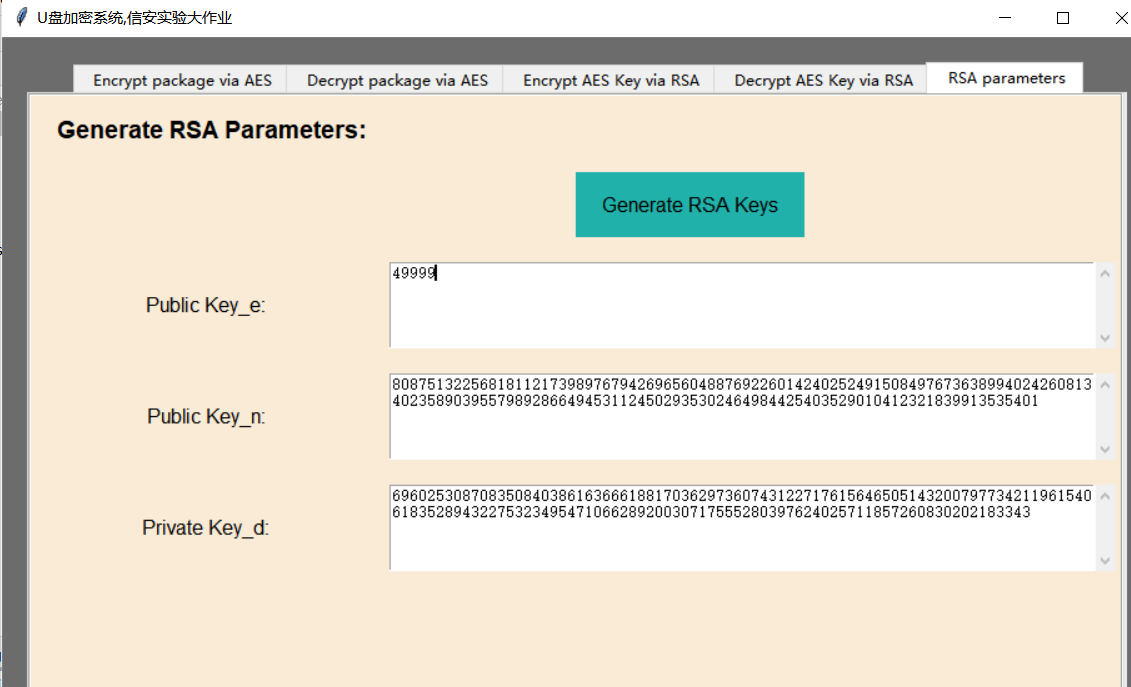


图（14） 用已生成RSA公钥加密AES密钥

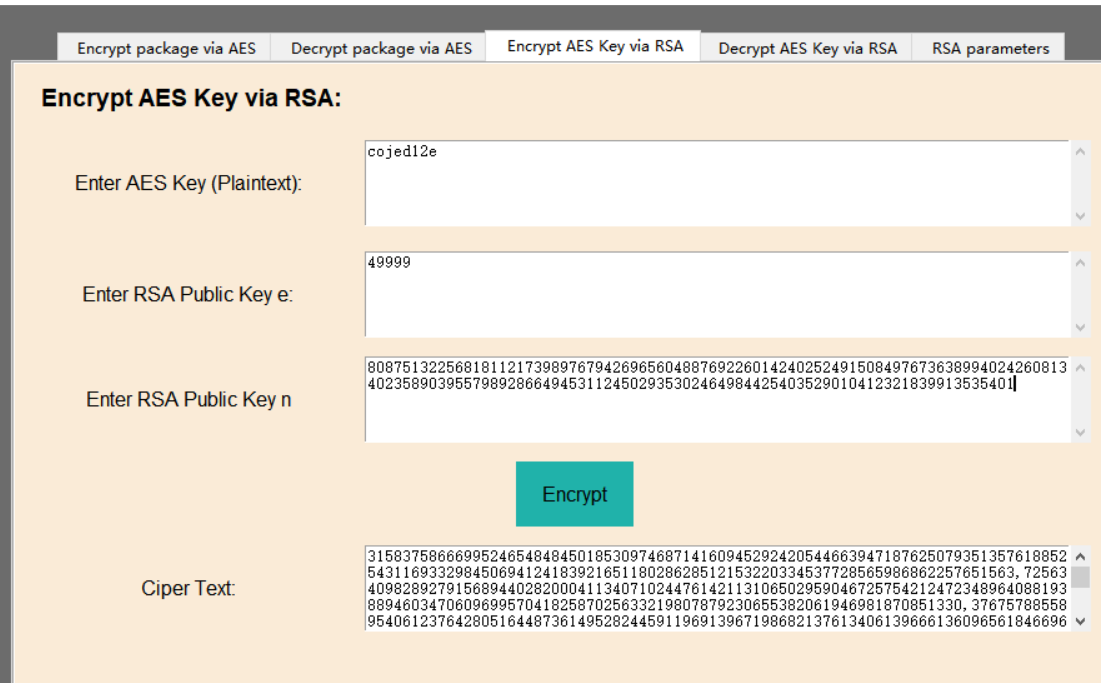
然后再对该加密后的AES密钥用私钥进行解密测试



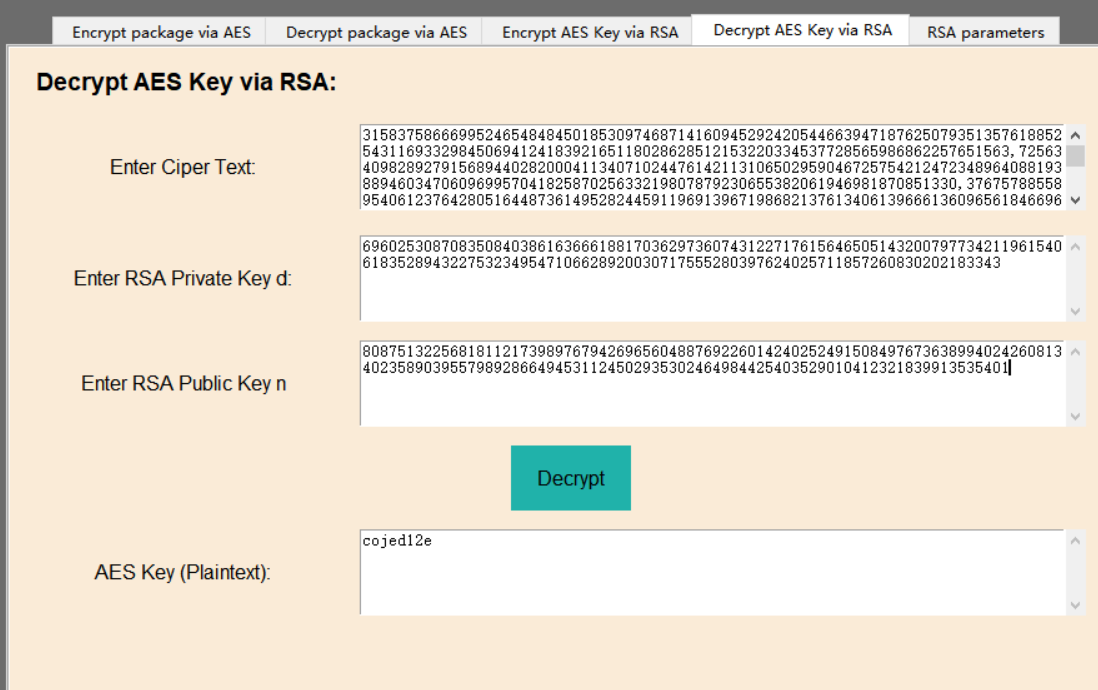
图（15） 用RSA私钥解密AES密钥



图（16）不同的公钥n和d生成测试



图（17） 不同的公钥n和d加密测试



图（17） 不同的公钥n和d解密测试

**六、课题完成过程中遇到的问题及解决方法**

问题1：在进行RSA加密测试的时候有时会出现加密异常的情况

原因及解决方法：经查找资料发现RSA[加密](https://so.csdn.net/so/search?q=%E5%8A%A0%E5%AF%86&spm=1001.2101.3001.7020" \t "https://blog.csdn.net/weixin_30635053/article/details/_blank)对明文的长度是有限制的。RSA加密明文最大长度117字节，解密要求密文最大长度为128字节，所以在加密和解密的过程中需要分块进行。如果加密数据过大则会出现错误。

问题2：分段加密解密后出现部分中文乱码

原因及解决方法：加密和解密数据都是要转成byte[] 类型的，字符串占字节为3，所以在分割字节的时候，将一个汉字分割成了两个数组的结尾和开头，这样就会出现乱码的情况。

1. **总结**

RSA+AES混合加密流程：RSA+AES的混合加密时，AES用于给传输的数据加密，然后通过RSA给AES的秘钥加密，所以接收到数据后，就需要先解密得到AES的秘钥，然后通过AES秘钥再去解密得到数据。

对称加密算法AES:AES 算法依次对每个 128 位数据块应用一系列数学变换。由于这种方法的计算要求较低，AES 可用于笔记本电脑和智能手机等消费类设备上进行数据加密，以及快速加密大量数据。AES 是一种对称算法，它使用相同的 128、192 或 256 位密钥进行加密和解密。128、192 或 256 位的密钥可以理解为分别对应16、24和32个字节的16进制字符串密钥，AES 系统的安全性会随密钥长度呈指数增长。即使使用 128 位密钥，通过对 2128 个可能的密钥值进行暴力枚举，来尝试破解 AES加密后的数据的任务也是个非常计算密集型的任务。事实上，AES 从未被破解，并且根据当前的技术趋势，预计在未来几年内仍将保持安全。

优点：（1）算法公开、计算量小、对称加密算法采用单密钥加密，在通信过程中，数据发送方将原始数据分割成固定大小的块，加密速度快，经过密钥和加密算法逐个加密后，发送给接收方，接收方收到加密后的报文后，结合密钥和解密算法解密组合后得出原始数据，解密速度快

（2）加密效率高、密钥管理简单、适宜一对一的信息加密传输，加密算法简单

（3）使用长密钥时安全性较高破解困难

缺点：（1）密钥单一安全性得不到保证

1. 密钥管理比较困难
2. 使用范围不如公钥算法

非对称加密算法RSA：RSA 以麻省理工学院的科学家（Rivest、Shamir 和 Adleman）的名字命名， 于1977 年首次公布。它是一种非对称算法，它使用公开的已知密钥进行加密，但需要另外一个不同的密钥进行解密，这个不同的密钥只有预期的接收者知道。

私钥和公钥是一对，配对使用，只不过公钥可以公布出去，而私钥是持有者自己保留的。一般的用法是私钥加密用于签名防数据被篡改，公钥加密用于加密防敏感信息，防止泄露。私钥加密公钥解密，能证明“私钥拥有者” 的唯一身份，用于签名。公钥加密私钥解密，确保发送的信息，只有"私钥拥有者"能够解密。

过程：RSA算法基于一个十分简单的数论事实：将两个大素数相乘十分容易，但那时想要对其乘积进行因式分解却极其困难，因此可以将乘积公 开作为加密密钥，可用于加密，也能用于签名

优点：（1）不需要进行密钥传递，提高了安全性

（2）可以进行数字签名认证

缺点：（1）容易遭受小指数攻击

（2）加密解密效率不高，一般只适用于处理小量数据（如：密钥）

具体流程：

（1）乙方生成两把密钥(公钥和私钥)。公钥是公开的，任何人都可以获得，私钥则是保密的。

（2）甲方获取乙方的公钥，然后用它对信息加密。

（3）乙方得到加密后的信息，用私钥解密。

由于单纯的使用 RSA（非对称加密）方式的话，效率会很低，因为非对称加密解密方式虽然很保险，但是过程复杂，需要时间长；

但是，RSA 优势在于数据传输安全，且对于几个字节的数据，加密和解密时间基本可以忽略，所以用它加密 AES 秘钥（一般16个字节）再合适不过了；

单纯的使用 AES（对称加密）方式的话，死板且不安全。这种方式使用的密钥是一个固定的密钥，客户端和服务端是一样的，一旦密钥被人获取，那么，我们所发的每一条数据都会被都对方破解；

但是，AES有个很大的优点，那就是加密解密效率很高，而我们传输正文数据时，正号需要这种加解密效率高的，所以这种方式适合用于传输量大的数据内容；

也基于以上这些优点，我们使用RSA算法加密AES密钥是十分有用的。

通过本次课程设计，我学会了综合运用信息安全、计算机技术等领域的专业技能分析问题并解决问题，同时对RSA和AES加密算法有了更进一步的了解，获得了解决信息安全领域复杂工程问题的实践创新能力。除此之外，本次课程设计加强了我们自己查找文献进行调研与资料收集的能力，提高了我们问题发现、研究、分析与解决的能力

在本次课程设计中，我们也遇到了一些困难，但我们通过小组讨论、分工合作，共同探讨商议解决方案，互相配合并各自发挥自己的长处，运用各种工程工具解决实际问题，这使我们的团队协作能力有了明显的提升。除此之外，在面对一些实验中所涉及的新知识，我们通过自学、查找资料等方式，解决了问题并完成实验，这也提高了我们自我学习与发展的能力。