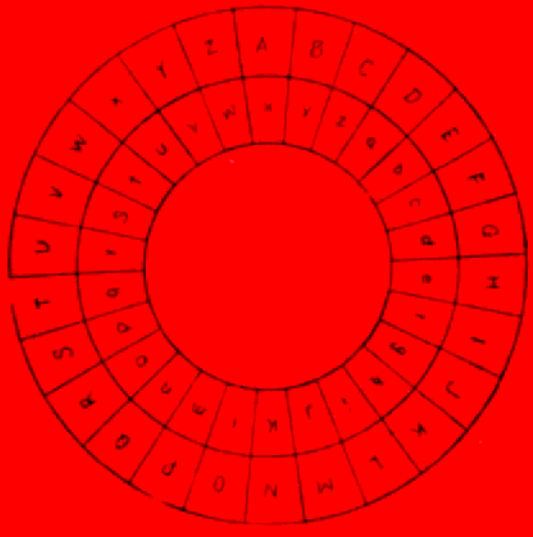
H·贝克 F·派普尔著

密码体制

通信保护



通信保密编辑部

密码体制

通信保护

H. 贝克
F. 派普尔 著

通信保密编辑部

封面设计：及金珩

密码体制
通信保护
（内部发行）
1983 年 8 月出版

编　辑　通信保密编辑部
印　刷　四川彭县306信箱印刷厂
发　行　四川彭县306信箱35分箱
成本价　8.00元

译 者 序

自古以来密码学的知识和经验一向主要掌握在与军事、政治、外交有关的保密机关手中，不便于公开发表，这是密码学的书籍一向稀少的原因。二次世界大战以后直到1978年，一共只出版了2—3本密码学的书，而且内容仅仅是手工作业的古典密码体制及其密码分析。

然而从1981年起情况有了急剧变化。1981—1982二年间一共出版了三本现代密码学的书。这种情况的发生当然和科学技术的进步（微电子技术、数字和数据通信、信息论、组合论、计算机科学等）是分不开的，但也和70年代商界和民间对保密的需要大大增加，导致密码学知识在民间传播分不开。由于民间的需要产生了一批民间公司的保密机设计人员，并在大学里产生了一批不从属于保密机关的密码学者（有人称这种民间的密码学叫公众密码学）。这些人可以无顾忌地发表文章，讨论观点，互相竞争。事实证明，正是这种情况大大加速了密码知识的传播和密码学的繁荣。它目前已受到数学、信息论、计算机科学等学者的广泛注意。大学已成为密码学研究的最活跃的基地。日益增多的民间厂商研究、生产了许多保密设备。

最近出版的三本书——一本书的作者是A·G·Konheim，一本是D·E·Denning。以上为81年出版，另一本就是本书，作者是H·Beker和F·Piper（82年出版）——各有其特点。前两本书主要着眼于计算机数据的保密，只有第三本书较为全面，既包括近年兴起的计算机数据保密问题，也包括传统的报和话的保密问题（当然是以现代的手段来解决问题）。但就我国当前的情况看，主要的应用还是在传统的报、话方面，因此我们优先译出本书。

本书的二位作者都是数学家。H·Beker博士还是Racal Comsec公司的首席数学家，对公司一切保密设备的密码学设计负责。而且他还具有相当丰富的实际知识与经验，包括通信系统的知识、用户对系统的要求的知识等。他曾两次来中国讲学。因而本书不仅是一本阐述密码体制的理论著作，而且还考虑到实际使用的情况及各种条件限制，对于实际的保密通信系统设计及应用亦有一定的指导作用。

本书是集体翻译的。参加校对的有林遇春、龙汶、金中、立早、良知、良言等同志，并由林遇春同志总校对。翻译的原则是尽可能做到技术上忠实于原文，符号上的个别差错作了修改，文字上的个别差错修改后作了说明，为便于阅读第三章有一处作了补充说明。在此并向参与编辑出版的所有人员表示感谢。

译者

1982年12月

绪　言

自从人们感觉到有让某些消息保守秘密的需要已有数千年的历史。当然，人们也会毫不犹豫地从截取的秘密情报中获得好处。这就导致“密码编码者”与“破译者”之间持续的、勾心斗角的斗争。然而作为斗争舞台的通信媒质在此期间也有相当大的变化。早在电报发明之前，通信技艺——像我们今天所了解的——就开始了。但是今天的社会是极大地依赖于现代的、快速而准确的消息传输方法。如同我们已有了长期建立的邮政和信使业务一样，我们现在已有了更加技术化和复杂化的媒质象无线电、电视、电话、用户电传和高速数据线路等。通常通信者的主要目标仅仅是尽可能快而且便宜地传送一份消息。但是有些情况下信息是机密的，截取者有可能从监听线路所得到情报中获得极大的利益。在这种场合，通信者必须采取步骤去掩盖并保护其消息内容。当然，所需的保护程度是不同的。有些时候阻挡偶然的“听者”使之不能懂得消息就够了，另一些时候就需要非常严格，甚至最坚毅的截取者也不应能解开它。本书的主要目标之一是阐述若干类可用的保护方法并强调评价一个给定体制所提供的保密程度的必要。

假如通信者能够采用不能被截取的传送方法，则显然他们的全部消息将是安全的。但是通信的最常用形式不能满足此要求。最接近于满足此要求的方法是派出信使。但这方法看来太慢、太费钱，并且假如要传送的消息量大的话甚至是不可能的。另一种使传送不能被截取的方法是在传送之前将每份消息的内容隐蔽起来。这是密码体制的目的。设计这种体制的技艺（及科学）被称作密码编码学。

毫无疑问，通信的保护和安全问题将在未来的年代中继续发展；不仅因为它在军事和政治方面的传统的作用，也由于在公众和商业领域的作用。密码编码人员在战时的作用已早被认识，但近来“大街上的人”也愈来愈认识到有关他的信息在若干数据库之间流通。这些信息中的某些属于私人性质，即这些知识虽对别人无用，他也宁愿别人不知道。然而其中的另一些是机密的，他需要感觉到未经授权的人将不能接触它，或许更重要的是不能更改它。在这种情况下通信者没有其他选择，只有着眼于他们的通信安全。事实上在本书写作时，一些国家正在立法以保护个人信息。

我们将看到，密码编码学的研究包含若干科学领域；尤其是计算机科学，电子学，数学和统计学。现代密码编码人员也需要实际通信的经验。我们的目的是对此题目提供广泛的介绍。本书适用于对密码学或通信有实际兴趣的人们，上述四个学科中的高年级大学生和研究生。为了使本书易于为具有不同基础的读者所阅读，我们试图使它“自完整”并尽可能少要预备知识。例如我们假设仅需要那些大多数电子工程师、计算机学者和统计学者都具有的数学知识。这并不意味着我们所用的全部数学对他们都是熟悉的，但我们相信任何新题目都阐述到足以读懂本书的程度。为了保险，也提供了基础材料的较深入的参考书。同样的原则应用于数学工作者所需要的电子学知识和计算机学者所要的

统计学知识等等。因此不论读者的学科是什么，几乎肯定有某些章节他感到很容易而另一些章节在初读时可能感觉困难。我们恳切地劝告初读者，在任一节当他发现很困难或太容易时就准备跳过。在埋头细读之前读完全书获得一个“全貌”是有很大收益的。我们再次着重指出本书的目的是对通信保护与安全的题目提供一个全面的介绍。无论读者打算继续进行密码编码的研究，制造密码设备或仅仅比较与评价不同的设备，本书都将为他提供符合其兴趣的适当的基础知识。他应当能有些眼光看出如关于密码体制的要求是什么；不同的部分如何配合起来以及本题目的理论和实际部分如何相互影响的。很清楚本书的任何一章都能写成一整本书。然而我们并不企图穷尽本书包含题目的任何领域，而仅试图为读者建立一个坚实的基础。

密码编码学直至今日的发展可以划分为若干阶段。第一阶段产生了许多密码体制，例如单表代替，能够用铅笔和纸或简单的器械实现。这些体制几乎已全部被破开了。已经证明只要给与足够数量已加密消息，整个消息（许多情况也包括后续消息）可以被解出。第一章中讨论了许多这些早期的体制。许多符号是在这章中介绍的，因此鉴于其重要性，我们尽可能地使它易读。我们细心地使它避免过于严密和正规，试图使它易于为所有读者所接受。

第二个发展阶段从20世纪之初（电报通信被真正建立的时间）到50年代末。这些体制通常采用复杂的机械和电气机械设备。第二章主要致力于一个这方面的例子，以及对它的分析和能够破开它的方法。虽然为破开它们所需计算量往往是巨大的，这些体制已有许多例子被证明是不保密的。有趣的是第二次世界大战中对一个这种机器的破译导致柯罗索斯 Colossus，最初奉献于人类的计算机之一的研究。（想做第二章密码分析的例题的任何人会立即懂得其缘由）。密码编码和密码分析（密码体制的破译）往往包含新技术和人才的先躯。

发展的第二阶段向第三阶段的推移往往被看成由两件事所促成。首先由于仙农在40年代末的划时代的论文，它证明密码编码学如何能置于坚实的数学基础上。然后微电子学在60年代的发展提供了追随仙农的某些思想，当然也包含引入的新思想的方法。本书的中心是这第三阶段。第三章介绍仙农的许多理论概念。第四章将许多这样的理论思想与实际保密的有关概念联系起来。第五到第九章涉及发展中的密码体制。

微电子学的应用意味着保密设备所能实现的函数的复杂性戏剧般地增长。这反过来使设计的数学更为复杂（第五到第七章）。少数场合，第三章和第五章较明显，那里含有一些证明或许涉及一些超出某些读者知识范围的概念。遇到这种情况，书中含有这些结果的非数学概要，如果读者限于读概要也不会丢失什么。虽然，这些更复杂的设备能够提供比以往任何时候高得多的保密程度是肯定正确的，但必须考虑到并非总是这样的。将某些复杂的保密设备组合成一个体制并假设它是安全的，这种做法是简单的但不是充分的。此外密码编码人员不应忘记密码分析者也能从这种新技术（微电子学）得到好处。密码编码学发展迅速的原因之一当然是由于密码分析者的出现。实际上通信保护在很大程度上能考虑为密码编码者与密码分析者之间的二人游戏；如果密码编码者输了将会有很严重的后果。为将游戏玩好，每个游戏者应使他自己十分清楚其对手所用的技术和自动化器

械。因此，离开了密码分析不可能发展密码编码的任何真正的技术，反之也一样。在本书中我们扮演密码编码者的角色，这意味着除非文中另有说明，象“好”这样的字眼的含意是“从密码编码的观点看来是好”。但读者也将看到，为了改进所研究的体制，往往要从密码分析者的观点去考虑情况。

这些近代发展的另一结果是密码装置的价格大幅度下降。这反过来意味着这些装置现在向着政府或军事以外的市场开放。当密码体制的使用者增多时，也必须发展新技术。要反复强调的一点是对一个系统的评价要对它的每一方面都考虑以后才是完全的。换句话说仅仅判定算法是好的，或传输媒质的性质是合适的，或用户打算使用系统的方法是合理的是不够的；应当将系统作为一个整体来考虑其适用性。假如一个另件被更换就应重新评价整个系统。此过程在第八章和第九章中讨论。

第八章涉及密码体制的不同的应用以及诸如密钥管理问题。我们研究了若干系统的例子并分析它们到不同的深度。例子之一是一个战略电报网可以用在例如军队、政府或高级商业用户。我们也比较了这样一个系统与轻便的战术装置的要求。另一研究得较仔细的例子是一销售点的智能终端。它可用于商店的结算以影响金钱从顾客的银行帐目向商店的帐目作直接的电子转移。假如顾客打算使其资金免于非授权的转移，通信安全在这里是另一种重要的使用环境。

第九章致力于与言语保密有关的问题。这是一个由于微电子学而产生划时代变化的领域。直到最近，模拟传输想要保密还要靠笨重的加密设备。现在已能在一个手机大小的保密装置中或将它装在无线电或电话机中而提供相当高度的保护。但将要看到，所有这些语音体制都具有许多密码学的困难。此章也致力于写好由于语音信号传输不同于数据而产生的某些问题。

最后一章涉及1976年 Diffie 与 Hellman 提出的公开密钥密码学。这是密码体制的一种新的划时代的类型。它能够解决许多密钥管理问题，这些问题自它们的概念产生之日起就困挠着密码体制的设计者。假如这些公开密钥密码体制成为可接受的，它们或许是密码学另一个发展阶段的报晓者。但只有时间的检验（所有检验中最难的）能告诉我们其结果。

已经提到过在对某一特定章深入研究以前读完全书获得全貌的重要性。或许也值得注意的是不必按章顺序来阅读。除去必须从第一章开始外，数学知识或对数学兴趣有限的读者宁可接着读第四、第八和第九章。这几章将使他信服对保密程度的某种形式的数学分析是绝对地重要的，因此推动学习其他章节。

最后关于书目作一注释。在每章的末尾列了少数有关的参考文献。然后在全书的末尾包含一份关于密码编码学的书籍文章的综合目录。不必为某些参考文献出现一次以上而吃惊。这样的文献在全书中有同样的编号，这也是对每章后面看来不规则的编号的说明。

目　　录

第一章　某些早期密码体制

1.1　引言

本章中我们研究某些早期密码体制。目的是尽可能非正式地并且试图说明基本概念而不过多涉及技术问题。实际上本章并不需要予先具备数学及统计学知识。为保持本章的连贯性，我们常常采用“安全的”和“随机的”这些术语而不正式地下定义。读者将对它们的意义有一个大致的直观概念，而正式定义在较后的章节中给出。眼下我们的目的是向读者介绍一些密码实例，而更重要的是使其了解面向加密人员的问题及对密码分析人员有用的一些技术。在所讨论的每个例子中，明文是英语，而密文是英语字母表字母的无意义的序列（或者更确切地说是外观上无意义的序列）。

密码体制的基本思想是伪装机密信息，使非授权者不了解它的意义。被隐藏的信息称作**明文**（或**消息**），而伪装的操作称为**加密**。已加密的信息称为**密文**或**密消息**。对消息加密的人员称为**加密者**，而密消息所送给的人员称为**收信者**或**接收者**。加密者用于加密他的明文的一组法则叫作**算法**。通常情况下，算法的操作依赖于密钥，加密者将密钥及消息一起送入算法当中。接收者知道密钥是非常关键的，知道这个后，可使他从密文确定出明文，因此，密钥和密文必须能唯一地确定明文。利用密钥从密文翻译成明文的程称作**译密**。如果以上述方法使用密钥，则所确定的体制的保密性应不依赖于算法而只依赖于密钥。不依赖于密钥的体制（或相当于只有一种可能密钥的体制）通常叫作**编码**。本书中我们将看到很多编码的例子。最著名的一种是莫尔斯，将字母表的字符转换成0、1序列的其他情况示于附录2。

凡截取加密者传送给接收者的消息的任何人称作**截取者**。一般情况下，截取者不知道密钥。加密者希望，由于缺少了这种知识而阻止截取者了解消息明文。**密码编码学**是密码体制的设计学，而**密码分析**是在未知密钥情况下给予从密文推演出明文的过程的名称。实际上密码分析者常常对推演密钥如同推演明文一样地感兴趣。如果他获得成功，那么他就能够译解出他所截取到的全部其他通讯，如同他是所指定的接收者。**密码学**同时包含密码编码学和密码分析学两者。

本章中的大多数密码已存在很多年了，而且无须求助于计算机或任何其他机器即可加密和译密。现在一般都不采用这些密码了。但为了追踪密码装置的发展及评价这些机器的设计者所取的方向，了解许多早期“手工”密码体制背后的原理是必要而正确的，虽然它们只有学术的或历史的意义。用于解开这些手工体制的很多分析技术，对于分析现代的电子密码体制仍然是重要的。我们后面将要看到，即使是一些“破译”某些早期密码的众所周知的基本方法，常常可以用作成功地攻击初看起来好象很复杂、而实际并未细心设计的电子密码体制。我们对“未细心”这个字眼的用法意味着，经稍多一

点思考，体制设计者就可保护它避免这些方法的攻击。但是必须认识到往往仅在对那个体制进行密码分析时，缺陷才能暴露。事后看来似乎是显而易见的，而在设备设计阶段不一定是很清楚的。

我们强调这些，并不意味着曾经被采用的所有“纸和笔”的加密方法有充分的价值。本章末我们给出了一个简短的文献目录，它们给出了比我们所需要的更详尽的内容，尤其是[2]和[5]。我们仅涉及到某些精心选择的例子以介绍贯穿全书以不同形式出现的各种技术和术语（避免突然出现的上下文）。因此，所有读者，不管他们的数学及技术知识基础怎样，希望能够把全章读完。

1.2 单表密码

当学生间互相传送“秘密”消息时，他们常常设计一种使字母表中的每个字母均表示另一个字母的“编码”。用我们的术语叫**单表密码**。为获得他的密钥，学生要写下字母表，然后在每个字母旁边写出在他们的编码消息中表示它的新字母，字母的选法就是他的密钥。一旦接收者有了这张密钥付本，他就可容易地译解消息。此外，显然的是如果正确地译密，那么秘密消息唯一地确定一个明文。但是如同学生们常有的情况那样，如果确定字母位置的规则是任意的，那么写有密钥的这张纸就很重要了。如果它丢失了或者被窃，则接收者就不能译出消息。密钥的存在招致希望截取消息的任何人的偷窃。显然，若加密者和接收者都记住了密钥，那么体制将更安全。为此，通常建立对明文字母选定密文字母的某种规则，使得记忆较容易些。单表密码通常叫作**简单代替密表**。表示一个字母表字母的有序序列叫**代替字母表**。

1.2.1 加法密码

单表密码最早的例子之一是在高卢战争中凯撒使用过的**凯撒密码**。在这种密码中，从a到w的每个字母均用字母表中在它后面第三个位置上出现的字母表示。字母x、y、z分别用A、B、C表示。这样，如果在明文相应字母下写密文等价字母时，凯撒密码的代替字母表给出如下：

明文：a b c d e f g h i j k l m n o p q r s t u v w x y z
密文：D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

（本章中明文用黑体小写字母，密文用黑体大写字母）。

对消息加密的算法仅仅是用明文字母下面的那个字母代替自身。接收者用代替表中上面的字母代替密文的诸字母来译密。例如：

明文：c a e s a r w a s a g r e a t s o l d i e r
密文：F D H V D U Z D V D J U H D W V R O G L H U

显然，凯撒密码是很简单的并且任何消息都可如此容易地加密和译密，对每种操作均

不需使用机器。尽管如此，在离开凯撒密码前，我们展示出实现这种加解密运算的简单机器。我们需要再次强调，在这种情况下，算法如此简单以致不需要机器。但是当我们讨论它们的算法变得更复杂时，我们将看到，加解密的自动方法是很关键的，否则浪费时间并且要产生很多错误。

图1.1示出了两个同轴轮子，外面的可以自由转动。如果转动外轮使D与a相重，而后通过将里面的一圈字母表示明文、用它外面的字母代替诸字母的方法来完成凯撒密码加密。

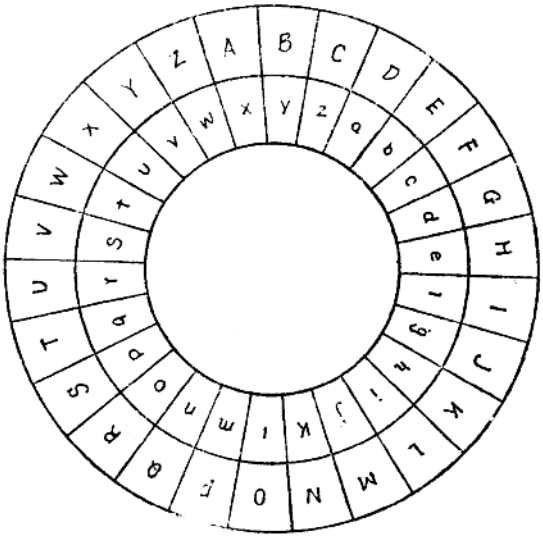


图1.1 一种实现加法密码的“机器”

现在我们有自己的机器，显然我们可以用它获得其他的密码。我们可转动外轮直到所选择的任一字母在a的外面，就可以得到不同的代替表，而后用同样的算法来加密我们的明文。由此可见，用我们的机器可得到26种不同的密码，而凯撒密码只是其中一个例子。这些密码称为**加法密码**或**移位密码**（注意，它们中之一即当A在a的外边时，明文和密文相同，当然这是通常不希望有的。我们常称这种密码为**恒等密码**，而称任何其他密码为**真密码**）。显然，倘若任一明文字母的密文等价字母为已知，那么这些加法密码中的任一完整的代替表就确定了。故我们可以定义字母a的密文等价字母作为该体制的密钥。因此，这就是加密者和接收者需要记住并保守秘密的全部内容。如果排列两个轮子使它们的字母重合，则各加法密码是按它的26种可能位置的某一数值逆时针旋转外轮得到的结果。外轮经26个位置转动以后其作用与不动相同，我们可用从0到25的整数与每个密钥联系起来。我们把这个数字叫作密码的**位移**。由上讨论现已清楚，凯撒密码是位移为3的加法密码，换言之，是具有密钥D的加法密码。

对于用密码通讯的双方，都需要知道密钥并能完成算法。由于密钥提供了保密性，

故他们通常试图保持其秘密。在有加法密码的简单机器情况下，一旦密钥被人知道，即人们知道怎样转动外轮时，实现算法便格外地容易。由于只有25种真加法密码，保持密钥的秘密仅得到很小的保密性。故现阶段讨论它大概是不值得的。顺序试探26种密钥以确定采用哪种密钥并不需要占用密码分析者多长时间。作为说明试探所有26种可能性而占用很少一点时间的一个实例，让我们把自己置于密码分析者的角色中，假设我们截取了下列密文，并知道采用了加法密码。（例如，若我们知道密码员用一种我们这样的简单机器，那么我们无疑可以知道该密码是加法的！）

密文：AOPZ TLZZHNL PZ H MHRL

我们首先选择密文中的一个字，此如说MHRL，顺序地用26种密码解译它。为简化此过程，我们先写出对应于26种密钥的代替表（表1.1）：

明文	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
位移0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

表1.1　26种加法密码的代替字母表

如果用的是位移1，明文信息将是lgqk。由于英语没有这样的单词，故我们知道位移不是1。简单且迅速地用MHRL依次试探每个位移的过程表明只有两个位移产生了可能的明文单词，即英语单词。它们是可给出明文fake的位移7和toys的位移19。到此我们知道是用了这两个位移中的一个，我们可用别的密文单词试探这两种位移。如果我们选择PZ，则位移7给出is，而位移19则给出wg。显然用的是位移7，而消息为this message is a fake。

对于这份特定的密文，还有更快的方法破译它。例如，我们注意到密文中的单字母H必定表示明文中的a或i。这就迅速提供给我们仅2个位移供考虑。然而现在我们不想研究分析任一给定信息的最好方法，我们仅想说明，一旦知道算法，在密钥量很小的情况下事实上是没有什么保密性的。这就意味着，不需告诉所用的密钥就可容易地确定消息。显然这是不希望出现的情况。由于这个道理，加法密码很少被采用。现在我们必须要试找允许密钥有较多选择的算法。

练习 1.1

我们已看到当译解MHRL时fake和toys是彼此相互的位移。（注意，由于位移19将toys加密成MHRL，位移7必将mhrl加密成TOYS。这样，既然位移7也将fake加密成MHRL，于是位移14就可将fake加密成TOYS）。找出其他的英语单词对，而它们是彼此相互的位移。

练习1.1实际上是相当困难的，因为很少有这样的单词对。事实上我们知道没有字长为6以上的。

在转向下节以前我们强调指出上例的攻击方法的一个特殊方面。它依靠这样的事实，绝大多数字母的组合在英语中（事实上，任何语言中都一样）是无意义的。这个简单性质是很多统计攻击方法的基础（统计方法在本章及后面的章节中讨论）。

1.2.2 仿射密码

在讨论加法密码中，我们已看到位移26与位移0是相同的。同样清楚的是任何数的位移，不管多大都与0至25内某个位移数等同。例如，为找出这个数，我们用我们的简单机器从a的外面为A开始转动它经过这个数那么多位置，当作完这个操作时，外轮的最终位置告诉我们是一个较小的数。例如位移84可以转3整圈（即3个连续位移26等于位移$3\times26=78$）接着再位移6得到，故位移84与位移6相同。

现在我们想利用这种观察结果以定义任两正整数间的新“加法”。如果α和β是任意两个正整数，则用$\alpha\oplus\beta$表示从0到25内的唯一正整数γ，使得位移$\alpha+\beta$与位移γ相同。例如我们已看到位移84与位移6相同，因为$21+63=84$，我们就有$21\oplus63=6$（了解模运算的任何人将意识到我们介绍的仅是模26加法。这样的读者对下面几页可很快浏览过去，当然不需要作练习1.2，1.3，1.5）。

练习 1.2

证明：

（i） $15\oplus19=8$；

（ii） $6\oplus11=17$；