**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（三）**

**基于中国剩余定理的秘密共享方案**

**班级：2218031**

**姓名：周仙辉**

**学号：22009201377**

**日期：2024-11-04**

一、实验目的（包括实验环境、实现目标等等）

实验环境： win wsl2 ubuntu22.04

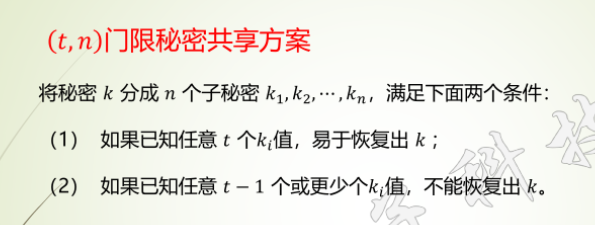
C++

实验目标：实现（t,n）门限秘密共享方案

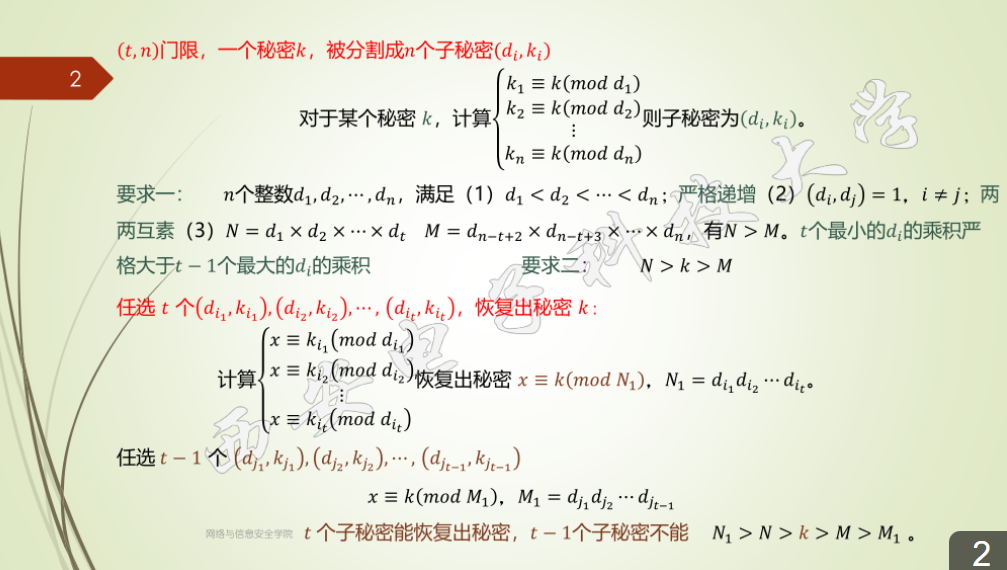
二、方案设计

（包括背景、原理、必要的公式、图表、算法步骤等等）

背景： 秘密共享

原理：

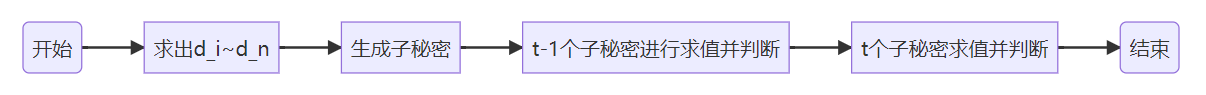
公式图表：



算法步骤：首先先求出,进而求出每对子秘密，然后随机选取t个子秘密进行验证。

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）

算法流程图：

主要函数：

pair<bool,mpz\_class> ch(vector<mpz\_class> &as,vector<mpz\_class> &ms)

通过中国剩余定理求解方程组

void get\_d(vector<mpz\_class> &d,const int n,const int tt,const mpz\_class & k,const int lenth)

求出

算法实现主要代码：

int main(){

int k = 2; // 测试文件个数

for(int i = 1; i<=k; i++){

string path{"./data/secret"};

// 输入秘密k、t、n

path += to\_string(i);

path += ".txt";

cout << "开始测试" << path << endl;

ifstream in{path};

mpz\_class k;

int t,n;

in >> k;

int lenth = k.get\_str().size();

puts("请输入t 和 n:");

cin >> t >>n;

// 获取符合要求1、2的n个d，不知怎么求，就暴力把

vector<mpz\_class> d;

get\_d(d,n,t,k,lenth);

vector<mpz\_class> son\_k;

// 求出n个子秘密

for(auto& i: d) son\_k.push\_back( k % i);

// 使用t-1个子秘密进行恢复的到faker,并与k对比

vector<mpz\_class> test1;

test1.assign(son\_k.begin(),son\_k.begin() + t - 1);

auto [flag,faker] = ch(test1,d);

cout << "使用t-1个子秘密恢复得到的值为" << faker << endl;

if(faker != k) cout << "恢复失败" << endl;

else cout << "恢复成功" << endl;

// 使用t个子密钥进行恢复并与k对比

vector<mpz\_class> test2;

test2.assign(son\_k.begin(),son\_k.begin() + t);

auto [flag1,key] = ch(test2,d);

cout << "使用t个子秘密恢复得到的值为" << key << endl;

if(key != k) cout << "恢复失败" << endl;

else cout << "恢复成功" << endl;

}

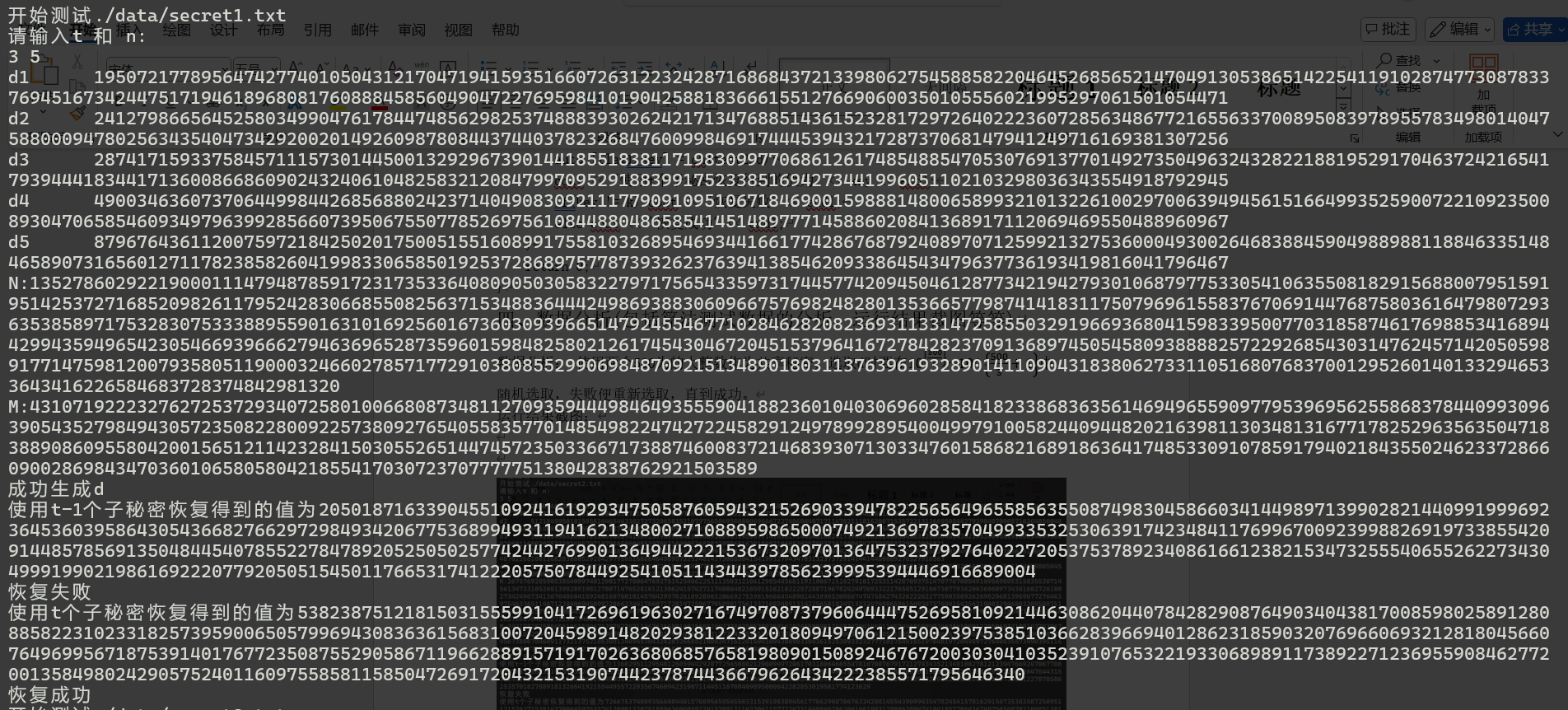
return 0;

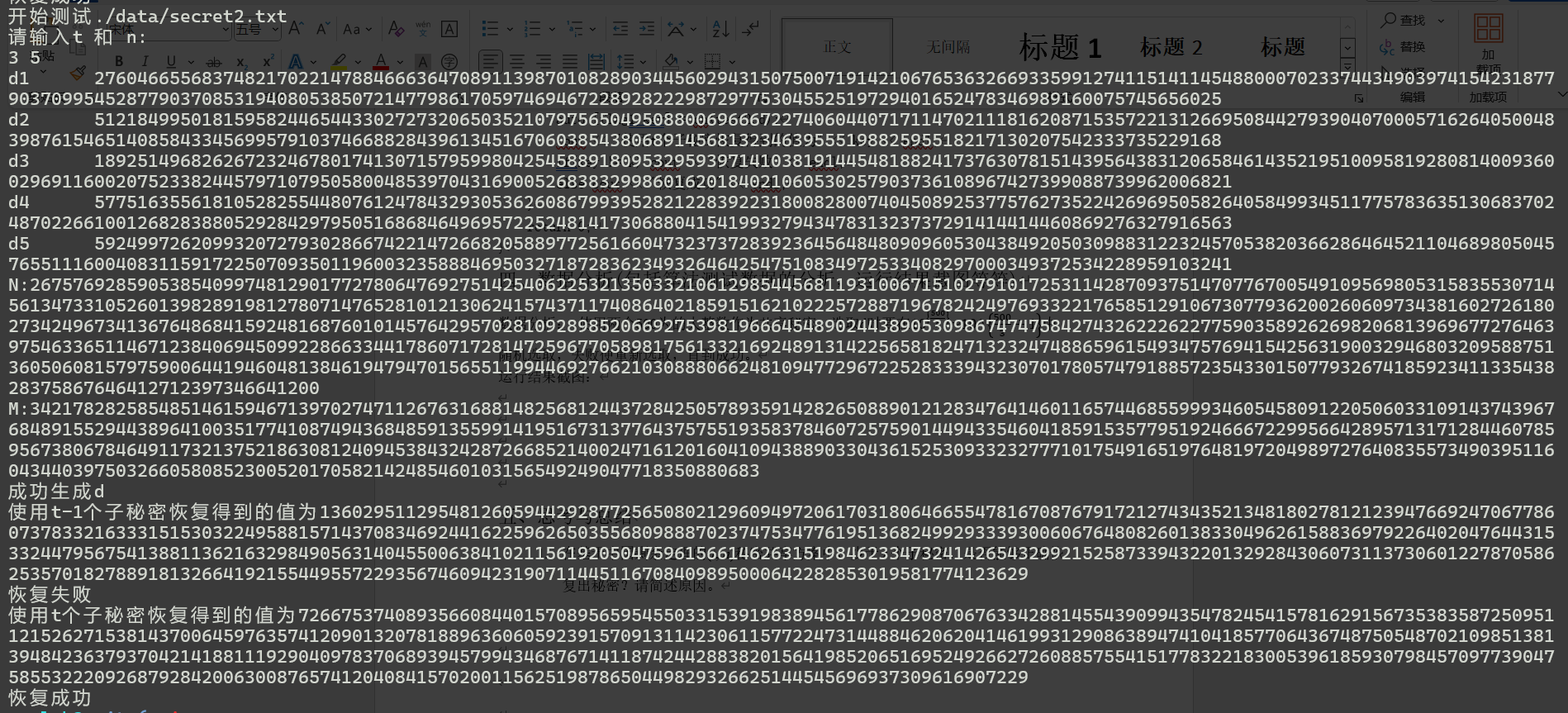
}

四、数据分析(包括算法测试数据的分析，运行结果截图等等)

数据分析： 使用两个500为的大整数作为共享秘密，选取d时要在中随机选取，失败便重新选取，直到成功。

运行结果截图：





五、思考与总结

1. 在基于中国剩余定理的(*t*, *n*)秘密共享方案中，少于*t*个子秘密，是否能够正确恢复出秘密？请简述原因。

不能，因为少于t个子秘密时，求出解的模数是 M1,小于t个子秘密的N1。N1 > N > k ,所以可以求出k。而 M1 < M < k ，求出的时候会被取模，所以求不出k。

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？

问题：求d的时候原本想用暴力破解，但难以实现

解决：将数字限定在所提供key的对应d的合适范围。

**收获：在大数问题中，暴力求解很难解决问题。**

**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3-学号-姓名，例如：实验3-20009200400-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。