**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：2118021**

**姓名：**

**学号：**

**日期：2023年11月11日**

一、实验目的（包括实验环境、实现目标等等）

1. 实验环境

macOS Sonoma、Python 3.9

1. 实现目标

编写程序实现ElGamal公钥密码算法，能够正确生成ElGamal公钥密码算法所需的公钥与私钥，并能够正确加解密。

二、方案设计

1. 背景

ElGamal公钥密码算法是基于Diffie–Hellman密钥交换思想的一种非对称加密算法。它在1985年由塔希尔·盖莫尔提出。GnuPG和PGP等很多密码学系统中都应用到了ElGamal算法。这一算法是基于离散对数求解问题而设计。即给定指数计算对应模指数运算相对容易，而给定结果求指数相对困难。

1. 原理

对于模的原根，给定任意整数，很容易计算，但若给定整数，计算满足的整数很困难。

ElGamal公钥密码算法正是基于这一离散对数困难问题而设计的。

1. 算法步骤
   1. 秘钥产生

首先随机生成一个大素数，随机取其一个原根。随机选取整数，计算。

此时公钥即为，私钥为。

* 1. 加密

对于明文消息，若要对其加密，首先随机选取一与互素的整数，计算，。

此时密文为。

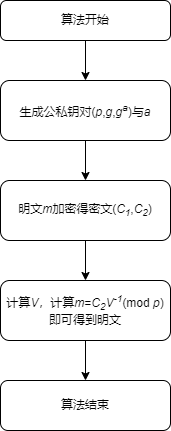
* 1. 解密

对于密文，若要对其解密，首先计算，。

此时即可得到明文。

三、方案实现

1. 算法流程图



1. 主要函数的介绍

* **generate\_strong\_prime\_num(m)**

生成大素数，传入明文判断秘钥长度

* **get\_primitive\_root(p, q)**

生成原根，传入p、q计算是否是原根

* **encrypt(p, g, y, m)**

加密算法

* **decrypt(c1, c2, p, a)**

解密算法

* **gcd(a, b)**

用欧几里得算法计算最大公因数

* **modular\_exponentiation(a, p, m)**

快速模指数运算，a^p(mod m)

1. 算法实现的主要代码

四、数据分析

1. 包括算法测试数据的分析

使用secret1.txt和secret2.txt中的数据。题目所给数据为大整数，在选取秘钥时其位数应不小于该整数位数，即能正确加解密。

1. 运行结果截图

secret1:



secret2.txt



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？。

原根：对于正整数与整数，设。若当且仅当时，则称为的原根。即若模的阶为，称为的原根。

可以遍历2至，并逐个计算其幂次从1至模的结果，若当且仅，则为原根。

1. 如果𝑘与𝑝−1不互素，可能会发生什么情况？

若𝑘与𝑝−1不互素，会导致私钥不唯一，有可能有其他的私钥能够实现解密。

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？

在编写过程中要注意细节问题，如要判断𝑘与𝑝−1互素，否则会导致不安全因素出现。

通过本次实验，我对公钥密码算法有了进一步的了解，并对ElGamal公钥密码算法的具体步骤有了更清晰的认识。