**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：**

**姓名：**

**学号：**

**日期：2024-11-3**

一、实验目的（包括实验环境、实现目标等等）

Python环境

1）实验3要求实现基于中国剩余定理的（t, n）门限秘密共享方案，本次实验中t=3, n=5。具体t和n的值需要测试数据的时候输入，而不是在代码中设定好t=3,n=5；

2）子秘密的选取也是在测试数据的时候输入，不是指定的；

3）需要验证少于等于t-1个子秘密，不能正确恢复出秘密，需与原秘密对比；

4）500位左右的大整数，作为原秘密，需要如何设置di的值，需要思考；

5）需要显示出来中间数据，包括5个d值，N值，M值，以及最后恢复出的秘密，并与原秘密对比，分析是否恢复正确。

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：

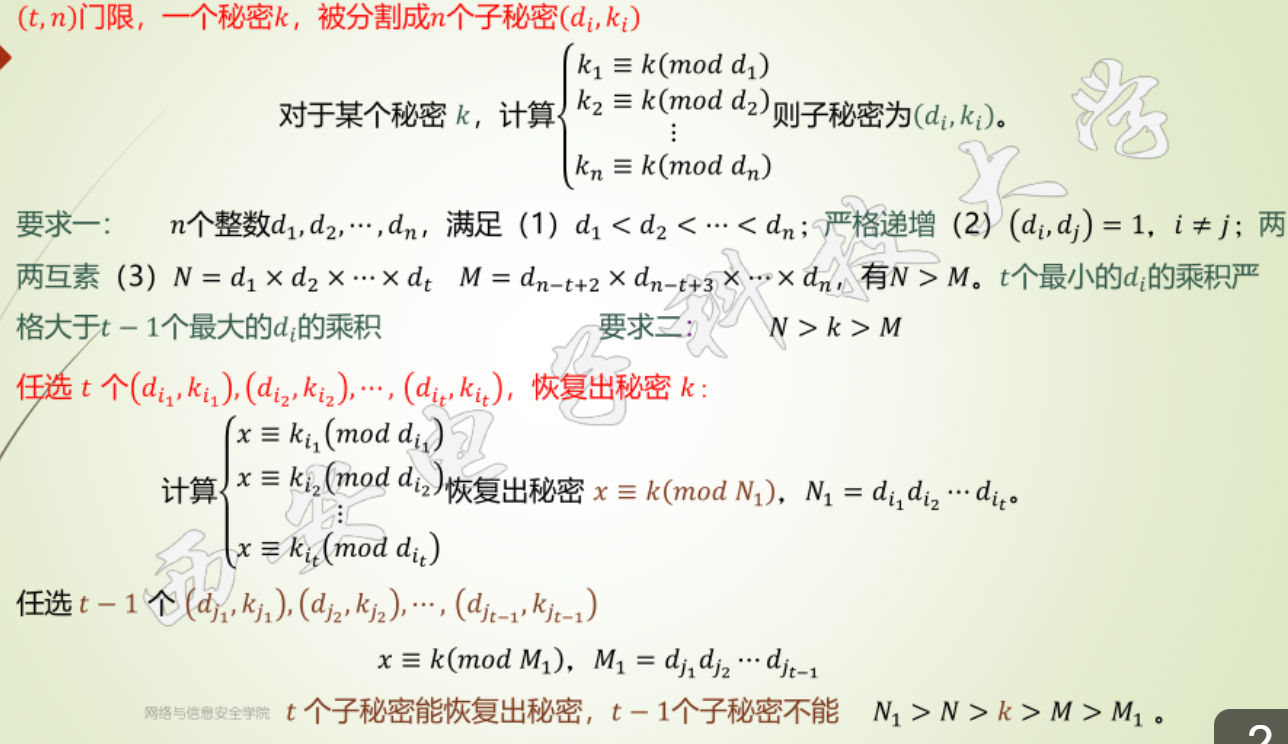
基于中国剩余定理的(t,n)门陷秘密分享方案

原理：

中国剩余定理可以求解同余方程。

基于中国剩余定理的(t,n)门陷秘密分享方案通过找到n个模数，将秘密（大整数）拆分成同余方程组，方程组有n个方程组成。这样，一个秘密分割成n份。

为了满足至少需要t个方程才能解出秘密，在选取模数时，需要保证t-1个最大的模数的乘积仍然小于k，这样，在少于t个方程时，不足以解出秘密。



算法步骤：

程序的关键在于找到一组（n个）符合要求的模数，我的算法设计如下：

Step1: 根据t, n, k ，首先计算出di合理的上、下界.

Step2: 初始化一个列表list

Step3: 生成随机数，其范围在区间(lower\_bound, upper\_bound)内

Step4：计算此随机数是否满足与list中其他数两两互素。若满足，进入下一步，若不满足，返回Step3.

Step5: 验证列表长度是否已经达到n，是，则进入下一步，否则返回Step3

Step6：根据上图的公式，计算出N,M。若满足 N > K > M,则返回list，若不满足，返回Step2, 重新寻找一组.

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）

def EEA(r0, r1) EEA算法，用于计算gcd，乘法逆元。

def generate\_coprime\_numbers(t, n, k) 找到一组（n个）符合要求的模数

def Chinese\_remainder\_theorem(a:list, m:list)实验2中已经实现，根据中国剩余定理求解方程组，给出的a，m分别代表余数、模数。

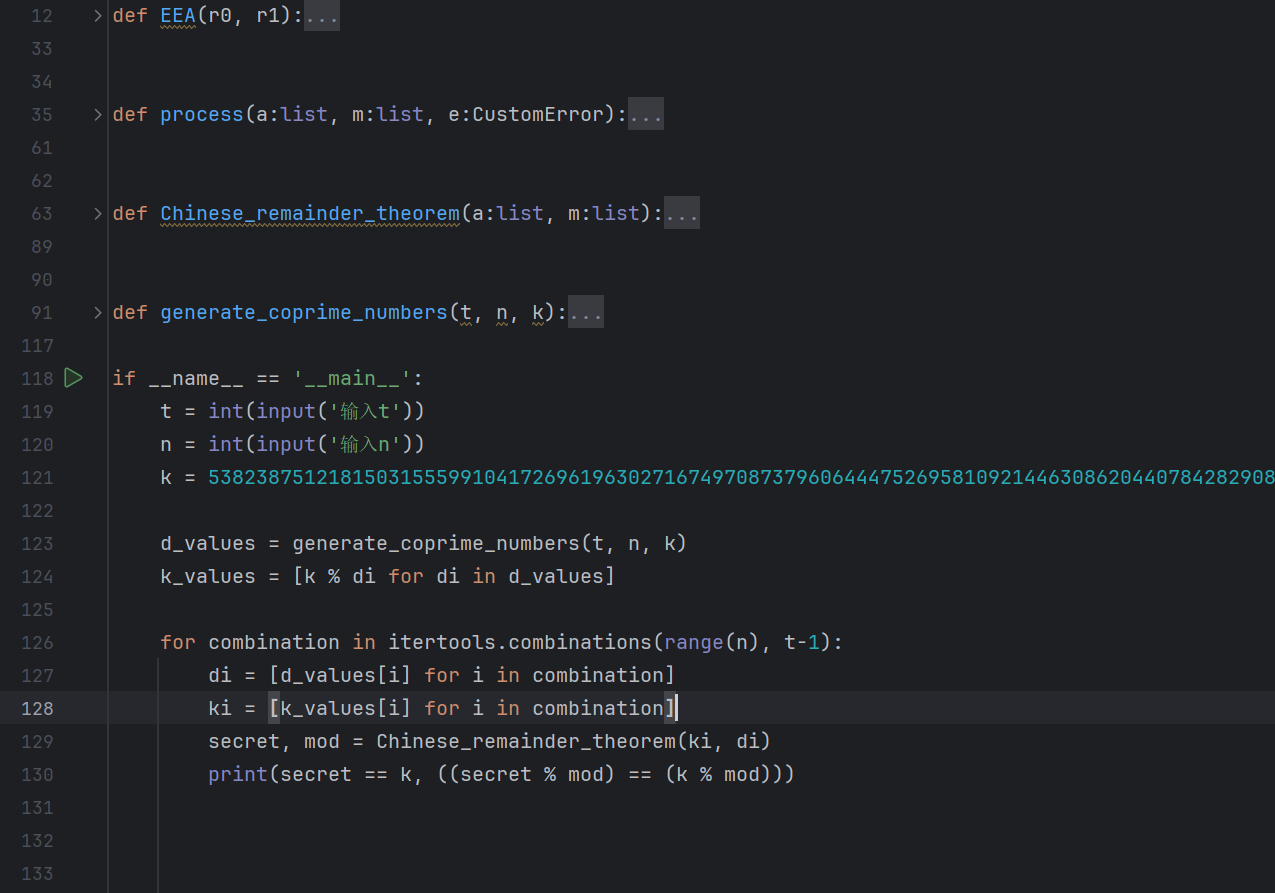
程序步骤：

Step1: 用户输入t,n

Step2: 调用generate\_coprime\_numbers，找到一组（n个）符合要求的模数。

Step3：秘密k对n个模数求余，得到同余方程组的余数。

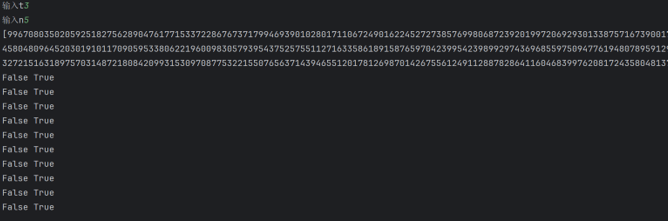
Step4: 对子秘密进行排列组合，然后调用Chinese\_remainder\_theorem，解子秘密组成的同余方程组，验证持有的子秘密数对复原结果的影响。



四、数据分析(包括算法测试数据的分析，运行结果截图等等)

选择测试数据1进行分析。

拥有t-1个子秘密的情况：



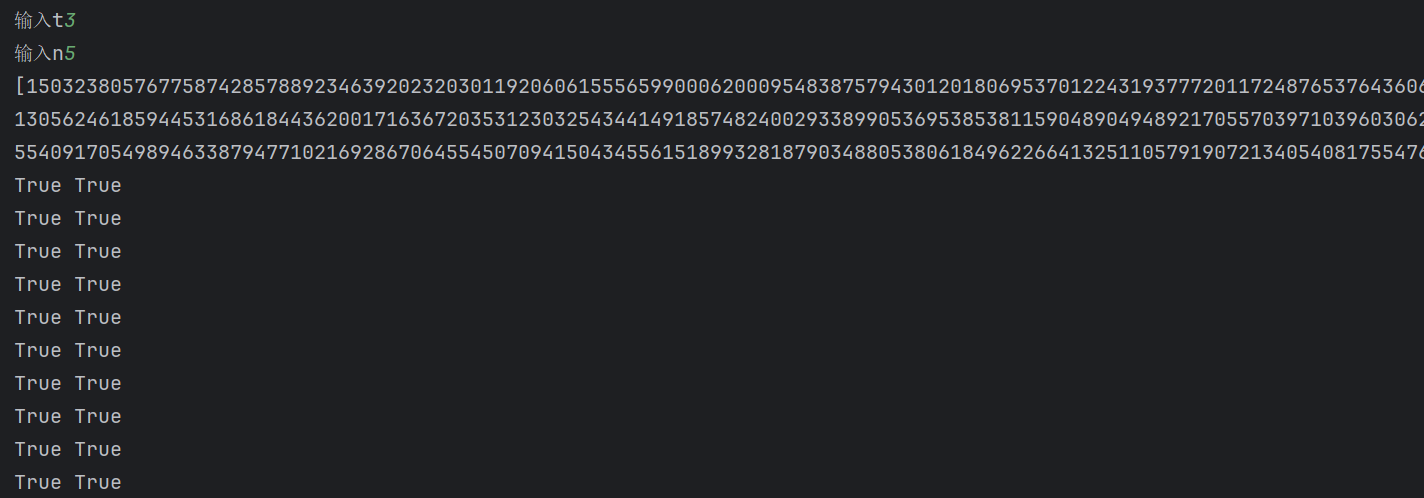
全部为False，True

通过中国剩余定理算法，解得了，并不等于秘密，无法恢复出秘密

但是，程序表明

附录中展示了控制台打印出的每个模数、N、M

拥有t个子秘密的情况：



成功还原了秘密。

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。

在我看来，既不能也能，尽管这听上去很矛盾。理论上可行，实际上不可行。

不能，原因在于任选t-1个子秘密，模数的乘积小于原秘密，因此根据中国剩余定理求解出的x是小于k的，一定不正确。

能，原因在于任选t-1个子秘密，解出，x在模n下等于原秘密，因此，t-1个子秘密可以大幅地缩小原秘密的空间。穷举，总有一个是原秘密

然而在实际操作中，面临两个问题。其一，可能缺乏有效的验证机制来确认恢复出的值是否确实为原始秘密。其二，计算上不可行。

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？

在此次实验过程中，没有遇到其他技术性问题。通过该实验和上一次实验，我收获了对基于中国剩余定理的(t, n) 秘密共享方案的深刻理解，尤其是其在理论和实践应用中的细微差别。大大提高了我的数论和代码水平。

**附录：**

**t-1个子秘密时，控制台的输出：**

**[996708035020592518275628904761771533722867673717994693901028017110672490162245272738576998068723920199720692930133875716739001750289581439456896870019430872281935338643902206759447, 1547752000998291374801955820947480685499856392823340071276151797739773663507535768204369831172004292535834209397981797761054750936652346761656677150750003791172123359735775486570421, 2969215705910578602379100489495680715332809609814419444785656398073274299485428548908343952236657288190321038765777422812879142978823593168296525869932366733059162030491372146448551, 3062158338027177012895927111552198488570473671262567506979563002030245167243910376069890382289379808914198518223735410164326888213363920382217782250150919265930580086366061414985987, 3282959018013701395811054110090076232139017053996414898232776696483332303815673224513889248512768152082048959813861111590089726976002132920684812634309347551117894445320070829307080]**

**4580480964520301910117090595338062219600983057939543752575511271633586189158765970423995423989929743696855975094776194807895912910147999112685136059913151895262169470700763049079554945878060088753975999900206466276461271374660866981542138544585332153435375527454763151512002431220187368436145991157946364058144565276367249973081960131595282238742168570367069329516051167215666069315444355137927820457949445825424847641998365888703825029607769746704521323677879168304536241851988758373845977578781785965024183171133483589404752330554058746037**

**3272151631897570314872180842099315309708775322155076563714394655120178126987014267556124911288782864116046839976208172435804813764044742703812472560427074359345306951411013170331307833994513975760452221717395862759966362912835231687153689811644057400472083410979633262407708726276950577995666743724790220047821397781029339718277476688963471475110094523253984760**

**t个子秘密时，控制台的输出**

**[150323805767758742857889234639202320301192060615556599000620009548387579430120180695370122431937772011724876537643606827671947772916908152500653603200147652978685816648302550722178, 850903899050858123899258153360008868115891842341718607997965249895851799812001187283735105927478396317455682367079352584426378434429011538473061909798676927630255499854572833625299, 1020728061548009969034056263740123702058260883884514533463398022598019335489539826034173064619381195743086585910897619740274337278774701826243257355048063050558459217030918973042883, 2048277524432635664442085882901746694604663284508237021496595058939242106340352090559479086879995973751619486176940571193841862771726655774457664460539218651991076517037975956961477, 3685987742719770985404811885376524400899699872223971401072515342152515165388098181181106860501648162413913160364277039777596071546994972012510798946009866918642305938339803212548315]**

**130562461859445316861844362001716367203531230325434414918574824002933899053695385381159048904948921705570397103960306278468192226162100203581042627363879993323745112337240079205845534649784472737164924840035226913495464954921339461407525474764096234780520954154288952505822746010159299710250948653554036591009055143080129386665313248148088896176746089204138410512920831905202119630987796769138095374448182249820274219686408776712868215186103258140537475740524204333508756924314312690229527021569525354133112777301038835452616437722560343026**

**554091705498946338794771021692867064554507094150434556151899328187903488053806184962266413251105791907213405408175547617877912747103683374542485229585566216612304395575083500000862527896318713785459255783038113333000841438824787126225231322306941454088826117980265351211596843529284299189013834300645012965093902070920716596246325435749512331667017134967030070**

**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。