公键密码的由来
陷阱系数
密码签名

# 公键密碼

# PUBLIC KEY CRYPTOSYSTEM

黄光明　R. L. 葛立恒

## 一　简介

把普通的文字经过一种有规则的变换而得到的新的文字就叫做码（code）。譬如说我们把英文字中所有字母都用它后一个字母来代替（z以a代替），则可得到下一行的码：

UIJT　JT　B　TJMMZ　DPEF

我们也可规定在一句中文中要除掉所有占着质数位置的字才得到隐藏着的一句话：

这里有是非一定个笨方向法国。

由于现代化的通讯设备必须把文字转换成数字（这种数字就是一种码）才能传送，码的研究遂很重要。码的设计通常有两种目的：一是保护不受天然的损害，像“纠错码”（error correcting code）可以纠正传送时发生的误失；另一是保护不被人为的偷听，即所谓“密码”（crypt），其目的在于使偷听的人听不懂。本文讨论的对象是密码。要达到使用密码的目的，则变换规则必须设计得相当精巧，使得局外人不容易摸索出来。上面举例中用的方法，明眼人一猜即透，当然不足为训。另外一点是变换规则必须确实地保密，只有收发双方知道。密码的被破译往往是出毛病在这第二点上。因为一套密码如果使用的时间过久则机密一点一滴外泄，迟早被摸清底细；但如果经常更换，则如何把新的变换规则安全地送到受者手里，便是一个大问题，因为如果真有这样一条安全通道可以经常传送信息的话，则又何必要用密码多费一道事呢？

在计算机普及以前，密码的设计和应用几乎是政府的专利品，但是在今天的美国，全国的计算机网络已逐步建造起来，计算机之间以惊人的速度大量地交换着信息，这些信息经过电话线，经过微波塔、经过人造卫星充塞在我们周围，以极简单的设备，谁都可以收听，谁都可以放送。我们究竟如何知道，我们发出的信息没有被第三者窃听？我们收到的信息不是第三者的伪造？因此密码在信息传递上的应用就不但是呼之欲出而且是急不可待了。

但是密码在工商界的应用和在政府机构间的应用有一点不同的地方，即一个工商用户交换信息的对象可能是很广泛的社会面，就像一个商店把它的电话号码以特大号字登在电话簿上一样，它希望越多的顾客和它联络越好，但很显然用户不可能事先把其信息变换规则分发到每一个可能的顾客手里。同时用户也不愿意这样做，因为它和某一个顾客的秘密通讯就会被所有其它顾客知道了。1976年狄非（Diffie）和黑门（Hellman）首先提出一种密码的构想，兼有网络公开和信息保密的好处，称为“公键密码制”（public key cryptosystem）。一套文字和密码间的变换规则可以分成把文字编成码和把码译回文字两部分，当然这只是一物的两面，在通常情形下有密切的联系。“键”是指一个编码方法的代号。譬如我们把有可能的编码法都指定一个代号，然后编一本代号簿的索引，登载了哪一个用户用哪一个代号的编码法，谁要和这个用户通信，就查出它的代号，把信息按照代号的规定编成密码传递。由于编码法是公开的，所以叫做“公键”。

但既然每个人都能查代号，别人收到了这密码是否可立即知道传递的信息呢？如果答案是肯定的话，当然这一套制度就不值一提了。关键在于编码法要有一种特殊的性质，称为“陷阱”（trap door）性质，即知道了编码法只能编码而不能译码（叫做陷阱是取其只能进不能出的意思）。要想译码还得知道译码的规则。而此译码法则是用户的独家机密，不泄於众。我们

黄光明（Frank K. Hwang）　贝尔实验室离散数学室研究员。
葛立恒（R. L. Graham）　贝尔实验室离散数学室主任。

可以想像某一位张三先生得到了世界上独一无二的蝌蚪文——中文字典，他把中文译成蝌蚪文的部分公之於众，所以每个人要和他通信都可以把中文译成蝌蚪文登在报纸上，成千上万的读者看到了却仍不知是什么信息，只有这位张三先生可以用他的字典中蝌蚪文译成中文的部分来看懂这个信息。这个譬喻唯一不恰当的地方是如果我们有一本把中文译成蝌蚪文的字典，则投资下足够的人力、时间后，我们可以编出一本蝌蚪文译成中文的字典。而狄非一黑门倡议用的编码法，必须是在实际情形下不可能从编码法来猜出译码法者。是否有这样的编码法呢？在下一节中我们介绍几种数学家想出的答案。

## 二　陷阱（trap-door）函数

所有的文字都可以用数字来表示，譬如以“1”代表a，“2”代表b，“3”代表C等。中文没有字母，比较不容易直接用数字代表，一个死方法是如果有十万个中文字，就用十万个数字来分别代表。（目前中文电报码就是用这一个方法）。其它的方法有用拼音来代替文字，则每一个的拼音符号都可以用数字表示；或以数字来代表点、竖、横、撇等基本笔划，把一个字分成几部分的特点以数字表出，如王云五四角号码等。所以我们可以假设原来的文字已是数字的形式，编码则是把一组数字换成另一组数字，所以编码法可以用一个函数来表示。下面我们介绍几种有陷阱性质的编码法。。

**李夏艾（Rivest-Shamir-Adleman）法**

用户选定两个很大的质数p和q，令$n=pq$；再随意选定一个大於p和q，但小於且互质於$\phi(n)=(p-1)(q-1)$的整数d［$\phi(n)$通常叫做欧勒（EULER）数，代表所有小於n且互质於n的整数数目］，用欧几里德算法可以算出d按$\phi(n)$模（modulo）乘法的逆元素（inverse）e，即

$$e\cdot d=1\ [\mathrm{mod}\ \phi(n)]$$

［$x=y\ (\mathrm{mod}\ z)$的意义是x被z除后余数（residue）为y］，此时e也是一个小於$\phi(n)$的正整数。

用户现在公布它的编码法如下：顾客首先把信息分段，每段所代表的数字不得大於n（若大於n则分成更小的段）。设M为某一段的信息，则通信者按照用户公布的n，e两数将M编成暗码

$$E(M)=M^e\ (\mathrm{mod}\ n)$$

设C为密码，则用户的译码法是

$$D(C)=C^d\ (\mathrm{mod}\ n)$$

所以当他收到E(M)时，按照译码法得到

$$D[E(M)]=(M^e)^d=M^{ed}=M\ (\mathrm{mod}\ n)$$

［$M^{ed}=M$是引用费马欧勒定理$X^{\phi(n)}=X\ (\mathrm{mod}\ X)$］

但是第三者收到了E(M)，因为不知道d，却无法译回成M。假定能把n分解成p和q，则可以算出$\phi(n)$，再从$\phi(n)$和e用欧几里得算法算出d。但到现在为止，还没有多项式算法来做因子分解问题。虽然因子分解问题还没有被证明是NP-complete问题，但一般相信其复杂性接近於后者（请参阅笔者“线性规划”的计算复杂性一文）。

**牟黑（Merkle-Hellman）法**

用户选定一组数字$\hat{a}_1, \hat{a}_2, \cdots\cdots \hat{a}_n$，m，w有下列的性质：

1. $\sum_{i=1}^{j-1}\hat{a}_i<\hat{a}_j,\quad j=2,3,\cdots\cdots n$

2. $\sum_{i=1}^{n}\hat{a}_i<m$

3. $w<m$，且w的mod m其乘法的逆元素$w^{-1}$存在。

用下列的公式把$\hat{a}_j$换算成$a_j$：

$$a_j=w\hat{a}_j\ (\mathrm{mod}\ m),\quad j=1,2,\cdots\cdots n$$

且公布$a_1, a_2, \cdots\cdots a_n$这组数字。假设顾客的信息都以二进数的向量来表示，即信息M可写成（$b_1, b_2, \cdots\cdots b_n$），$b_j=0$或1。则顾客的编码法是

$$E(M)=\sum_{j=1}^{n}a_j b_j$$

设C为密码，则用户的译码法为先算出$\hat{C}=w^{-1}c\ (\mathrm{mod}\ m)$，当$C=E(M)$时，$\hat{C}=w^{-1}\sum_{j=1}^{n}a_j b_j=\sum_{j=1}^{n}w^{-1}a_j b_j=\sum_{j=1}^{n}\hat{a}_j b_j$。然后$b_1, b_2, \cdots\cdots b_n$可从$\hat{a}_j$的特殊性质解出。设$\hat{a}_i$是所有不大於$\hat{c}$的$\hat{a}_j$中最大的一个，则令$b_i=1$。再用$\hat{c}-\hat{a}_i$代替$\hat{c}$来循环得到所有值为1的$b_j$。读者可以假设$\hat{a}_i=2^{j-1}$法来试验一下。

当第三者收到E(M)时却因不知道w而不能算出$\hat{C}$，当然也无法利用$\hat{a}_j$来解$b_j$。如果想要从

$$E(M)=\sum_{j=1}^{n}a_j b_j$$

来直接解$b_j$时，则因$a_j$并没有特殊性质可利用，这问题就变成了所谓的背包（knapsack）问题，是已知属於NP-complete类的难题。如果把w和m的换算多运用几次，当然更增加了暗码的安全性。

葛、夏(Graham-Shamir)两氏建议在信息（$b_1, b_2, \cdots\cdots b_n$）的前后再加上一些和信息无关的数字作疑兵以进一步保护暗码，略微要注意的是紧接着$b_n$后的几位数字要稍加安排以保证它们的进位不影响$b_n$，这样（$b_1, b_2, \cdots\cdots b_n$）的运算和前后附加的疑兵无关，用户在译码后削头去尾就得到了原来的信息。

**麦（McEliece）氏法**

这个方法的基础在於一般的“线性纠错码”。其译码是一个NP-complete的难题。但也有些有特殊性质的码，如哥帕（Goppa）码，译码却很简单。设$\hat{G}$代表哥帕码的$k\times n$生成矩阵（即所有哥帕码都可写成$A\hat{G}$，A是一个含n个二进数的向量），用户任意选一个$k\times k$非奇异（nonsingular）矩阵S，再任意选一个$n\times n$的排列（permutation）矩阵p（这两个矩阵的元素都是二进数），令$G=S\hat{G}P$。设顾客的

信息是一个长度为n的二进数向量M，编码的方法是

$$E(M)=MG+Z$$

此处Z是一个n元素中有t元素其值为一的随机向量。用户收到E(M)后，即计算

$$\hat{C}=E(M)P^{-1}=MGP^{-1}+ZP^{-1}$$
$$=MS\hat{G}+ZP^{-1}$$

因此$\hat{C}$是一个哥帕码。用Patterson算法可以将码$\hat{C}$译成$\hat{M}=MS$，再乘以$S^{-1}$，即得原信息M。当第三者收到E(M)时却因不知$P^{-1}$和$S^{-1}$而无法如上进行。但是直接从E(M)译成M则如前述是一个NP-complete难题。

## 三　密码签名

当一种码的编码和译码方法可以互换时，狄非和黑门二氏设计出下述的一套公键密码签名法：设$E_i$、$D_i$分别为用户i的编码译码函数。如A要将信息M传送给B，且要B确知M是A所发，则A首先算出$S=D_A(M)$，再用B公布的编码法得到$D_B(C)=S$，再用A公布的编码法算出$E_A(S)=M$。当B译出M时，可推知S一定是$D_A(M)$。但除A外无人知道$D_A$这一译码函数，故M一定是A所发。

我们现在来检查一下在上一节所介绍的三个方法中，哪些有编码译码互换性质。设$M=(b_1, b_2, \cdots\cdots b_n)$是要传递的信息。

1. 用李夏艾法时，用户将M编成$D(M)=M^d \pmod n$，顾客收到后可译回得$E(M^d)=(M^d)^e=M^{\phi(n)+1}=M \pmod n$。

2. 用牟黑法时，用户将M编成$D(M)=\sum w^{-1}M$。顾客译码时得$E(\sum w^{-1}M)=\sum_{i=1}^{n} w^{-1}a_i b_i=\sum_{i=1}^{n}\hat{a}_i b_i$。但顾客不知道$\hat{a}_i$之值，故不能获知$b_i$。

3. 用麦氏法，用户将M编成$D(M)=MP^{-1}$。顾客译码时得$E(MP^{-1})=MP^{-1}G+Z=MP^{-1}S\hat{G}P+Z$，也不能复原成M。故三法中只有李夏艾法可用来签名。

## 四　结　论

公键密码制目前最大的缺点是在理论上尚不能证明第三者不能在实际可能的物力、时间内破译。其理由如下：

1. 虽然牟黑和麦氏法都把破译和NP-complete难题搭上关系，但若加上陷阱函数的咨询后，NP-complete的性质是否仍被保持则是一未知数。

2. NP-complete的观念只应用在一个算法最不利的情形下，而不论及其一般情形。因此一个破译法也许在最不利情形下需要天文数字的时间，但在很多普通情况下可以很快破译。

3. 究竟一个NP-complete问题是否没有多项式算法迄今尚无严格证明。

最麻烦的是实际的经验也不足以来断定公键译码的安全性。因为如果有人发现了有效的破译法，国家将把它列为最高机密而不让它公布。站在国家的立场上，有一破译法而不让别国知道，让别国继续使用一个不安全的公键密码制是其期望的。

在工商应用上，公键密码制为了安全的要求，在编码时必须大量增加信息的长度，因而减低了实际讯息传送的速度。一个可行的折衷办法是大量的信息仍以简捷没有陷阱性质的编码法作业，但编码法的键却用公键密码法传递。这种方法也叫做“公键输送”（Public Key distribution），其实键是密键，只是由公共网络输送而已。因为键的长度很短，输送不化费什么时间，所以可以经常换送新键。这样编码法虽然容易破译，但破译的速度显然远跟不上换码的速度，因此破译所得的信息可能早已明日黄花，破不破已经无关紧要了。

（本文主要参考Cryptology in transition: a survey, A.Lempel, Computing Surveys, March 1980）

• 上接46頁 •

1. 假如我们只提供研究生的教学计划，则不得不把注意力集中于培养在某一专门领域中的研究能力上，就没有足够的时间来进行广度方面的教育。这将导致应用数学工作的分裂，从而削弱总体方面的努力。通常，这会导致只有少数优秀学生进研究院学习应用数学。

2. 保持大学的教学规划，会使应用数学的教师们的兴趣和工作有一个共同的中心。大学教学规划的内容是要变化的，但是比较慢（牛顿力学还在起作用，量子力学也不会一夜间面目全非）；这就使教员有可能相对稳定地共同努力。而共同努力又造成稳定的局面。

在研究生的教学规划中，教员的兴趣必然会有不同。况且，他们的兴趣常常要随科学发展的趋势和学科的生命力而频繁地变化。这样一来，只有同一专门领域的人们之间才可能进行交流。然而，同事之间缺少交流，对于任何集体来说都是不利的。

3. 数学方法课程，包括概述性的课程，对于纯粹数学、自然科学、以及工程方面的许多其他学生具有很重要的教学价值。的确，系统地开设了数学方法的课程，就不必再开设那些“服务性课程”了，这种课程常常引起大学中极大的不满。

大学的教师有义务完成一定量的教学任务。有了大学本科的教学计划，应用数学家的教学任务基本上就是去讲授哪些为培养未来的应用数学家而开设的课程。这些课程对于前述种种目的会产生一种自然的、良好的副作用。如果应用数学家总是得去教那些“服务性的课程”，那就难怪他们会觉得自己是学术界的“二等公民”了。　（马希文译）