电信技术普及丛书

密码通信入门

王德文 编著

人民邮电出版社

电信技术普及丛书

密码通信入门

王德文　编著

人民邮电出版社

内 容 提 要

本书通俗地、富有趣味性地介绍密码通信的基本概念、密码构造和破译等一般知识。在此基础上介绍了用于计算机通信的密码技术及加密设备。最后，介绍了密码通信系统的密钥管理。

本书可供从事通信、数据处理、计算机的工人、技术人员阅读。

电信技术普及丛书

密 码 通 信 入 门

王德文　　编　著

责任编辑　　董乐前

人民邮电出版社出版
北京东长安街27号
河北省邮电印刷厂印刷
新华书店北京发行所发行
各地新华书店经售

开本：787×1092 1/32　　1987年10月第　一　版
印张：9 8/32　页数：148　　1987年10月河北第一次印刷
字数：211千字　　印数：1-4 100册

ISBN7115—03473—7/TN

定价：1.80元

序　言

密码学对一般人来说也许是陌生的，甚至是神秘的。这是因为密码的使用，大都是在极其秘密的或者不容易被第三者所觉察的情况下进行的。也因为密码的使用者主要是政府部门和军事部门，他们对密码采取了极其严格的保密措施。同时，密码学也不像物理学或化学那样，容易为人们所理解并产生浓厚的兴趣。这也许是迄今为止，使得密码学这门古老而新奇的科学未能普及的主要原因吧。

然而，密码通信的历史极为久远，特别是自从战争、贸易和外交事业问世以来，它就一直成为人们用以保护秘密信息传输的有力手段。因此，密码通信自古以来就受到了国家和社团的高度重视。目前，密码通信已经发展成为一门系统的技术科学，甚至形成了信息传输理论中的一个重要分支。几个世纪以来，密码通信已经从传递手工构造的最简单的代替式或换字式密码，发展成为能够自动产生10^N（N值可以高达数百）个密钥的极为复杂的密码传输系统，而要破译这种密码，需要花费漫长的时间和高昂的费用。换句话说，今天现代密码通信系统所构造出来的最佳化密码，几乎可以提供无限制的保密度。从实践意义上讲，那种所谓“没有破译不了的密码”的传统观点，受到了挑战。

尽管如此，在人类社会高度现代化的今天，由于电子通信应用的范围愈来愈广泛，特别是由于卫星通信和微波通信的大力发展，从而极大地便利了破译者的活动。要对那些拥有先进

的电子计算机技术和信息处理技术的人保守机密就更为困难。正是在这样的形势下，对密码通信进行深入研究以提高信息传输的安全性，就显得十分必要了。

如果说在三十年前，密码通信还仅仅局限于军事、外交和安全等特殊部门的话，那么今天的密码通信则已经趋于社会化。在许多部门，其中包括军事、外交、贸易、金融，工业、渔业、安全、气象和邮电等部门，甚至在私人通信和数学游戏中都广泛地应用着密码术。那种仅仅依靠少数人关起门来从事密码学研究的原始做法，显然已不能满足整个社会的需要。

保密通信方式归纳起来可以分为两大类。一类是保持所传送的消息的形态不变，而对信道加以保护，使消息不为他人所截获来达到保密的目的。例如派遣武装信使送信，化学密写、显微点、专线电话、保密电缆、瞬间通信以及扩展频谱通信等方式就属于这一类。另一类是仍然利用普通的邮路或通信线路，而将消息的形态加以变换后再传送，使除了通信双方外任何第三者都不能对消息解读，同样达到了保密目的。通常人们把前一种方式称为信道保密方式，而将后一种方式称为消息保密方式或密码通信方式。在实际上二者常常并用，但是在保密学领域中，最具有吸引力、也最有发展前途的乃是第二种保密方式，即密码通信。

呈现在读者面前的就是一本普及密码通信技术的小册子，它的目的在于通俗地介绍密码通信的基本概念，讨论密码的构造、传输和破译方法等一般知识。书中所引用的素材，全部来自国外公开发表的文献资料。

本书初稿承蒙齐忠涛、傅有卿以及华庆同志审阅，谨在此表示诚挚的谢意。

作者于北京

目　　录

第一章　密码通信的发展历史

密码通信有几千年的发展历史，其中古典密码术、近代密码学和现代密码理论构成了密码通信的三个发展阶段。而仙农保密通信理论和电子计算机的出现，从理论和技术两个方面为密码通信开辟了广阔的前景。

悠久而传奇的古典密码术

密码通信的历史极为久远，它的起源可以追溯到几千年前的埃及、巴比伦、古罗马和古希腊。在古希腊神话和巴比伦王朝的《旧约圣书》中，都有许多传奇式的密码故事。

我国虽然是文字出现最早的文明古国之一，但是，由于我国长期使用形意文字，限制了编码学的发展；另一方面，也许是更重要的原因，那就是几千年的封建制度，将文字通信只笼断在少数人手中，从而极大地妨碍了密码学的研究。

在历史上有文字记载的用手工构造的密码，大概要算是公元前四百年斯巴达人用的“塞塔”（Sitar）式密码（又称“天书”）了。这种密码的构造方法十分简单：将一条一厘米

宽，二十厘米左右长的羊皮纸带，以螺旋形斜绕在一根铅笔或竹棒上（参见图1.1），然后将通信文（明文）沿铅笔纵轴方向从左至右写入，写完一行以后，将铅笔旋转九十度，再从头接着写，直到写完。最后将羊皮纸带从铅笔上解下，沿纸带重新排列的文字即是密文。从这种密码的构造方法来看，实际上就是最早的转置（或叫移位式）式密码了。

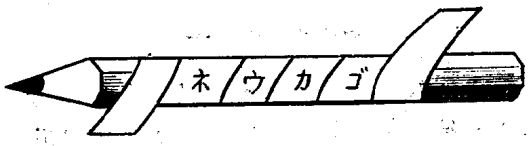


图 1.1 塞塔式密码的解读方法

古典密码早期曾被用于占星术和炼金术中记载口诀或秘方（参见图1.2）。进入罗马帝国之后，密码通信才被用到政治、军事和外交的通信中。例如，古罗马皇帝凯撒，就曾发明并亲自使用了一种密表，后来称之为“凯撒”密表。它将明文字母用该字母后的第三个字母代替。到了中世纪后期，特别是文艺复兴时期，由于异常复杂的政治和外交斗争的需要，同时也由于天文学、数学、文学和艺术的蓬勃发展，使古典密码术有了显著的进展。在意大利的元老院和东罗马帝国，都广泛地采用了密码通信。据历史记载，当时在罗马、米兰等地可以买到关于密码方面的书籍。而且在这些密码书中，已经使用了约束语。

A= ⊙	N= ☊
B= ☿	O= ♍
C= ♄	P= ♒
D= ♆	Q= ♏
E= ♅	R= ♑
F= ♁	S= ♐
G= ♀	T= ♓
H= ♂	U= ♉
I= ☿	V= ♊
J= ☾	W= ♈
K= ♉	X= ♋
L= ♊	Y= ♌
M= ♋	Z= ♎

图 1.2 中世纪时期的换字式密码

从十六世纪至十八世纪，古典密码术在意大利、英、法等国已非常发展。特别是在意大利商业城市威尼斯，专门设有密码局，从事职业性的密码编译工作。同时在法王路易十四的宫庭内，收藏有二册制密码书。所有这些都标志着古典的换字式密码已经达到相当完美的程度。

在古典密码术发展的进程中，值得推崇的密码学家有意大利物理学家、医学家波达（G.B.Porta），和法国外交官维吉尼亚（B.Vigenere）。波达于一五六三年发表了《秘密书记法》(«De Furtivis litteratum Natis»)的有关密码学的著作，并第一次提出了多表式的波达换字表。维吉尼亚一五八六年发表了《密码纲要》(«Traite des chiffres»)这一极为重要的密码学著作。在这部著作内他提出了采用二十六进制的多表式换字表，而根据这种换字表构造出来的维吉尼亚式密码，曾被认为是三百年内破译不了的密码。正因为这样，维吉尼亚式密码直到今天仍作为一种有效的加密体制而被应用着。

古典密码术所以有如此巨大的发展成就，一个极为重要的原因是当时的数学、天文学、文学、艺术和占卜术等有了相当高的水平。例如十六世纪英国的大数学家皮埃特，曾任过英王亨利四世的专职密码破译人员。罗马皇帝凯撒，不仅是密码学家，政治家，军事家，同时也是一位诗人。图1.3是他写的密码诗。另外在古典密码体制中，有相当一部分密码采用了音

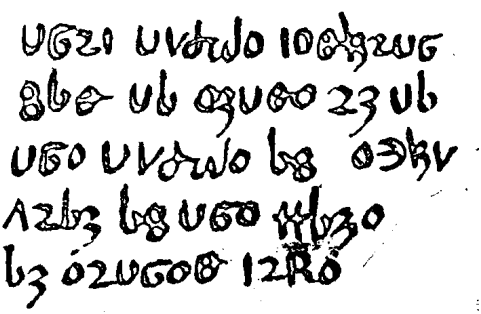


图 1.3 凯撒的密码诗

符、乐曲、艺术图形或诗句的形式，图1.4就是有名的舞蹈人形密码。

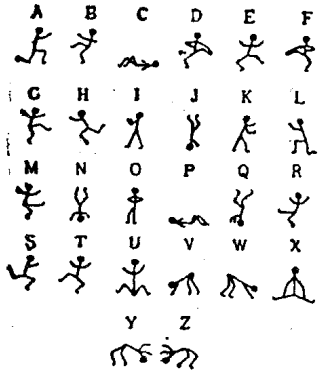


图 1.4 著名的舞蹈人形式密码

世界大战与近代密码学

古典密码术虽然不是源于战争，但是它的发展成果却首先被用于战争，并且反过来又进一步刺激了它的发展。

一八三四年，伦敦大学的实验物理学教授惠斯登（C. Wheastone）发明了电报机，这是通信向机械化、电气化跃进的开始。同时也为密码通信采用在线加密技术开创了前提条件。一八六七年，惠斯登发明了圆盘式密码机和由这种密码机构造的普雷佛尔密码。这种密码是根据多表代替加密原理设计出来的。

到一八八三年，出生于荷兰而后加入法国籍的奥古斯特·克尔克霍夫斯发表了《军事密码学》一书。在此书中他提出了建立军事密码通信系统的两项基本原则，即，

1. 任何一种密码必须能用于实际的大容量、快速通信；必须假定破译者已经掌握了一般密码通信体制，因而必须用高度可靠的密钥来保证所用的体制。

2. 只有破译才是验证一种密码体制可靠性的唯一途径，因此破译技术也就成了刺激密码学发展的有力手段。

在这两项原则下，他提出了六项基本要求，这也是第一次系统地对军事密码通信提出的定性要求。它们是：

1. 可靠的军事密码体制，应该既在理论上，同时也在实际上是不可破译的。

2. 加密体制的泄露，不应该给通信者带来更大的损失。

3. 密钥应便于记忆，而且容易变更。

4. 密文应能用于电报传输，并可扩大到数据和电话信息。

5. 密码通信设备及附件应能由一人携带或操作。

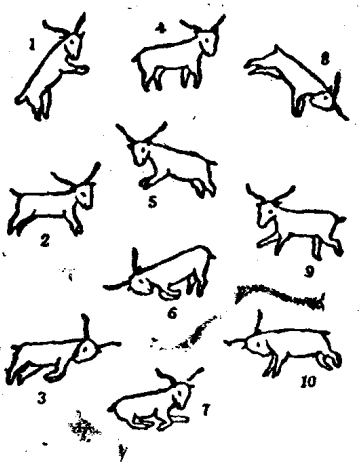
6. 所采用的加密体制应简单明了，既不需要掌握冗长的规则，又不致于使人神经过分紧张。

我们可以看出，这些要求直到今天仍然是适用的，但是第一条往往是做不到的，而且也是不必要的。因为在战争中使用的军事密码，一般仅仅要求能拖延敌方的破译时间，而并不要求无法破译。

一九一四年第一次世界大战爆发，德、俄相互宣战。当时俄国方面采取了攻势，把主力分成两路挺进，而德军则采取了战略转移，于八月二十六日至三十日，德军主力在但丁布尔希平原把十万余名俄军歼灭。这次战役作为著名的一次歼灭战虽然铭记在作战史册，但是对于使这次战役德方取得成功的关键原因之一的德军通信情报的巨大贡献却很少有人知道。

原来德军无线电通信谍报班在平时十分注意破译俄军密码

通信的电文。在交战后，德军破译了俄军第一军发给第二军的密电，从中得知，第一军的给养已经中断。根据这一重要的情报，德军在这次战役中取得了全胜。此外，也有人认为是德军无线电通信谍报班破译了俄军的密码后，又模仿这种密码给俄军发送假电文，诱敌上钩。这也说明当时已开展了密码战。图1.5是第一次世界大战期间，德军曾使用过的山羊式密码。它使用十种不同的山羊姿态，代表不同的敌情。



(1)	道路两侧有敌人	(6)	飞机侦察过的道路
(2)	防守严密的道路	(7)	骑兵侦察过的道路
(3)	向右行动中的敌人	(8)	步兵侦察过的道路
(4)	向左行动中的敌人	(9)	准备退却之敌
(5)	已暴露的敌通信线路	(10)	转入进攻之敌

图 1.5 第一次世界大战时德军用的山羊式密码

一九二〇年，美国电报电话公司的A·S·弗纳姆，利用将电传打字机的五单位码，与密钥字母进行模2相加的原理，发明了巴纳姆密码，它的加密原理是在发信端和收信端各有一个相同长度（码元数相同）的密钥纸带，二者分别以同步速度输

入和输出。当发信端有电传信息输入时，便将代表这些信息的五单位电传码与密钥码在一个异-或逻辑电路中进行模 2 相加。亦即如果信息码为11010，密钥码为11101，
则按以下方式进行模 2 相加，得出密文：

信息码　　11010
密钥码　　11101
⊕
密文码　　00111

在接收端，只要把接收到的密文纸带与密钥纸带在异-或逻辑电路中再一次进行模 2 相加，便可恢复出原来的信息，也就是实现了解密，亦即

密文码　　00111
密钥码　　11101
⊕
信息码　　11010

虽然这种密码结构在今天来看已经非常简单，但是由于这种密码体制第一次使加密由原来的手工操作进入到由电子电路来实现，亦即实现了在线加密，因而在近代密码学发展史上占有重要的地位。

后来，美国人J.O.摩波卡金少校在这种密码基础上设计出一种一次一密体制，他采用随机噪声做为密钥，因此没有重复性。也就是说密钥码不可能人为复制，所以是一种不可破译的密码体制。但这仅仅是理论上的情形，实际上在通信业务量很大时，所需的密钥量相当庞大，为使用带来很多困难。

在一九二〇年至一九三〇年期间，这种一次一密体制又有了进一步改进。其中一种方案是在上述密码体制基础上，研究出了具有五个或更多个转轮的密码机（每个转轮代替一步加

密）。但历史事实已经证明，这种密码是相对地不保密的。因为密码分析家只要掌握了大量的通信资料便可破译。在太平洋战争中日本使用的九七式机械密码（又称为紫密），就是属于这一种。它的基本原理是把多表代替式密码，用机械的方法来实现，也就是用多个转轮来构造多个换字表，然后逐次使用。

上述这种机械密码开始作为日本海军内部通信使用。一九三八年后用于外交通信。而从此，美国海军通信机关便开始研究破译这种密码。一九四〇年，在美国陆军通信情报机关任职的密码分析家弗里德曼，终于破译了这种密码。在中途岛海战中，日本海军大将山本五十六因密码电报被美国截获破译，而被击毙在飞机上。

总之，由加密和破译构成的密码战不仅对战局起着极大的影响，而且也使密码学本身获得了飞速的发展。

仙农对密码通信理论的卓越贡献

尽管密码通信有几千年的发展历史，并且在密码的构造和破译方面积累了相当丰富的经验，但是可以说直到一九四五年甚至更晚一些时候为止，密码通信中的一些最本质的东西，并没有被发现。这就使得人们长期以来无法用一种统一的理论和方法对密码通信进行描述，并从而进行定量的分析和计算。同时在过去关于密码学方面的书中，也大都是一些新的加密体制的罗列，缺乏系统性。

仙农是信息理论的创始人，一九四九年十月他在《B.S.T.J》杂志上发表了《保密系统的通信理论》的著名论文，提出了密码通信系统模型，把各种各样的加密体制概括成了一对加密和解密变换器，而把整个系统概括为一条传输密钥的秘密

信道，以及受密钥控制的加-解密变换和传输这种变换的普通信道。这样就可以用数学模型法和现代信息论对任一个密码通信系统进行定量的分析了。

仙农贡献的另一方面是在他的理论中，引入了熵和保密度这两个极为重要的概念。前者是信息量的计量标准，后者是保密强度的理论指标。有了这两个物理量之后，人们不仅可以对任何一个密码通信系统进行分析或计算，而且也是设计新的保密通信系统的理论依据。

仙农理论的主要成果，表现为由一组图解曲线所确定的交点理论。这一理论把密码学者从历史上就遇到的解密置信度问题，作了一个具有普遍意义的解释。他从这个交点理论出发，提出了两种在理论上是不可破译（即破译结果的置信度为零）的加密体制，亦即在图上无交点的那种体制，称为“完全保密的体制”。我们在前面介绍的弗纳姆用随机穿孔纸带作密钥与信息文逐一进行模 2 相加的方法，当密钥的随机性十分理想，因而不产生重复时，就属于这种完全保密体制。只是由于它所要求的密钥量至少不小于所要传送的信息数量，所以在信息量较大时，就不适合于实际应用。

仙农从理论上阐明了增加密钥量和减少多余度可以把解密交点推移得更远，因而更加有利于提高保密度。

信息化时代的密码通信

电子计算机的发明是人类科学技术史上最伟大的创举之一，有人将它与蒸气机的发明相媲美，誉之为第二次产业革命，这是并不过分的。

电子计算机的出现，不仅是自动化时代的开始，而且也是

信息化时代的开始。目前信息交换的形式已经由传统的电报电话方式，扩展到声音、图象（包括文字、文书、图片、照片等），数据等不同的形式。这样就使得信息的传输、变换与控制以及处理等全部过程都归结到计算机中来。

信息加密—解密变换是信息变换处理的一种特殊形式，因此不仅能够用计算机实现，而且表现出一系列的优点。其中最重要的是能够实现自动化加密。这对于高速、大容量的数据通信的加密尤其显得重要。另外由于计算机能够产生长周期伪随机化的密钥序列，所以计算机加密的保密度也很高。

当然，在计算机加密技术迅速发展的同时，采用计算机对密码通信进行截获和破译的技术也越来越先进。尤其在卫星通信，微波中继等大容量无线通信广泛应用的今天，信息被截获并利用计算机迅速破译的机会变得越来越多。

但是，上述情况还仅仅是问题的一个方面，在今天威胁更大的则是计算机本身数据保护的问题变得越来越突出。在国外，利用计算机犯罪的现象已经发展成为一个新的社会问题，犯罪分子通过篡改或窃取计算机程序，可进行盗窃巨款等犯罪活动，甚至转眼可以使一个公司破产，而犯罪分子却一跃成为百万富翁。

正是在这种形势下，促使人们极需研究数据加密技术和手段。其中首先被提出来的就是数字加密技术。

数字加密技术的基本原理，是先把话音信号（模拟信号形式），用增量调制或脉码调制方式，变成数字信号的脉冲序列，然后将这些数字形式的信号与一个数字化的密钥序列进行加密变换，就得到了数字加密信息。从五十年代至六十年代中期，由于数字电路和装置的体积大，造价高，限制了这种体制的发展。自七十年代以来，由于半导体集成电路技术的突破，