离散数学课程论文（研究论文）

初等数论在密码学中的应用

清华大学

电子工程系

无 47 班

刘前

2014011216

2014 年 1 月 3 日

初等数论在密码学中的应用

清华大学电子系 无47班 刘前
2014011216 E-mail:liuqian14@mails.tsinghua.edu.cn

摘要：学习了离散数学中的初等数论，对密码学产生了浓厚的兴趣。该论文简单回顾了密码学的一些基本概念和术语之后，介绍了初等数论知识在密码学方面的应用，并且介绍了包括著名的RSA密码体制在内的诸多密码体制及其破译方法。

论文把初等数论蕴含在整个密码学的算法的阐述之中，强调初等数论的使用，体现了离散数学中初等数论对密码学发展起到的重要作用。

关键词：初等数论 密码学 古典密码体制 RSA公钥密码体制

The Application of Elementary Number Theory in Cryptography

Department of Electronic Engineering in THU Liu Qian
2014011216 E-mail:liuqian14@mails.tsinghua.edu.cn

Abstract: The paper briefly reviews some basic concepts and terms of cryptography, and introduces the application of elementary number theory in cryptography, then introduces many cryptosystems, including the famous RSA cryptosystem, and the deciphering methods.

This paper takes the elementary number theory into the whole elaborations of cryptography algorithm, emphasizing the use of elementary number theory, which also reflects the important role of discrete mathematics and elementary number theory in the development of cryptography.

Key words: Elementary number theory, cryptography, Classic cryptosystem, RSA cryptosystem

引言：

数论，顾名思义，就是研究数，特别是整数的规律和性质的数学分支，它被高斯誉为“数学中的皇冠”。在数学史上，它与平面几何学同样历史悠久。考虑到数论研究方法中难易程度的不同（发展历程的先后），数学界将数论大致分为

初等数论（古典数论）和高等数论（近代数论）。

一般来说，初等数论主要是用整数的“四则运算方法”研究整数性质的数论分支，其内容主要包括整数的整除理论、同余理论以及对素数性质的相关研究，难度不及高等数论。另外，较直白地说，初等数论也可以理解为用初等数学方法研究的数论。

随着科学技术尤其是信息科学技术的发展，我们可以看到初等数论以其特有的性质发挥着越来越重要的作用，这或许也是清华大学信息学院开设离散数学这门课程的原因。而在信息科学技术中，密码学是一支十分重要的学科，其研究意义重大。因为现代社会中，信用卡、社交软件、邮箱等均包含着用户大量的隐私，为了保护用户个人的隐私，密码成为一个有效的手段；而随着个人信息的安全越来越受到人们的重视，密码学也始终不断在发展和完善。密码学是初等数论在现实中的一个重要应用，密码学从古至今的发展与数论特别是初等数论已经密不可分，可以说初等数论是密码学的重要基石。本论文就主要研究了初等数论在密码学中的重要作用。

一、初等数论

1.基本概念

人类历史上首先认识了自然数，之后，随着生产和技术的需要，将范围扩大至整数。数论这门学科就是随整数的出现开始的，最初被称作整数论，经过进一步发展成为现在的数论。确切地来说，数论是研究数的规律，特别是整数性质的数学分支，被高斯誉为“数学中的皇冠”。初等数论主要是研究基本的整数性质（特别是一些特殊类型的正整数的性质及其关系）的数学分支。以下简要介绍了一些初等数论的基本知识，这些知识便是密码学的基础。

1.1 整除

1.1.1整除的引入

我们知道，全体整数的集合记作Z。显然，对任意a,b∈Z，有a+b,a-b,ab∈Z，说明Z关于加、减、乘是封闭的，但是存在a,b∈Z，使得a/b∉ Z，于是最先引入了整数的整除性。

1.1.2整除的定义及性质：

定义 设a,b∈Z，且≠0.若存在q∈Z，使得a=bq,则称b整除a，记作b|a,此时b叫做a的因数，a叫做b的倍数。若a，b不满足上述条件，即b不能整除a。

性质

整除有以下基本性质：

1．若a|b，a|c，则a|（mb+nc）,对任意m , n∈Z；

2．若a|b，b|c，则a|c；

3. 若a|b，c≠0，则ca|cb；

4. 若a | b，b | a，则a=b，或a= - b；
5．若a | bc，且(a , c)=1，则a | b，特别地，若质数p | bc，则必有p | b或p | c；
6．若b | a，c | a，且(b , c)=1，则bc | a。

1.1.3 若干整数整除的定理

定理① 设a，b∈Z，且b≠0，则存在唯一的q,r∈Z，使得

$$a=bq+r,\ 0\le r<|b|.$$

（定义q为用b除a得出的不完全商，称r为用b除a得到的最小非负余数，也简称为余数，常记作a mod b.）

定理② 设$b\ge 2$是给定的正整数，那么任意正整数n可以唯一表示为

$$n=r_k b^k+r_{k-1}b^{k-1}+\cdots+r_1 b+r_0,$$

此处整数$k\ge 0$，整数r_i(i=0，1，2，…，k) 满足$0\le r_i<b$，$r_k\neq 0$.

此外，整数论中最大公因数、最小公倍数、欧几里得算法（辗转相除法）、一次不定方程等均在离散数学课堂上进行了学习，由于本论文强调初等数学的“运用”，因而后续已熟悉的整除性将不再赘述！

1.2 同余

同余的概念第一次出现是在高斯的名著《算数研究》中，设m是大于1的正整数，a,b是整数，如果m｜a-b,则称a，b关于模m同余，记作a≡b(mod m),读作a同余b模m，即m除a,b余数相同则a,b关于m同余。

有关同余的性质如下：

(1) $a\equiv a(\mathrm{mod}\,m)$；（自反性）

(2)若 $a\equiv b(\mathrm{mod}\,m)$，则 $b\equiv a(\mathrm{mod}\,m)$；（对称性）

(3)若 $a\equiv b(\mathrm{mod}\,m)$，$b\equiv c(\mathrm{mod}\,m)$ ，那么 $a\equiv c(\mathrm{mod}\,m)$；（传递性）

(4)若 $a\equiv b(\mathrm{mod}\,m)$，$c\equiv d(\mathrm{mod}\,m)$，那么 $a\pm c\equiv b\pm d(\mathrm{mod}\,m)$，

$ac\equiv bd(\mathrm{mod}\,m)$；

(5)若 $a\equiv b(\mathrm{mod}\,m)$ 那么 $a^n\equiv b^n(\mathrm{mod}\,m)$ ；

(6)若 $a\equiv b(\mathrm{mod}\,m)$，$n\mid m$ 则 $a\equiv b(\mathrm{mod}\,n)$；

(7)若 $a\equiv b(\mathrm{mod}\,m_i),i=1,2\cdots n$，则 $a\equiv b(\mathrm{mod}[m_1,m_2\cdots m_n])$，其中 $[m_1,m_2\cdots m_n]$ 表示 $m_1,m_2\cdots m_n$ 的最小公倍数；

(8)**欧拉定理**：设 $a,m\in N,(a,m)=1$，则 $a^{(\varphi(m))}\equiv 1(\mathrm{mod}\,m)$ ，$\varphi(m)$ 指模m的简

系个数，$\varphi(m)=m-1$；

1.3 素数与互素

定义　若一个整数（不包括1）只有1和它本身两个因数，则这个数是素数（即质数）；若两正整数p,q的最大公因子(因数)是1，则我们称p,q互素，以$(p,q)=1$表示之。如7是素数，7与15互素，记作（7,15）=1。

自素数被发现和定义以来，一个数是否为素数的检测和判定是数论中一个十分经典的问题。而后，近代密码学的出现和兴起，给它注入了新的生命力，其中最重要的是素数的判定 ，特别是在素数的生成和分解。

目前已有的与判定素数的定理有以下若干：

①Fermat 定理（费马小定理）：此定理给出素数的必要条件 p，若不满足 ，则可断定它为素数。定理内容为，若 p 是素数 ，则对于任意的整数 a ，应有

$$a^{p-1}\equiv 1(\mathrm{mod}\ p)\text{。}$$

②素数分布定理：

设π（x）为小于或等于x的全部素数个数 ，则

$$\lim_{x\to\infty}\pi(\mathrm{x})=\frac{x}{\ln x}$$

③威尔逊定理：

p 是素数的充要条件下有：

$$(\mathrm{p}-1)!\equiv -1(\mathrm{mod\,p})$$

证明：

1.当 p=2 时显然成立；

2.当 p>2 时，p-1 为偶数

令　　$f(x)=(x-1)(x-2)\cdots(x-p+1)-(x^{p-1}-1)$

显然 f(x)的最高次数最多为 p-2

当$i=1,2,\cdots,p-1$时，(i,p)=1

故由费马小定理得

$$i^{p-1}-1\equiv 0\ (\mathrm{mod}\,p)$$

故

$$f(i)\equiv 0\ (\mathrm{mod}\,p)$$

根据拉格朗日定理，知 f(x)展开式中各项系数都为 p 的倍数

故

$$(-1)^{p-1}(p-1)!+1\equiv 0\ (\mathrm{mod}p)$$

所以，综上可证得，p 为素数时，$(\mathrm{p}-1)!\equiv -1(\mathrm{mod\,p})$。

注意：威尔逊定理直接给出了判定素数的充要条件，在判定方面有很高的理论价值。，但在寻找素数时具有很大的局限性。

二、密码学

2.1 密码学基本知识

定义　　密码学是一门研究信息的加密（encryption）与解密（decryption）技术（统称为 cryptography）以及密码破译（cryptanalysis）技术学问。

基本目的　使两个在不安全信道上通信的对象能够进行保密通信，使得即使在信道上截获了通信双方的通信内容，也没有办法理解所截获内容的准确意义。

基本概念

明文(plaintext)　　人们可以直接识别和使用的信息，例如文字、数据或声像等。

密文(ciphertext)　　将明文经过一定处理之后变换成第三方无法直接识别或使用的信息。

加密(en-cryption)　从明文到密文的变换。

解密(decryption)　从密文到明文的变换。

密钥(key)　　在明文转换为密文或将密文转换为明文的算法中输入的数据。

密码的体制　　进行明密变换的法则。

满足下述条件的五元组（P,C,K,ε,D）被称作一个密码体制:

（1）P,C,K 均是有限集，分别表示所有可能的明文，密文和密钥；

（2）$=\{e_k: P\to C|k\in K\}$ 和 $D=\{d_k=C\to P|k\in K\}$ 分别是加密法则和解密法则组成的集合。对任意密钥 $k\in K$ 和明文 x$\in P$，都有 $d_k(e_k(x))=x$。

密码学历史及现状

密码在早期仅对文字或数码进行加、脱密变换，随着通信技术的发展，对语音、图像、数据等都可实施加、脱密变换。

密码学是在编码与破译的斗争实践中逐步发展起来的，并随着先进科学技术的应用，已成为一门综合性的尖端技术科学。它与语言学、数学、电子学、声学、信息论、计算机科学等有着广泛而密切的联系。它的现实研究成果，特别是各国政府现用的密码编制及破译手段都具有高度的机密性。

2.2 几种古典密码体制及其破译

下面介绍移位密码、仿射密码、置换密码和维吉尼亚密码四种简单的对称密码体制及其破译的方法。

2.2.1 移位密码（shift cipher）

古典的移位密码（shift cipher）是以初等数论中的模运算为基础的。

出于叙述的方便，本章中将{0,1,…，m-1}记作 Z_m。

令 $P=C=K=Z_{26}$，则对任意 $K\in Z_{26}$ 以及对任意 x,y$\in Z_{26}$，定义

$$e_k(x)\equiv(x+k) \mod 26$$

$$d_k(x)\equiv(y-k) \mod 26$$

K=3 时，该移位密码体制通常被称作凯撒密码。根据移位密码的定义，可以将英文字母与 Z_{26} 中的元素建立起一一对应的关系。下表即表现了这种关系。

表 1-3　移位密码中的字母编码

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

移位密码最突出的作用就是加密普通英文词句。

2.2.2 仿射密码（affine cipher)

在熟悉了移位密码之后，将其进行推广得到了仿射密码（affine cipher)。其加密函数定义为

$$e(x)\equiv（ax+b）\mod 26,$$

其中 a,b$\in Z_{26}$。显然，当 a=1 时，仿射密码即为移位密码。

我们知道，为了能够准确的对密文进行解密，必须保证密码所用的函数是单射。数学语言表示为：

$\forall$ y$\in Z_{26}$，关于 x 的同余方程 $ax+b\equiv y(\mod 26)$,有唯一解。而

$$ax+b\equiv y(\mod 26)有唯一解\Leftrightarrow（a,26）=1$$

当（a,26）=1 时，该方程唯一解为 $x\equiv(y-b)a^{\varphi(26)-1}\equiv a^{11}(y-b) \pmod{26}$，因此相应的解密函数定义为

$$d(y)=a^{11}(y-b) \mod 26.$$

2.2.3 置换密码（permutation cipher）

置换密码的定义　将明文中的字母重新排列，改变其位置但字母本身不发生改变。

置换密码体制

令 $P=C=Z_{26}$，K 由{0,1,2,…，25}上的所有置换组成，对于每个置换 $\pi\in$K

以及 $\forall x, y \in Z_{26}$，可将加密函数定义为

$$e_\pi(x) = \pi(x)$$

及其相应的解密函数

$$d_\pi(x) = \pi^{-1}(x)$$

此处用 π^{-1} 表示 π 的逆置换。

显然，仿射密码是置换密码的特例。

置换密码的破译

密码分析者在破译置换密码时，常常利用字母和字符串的统计数据对置换密码进行破译。

其大致过程为：

①对密文的一些统计特征进行统计；

②确定大部分的密文字母；

③分析两字母或三字母等密文串；

④分析字母较多的密文。

2.2.4 维吉尼亚密码(Vigenere cipher)

维吉尼亚密码(Vigenere cipher)与之前介绍的三种密码有明显的不同，在前三种密码体制中，一旦确定了密钥，则每个明文字母在该密钥下对应的密文字母在密文中将保持不变（将这种密码体制称作单表密码体制）。而维吉尼亚密码与此不同，在维吉尼亚密码中，明文中不同位置的同一明文字母在密文中对应的密文字母不同，则称其为多表密码体制。

下面介绍维吉尼亚密码体制：

设 m 是一个正整数，令 P=C=K=$(Z_{26})^m$。对于每个密钥 K=（k_1，k_2，…，k_m）

以及任意（x_1，x_2，…，x_m），（y_1，y_2，…，y_m）$\in (Z_{26})^m$，定义加密函数

$$e_k（x_1，x_2，…，x_m）=（x_1+k_1，x_2+k_2，…，x_m+k_m）$$

以及相应的解密函数

$$d_k（y_1，y_2，…，y_m）=（y_1-k_1，y_2-k_2，…，y_m-k_m）$$

注意 此处所有的加减运算都是 mod 26 的运算。

2.3 RSA 密码体制

2.3.1 公开密钥

公开密钥算法是美国斯坦福大学的迪菲（Diffie）和赫尔曼(Hellman)两

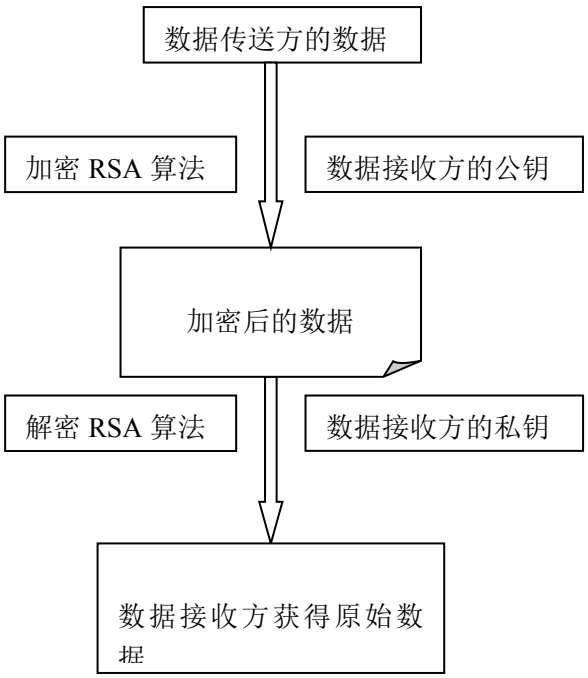
人首先发明的（ 论文“New Direction in Cryptography”）。但目前最流行的RSA是1977年由MIT教授Ronald L.Rivest,Adi Shamir和Leonard M.Adleman共同开发的，分别取自三名数学家的名字的第一个字母来构成的。

公钥 RSA 加密算法的基本思想（朱萍.《初等数论及其在信息科学中的应用》）：

公钥加密算法中使用最广的是RSA。RSA使用两个密钥，一个公共密钥，一个专用密钥。用公钥加密后，发送给私钥持有者，即使被拦截或窃取，没有私钥的攻击者也无法获得加密后的信息，可以保证信息的安全传输 另外，先用私钥加密，再用公钥解密，可以完成对私钥持有者的身份认证，因为公钥只能解开有私钥加密后的信息。 虽然公钥和私钥是一对互相关联的密钥，但是并不能从两者中的任何一把，推断出另一把。

以下是一个简单的示意图，帮助理解基于RSA算法的数据传输（加密与解密）过程。

基于 RSA 算法的数据传输过程



RSA密码体制易于理解和操作。RSA从提出到现在的三十多年里，经历了各种攻击的考验，逐渐被接受，并被普遍认为是目前最优秀的公钥方案之一。

*2.3.2 公钥与密钥的产生

假设A给B传送一个消息 m，A可以用以下的方式来产生一个**公钥**和一个**私钥**：

（1）由欧拉函数可得，不大于 N 且与 N 互质的整数个数为 $(p-1)(q-1)$

（2）选择一个整数 d 与 $(p-1)(q-1)$ 互质，并且 e 小于 $(p-1)(q-1)$

（3）用公式计算 $e:(d*e)\equiv 1(\mathrm{mod}((p-1)(q-1)))$

（4）将 p 和 q 的记录销毁（重要）。

(N,e) 是公钥，(N,d) 是私钥。(N,d) 是秘密的。A 将公钥 (N,e) 传给 B，而将私钥 (N,d) 藏起来。

2.3.3 加密消息

B 使用起先与 A 约好的格式将 m 转换为一个小于 N 的整数 n，因为 B 知道产生的 N 和 e。比如可以将每一个字转换为 Unicode 码，再将数字连在一起组成一个数字。假如信息非常长的话，他可以将这个信息分为几段，然后将每一段转换为 n。

用下面这个公式他可以将 n 加密为 c：

$$n^e \equiv c(\mathrm{mod}\, N)。$$

2.3.4 解密消息

A 得到 B 的消息 c 后就可以利用密钥 d 来解码。

以下这个公式来将 c 转换为 n：

$$c^d \equiv n(\mathrm{mod}\, N)。$$

得到n后，他可以将原来的信息m复原。

解码是根据

$$c^d \equiv n^{e-d}(\mathrm{mod}\, N)$$

以及

$$e*d \equiv 1(\mathrm{mod}(p-1)) 和 e*d \equiv 1(\mathrm{mod}(q-1))。$$

由费马小定理可证明（因为p和q是质数）

$$n^{e-d} \equiv n(\mathrm{mod}\, p) 和 n^{e-d} \equiv n(\mathrm{mod}\, q)。$$

这说明（因为p和q是不同的质数，所以p和q互质）

$$n^{e-d} \equiv n(\mathrm{mod}\, pq)。$$

2.3.5 安全性

假设加密信息被偷听，但偷听者无法直接获得甲的密钥d。而要获得d，最简单的方法是将N分解为p和q，这样可以得到同余方程

$$(d*e)\equiv 1(\mathrm{mod}((p-1)(q-1)))$$

解出d之后，代回解密公式

$$c^{d}\equiv n^{e-d}(\mathrm{mod}\,N)$$

解出n（破密）。

弊端和缺陷

至今为止还没有人找到一个多项式的算法来分解一个大的整数的因子，同时也还没有人能够证明这种算法不存在，因而目前该问题悬而未决。

但根据彼得·秀尔（Peter Shor）在1994年的证明，假如量子计算机有朝一日可以成为一种可行的技术，那么彼得·秀尔的算法可能够淘汰RSA和相关的衍生算法。

总之，如果有人最终找到一种分解大整数的有效的算法的话，亦或是量子计算机最终得以实现，在解密和制造更长的钥匙之将会展开一场更为激烈的竞争。但从原理上来说RSA在这种情况下是不可靠的。

2.3.6 RSA 前景

由RSA的算法及其密码体制，我们可以看出，RSA加密在未来很长一段时间内仍然是市场的主宰，除非有朝一日量子计算机真正问世；然而RSA本身由于需求的位数越来越高，对计算机的要求也会越高。

同时，我们要从长远考虑，以发展的眼光看待密码学，站在科技发展史的角度，RSA终将被新的更高级的算法所替代，而且新加密方法的破译也会越来越难，加密与破译的博弈也将永远持续下去。

结束语

经过一学期离散数学课程的学习，已对离散数学尤其是数论有了较为深入的了解，并且偶然间对密码学产生了兴趣，因而各处搜集、整理资料，重点探究了初等数论在密码学方面的重要运用。

我们知道，凡是理论最终都是要付诸于实际应用之中的，离散数学、数论也是如此，于是论文集中介绍展示了初等数论在密码学中的重要地位。

尽管上述密码体制建立在较为简单的初等数论之上，公式推导也不是很繁琐，但这并不表示本论文比较简单，因为密码学重要程度远远大于其理论上表现出来的难度。而且，密码学中仍然存在许多难以解决的问题，尤其集中在密码的破译中。如，基于大整数因子分解问题（Integer Factorization Problem）的公钥密码体制、基于有限域上离散对数问题（Discrete Logarithm Problem）的公钥密码体制、 基于椭圆曲线离散对数问题（Elliptic Curve Discrete Logarithm Problem）公钥密码体系等等都未彻底解决，还需要一代代的数学工作者来完成。

由此可见，数论作为密码学的基础学科之一，在密码学中的应用十分普遍，

并且未来密码学的发展仍将牢固建立在数论这一理论基础之上。

【参考文献】

[1] 朱萍. 《初等数论及其在信息科学中的应用》[M]. 北京：清华大学出版社.2010：1-85.
[2] 陈鲁生.沈世益. 现代密码学[M]. 北京：北京科技出版社. 2002:200-300.
[3] 吴晓刚. 数论在密码学中的应用与算法的优化实现. 贵州：兴义民族师范学院学报. 2010年10月第3期》.