**西安电子科技大学网信院**

**信息安全基础与密码学**

**综合实验**

**实 验 报 告（四）**

**ElGamal公钥密码算法**

**班级：2018039**

**姓名：叶振雷**

**学号：20009101064**

**日期：2022.11.20**

一、实验目的（包括实验环境、实现目标等等）

实验环境：pycharm+anoconda+windows11

1.通过算法编程，熟悉使用python库的基本函数操作

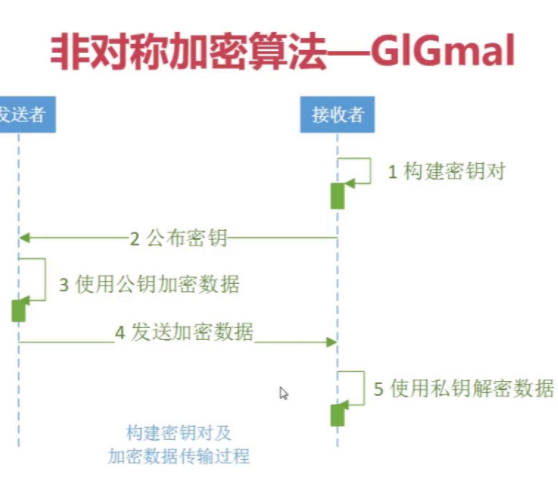
2.通过编程实现elgamal公钥密码算法，提升编程能力

3.体会密码学与数论的紧密联系,将数论的知识运用于密码学的方案设计中

4.提高逻辑思维能力与实践能力

二、方案设计

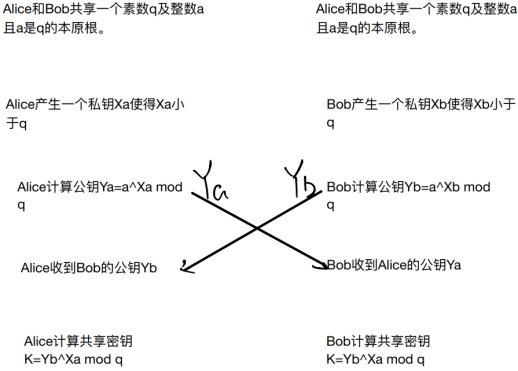
（包括背景、原理、必要的公式、图表、算法步骤等等）



ElGamal算法是由Tather ElGamal在1985年提出的，它是一种基于离散对数难题的加密体系，与RAS算法一样，既能用于数据加密，也能用于数字签名。ElGamal算法是基于因数分解，而ElGamal算法是基于离散对数问题。与RSA算法相比，ElGamal算法哪怕是使用相同的私钥，对相同的明文进行加密，每次加密后得到的签名也各不相同，有效的防止了网络中可能出现的重放攻击。

三、方案实现

（包括算法流程图、主要函数的介绍、算法实现的主要代码等等）



算法原理：

1、ElGamal密钥生成

（1）随机选择一个大素数p，且要求p-1有大素数因子。再选择一个模p的本原元α。将p和α公开。

（2）随机选择一个整数d作为密钥，2≤d≤p-2 。

（3）计算y=α^d mod p，取y为公钥。

2、ElGamal加密

（1）对于明文M加密，随机地选取一个整数k，2≤k≤p-2

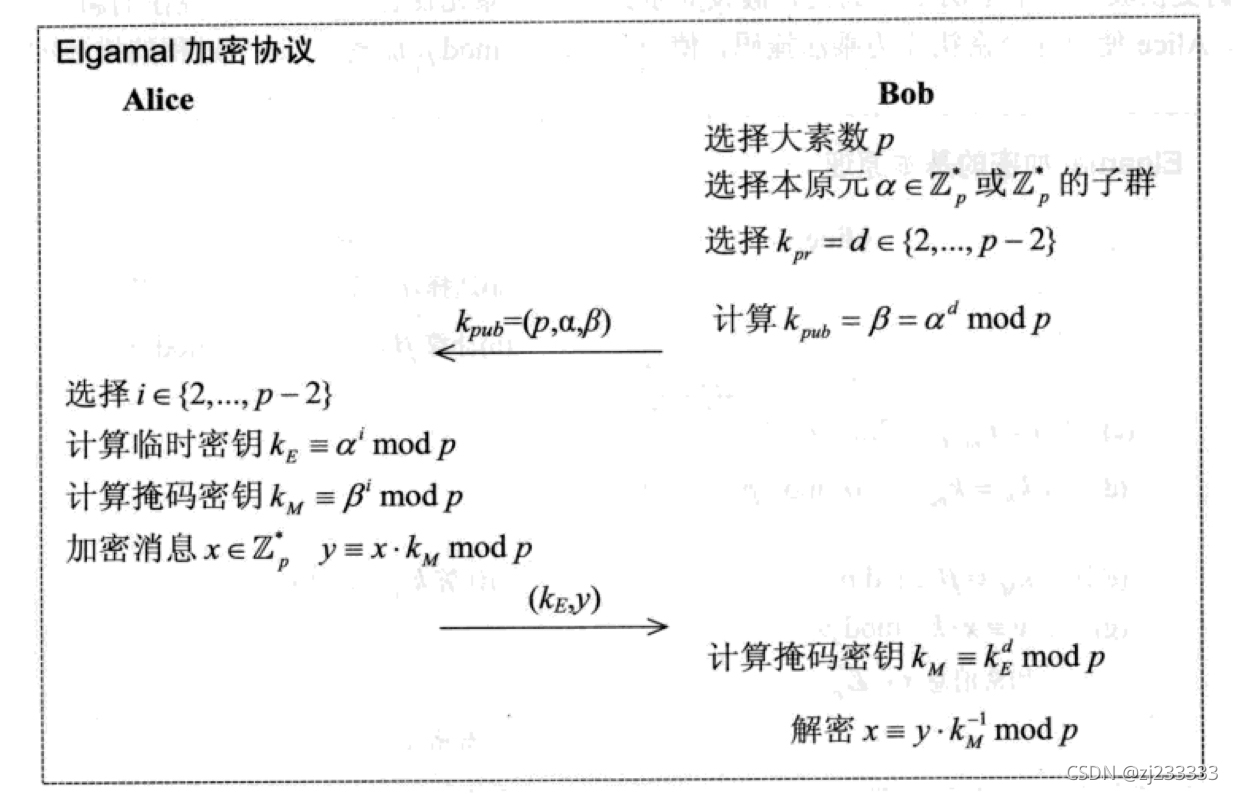
（2）C1＝α^k mod p

（3）C2＝MY^k mod p

（4）密文为（C1,C2）

3、ElGamal解密

由密文可得明文M，M=C2/C1^d mod p



主要函数介绍：

（1）large\_prime()

函数原型：large\_prime()

参数类型：int

功能：生成强素数

（2）source\_root()

函数原型：source\_root(p: int)

参数类型：int

函数功能：生成原根

（3）gen\_key\_pair()

函数原型：gen\_key\_pair()

功能：生成公钥和私钥

（4）encrypt()

函数原型：encrypt(m:int,pub\_key:tuple)

参数类型：int tuple

功能：加密

（5）decrypt

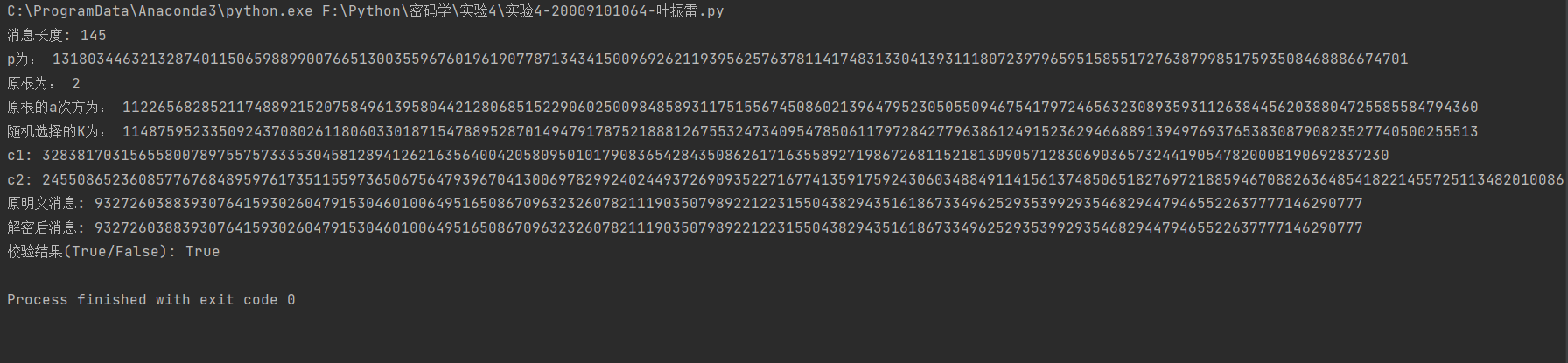
函数原型：decrypt(c:tuple,pub\_key,private\_key)

参数类型：tuple,tuple,int

功能：解密

1. 数据分析(包括算法测试数据的分析，运行结果截图等等)

选取给定文件的secret0.txt进行读取，数据为145位（10进制），我们生成的大素数有512位（2进制），满足条件，中间参数如下所示：



五、思考与总结

1. 请简述什么是本原根，给定素数P，如何求其本原根？。

本原根是数学内的一种术语。如果使得a^m≡1 mod n成立的最小正幂m满足m=φ（n）,则称a是n的本原根。 其中φ（n）为欧拉函数。

一、枚举

从2开始枚举，然后暴力判断g^(P-1) = 1 (mod P)是否当且当指数为P-1的时候成立

而由于原根一般都不大，所以可以暴力得到.

二、讲究方法

例如求任何一个质数x的任何一个原根，一般就是枚举2到x-1，并检验。有一个方便的方法就是，求出x-1所有不同的质因子p1,p2...pm，对于任何2<=a<=x-1,判定a是否为x的原根，只需要检验a^((x-1)/p1),a^((x-1)/p2),...a^((x-1)/pm)这m个数中，是否存在一个数mod x为1，若存在，a不是x的原根，否则就是x的原根。

原来的复杂度是O(P-1)，现在变成O(m)\*log（P-1）m为x-1质因子的个数。很明显质因子的个数远远小于x-1。

1. 如果𝑘与𝑝−1不互素，可能会发生什么情况？

会有机会暴露原文尤其是ak=p-1的时候

1. 实验过程中还遇到了什么问题，如何解决的？通过该实验有何收获？

在寻找大素数的过程中，一开始采用生成随机数，再用实验一中学习的素性判断其是不是素数，然后判断其是不是强素数，发现这个过程十分缓慢，程序一直运行不出结果，原因是大数中素数本身就很稀少，加上强素数的条件，可能性就更低了

解决方案：使用from Crypto.Util.number import getStrongPrime方法直接生成强素数供实验使用。通过本次实验我体会了密码学与数论的紧密联系,将数论的知识运用于密码学的方案设计中，并且提高了逻辑思维能力与实践能力。

**实验报告提交说明**：

1. 实验报告同时提交word文档与源代码（.c或者.py）。
2. 实验报告与源代码命名规则：实验4-学号-姓名，例如：实验4-20009200400-张三。
3. 请于截止日期前在西电智课平台（学在西电）提交相关文档，逾期未提交，该部分成绩记为0分，周知。