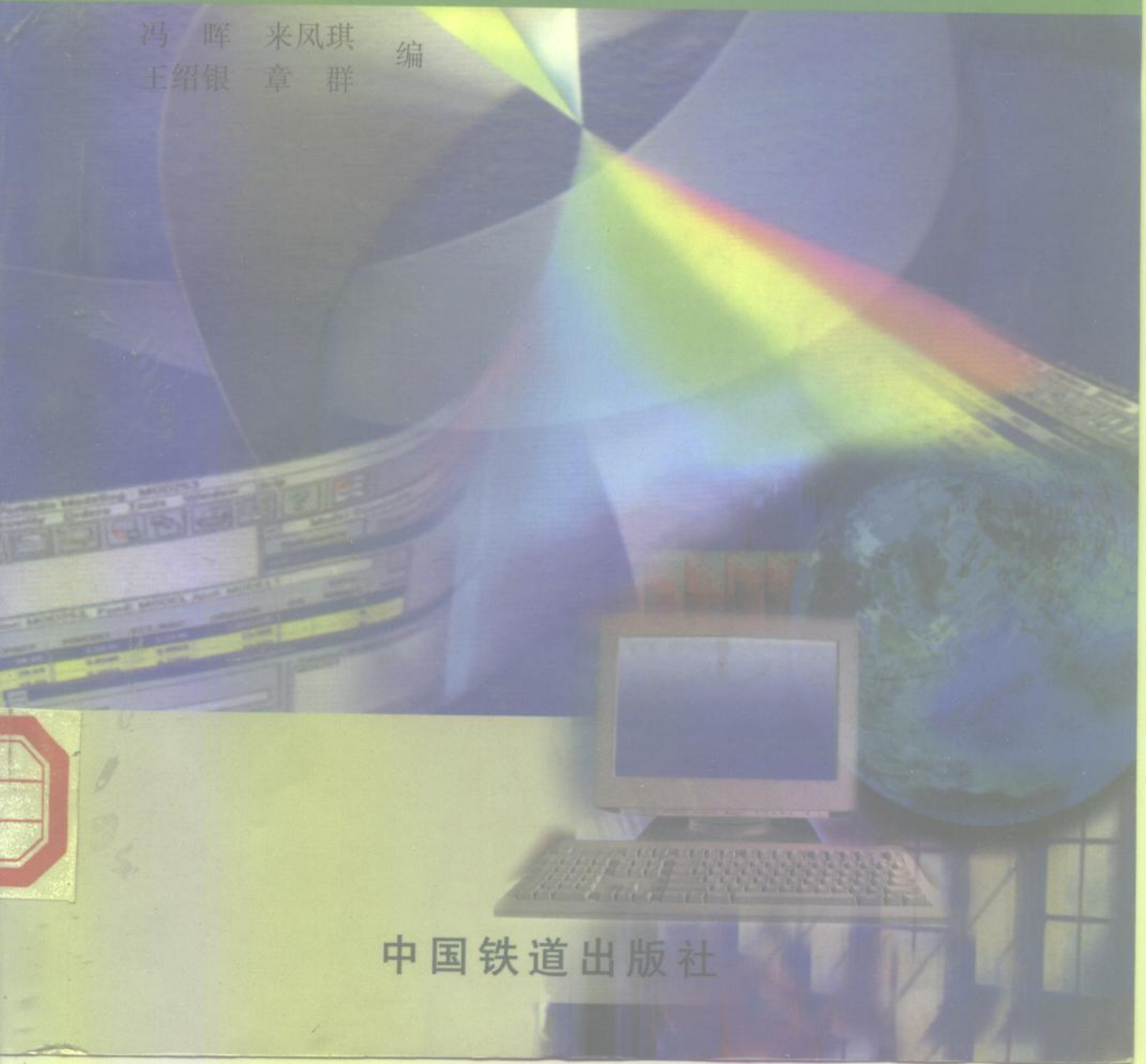
JISUANJI MIMA XUE

# 计算机密码学

冯 晖 来凤琪 编
王绍银 章 群



中国铁道出版社

# 计算机密码学

冯　晖　来凤琪
王绍银　章　群　编

中　国　铁　道　出　版　社
1999年·北京

(京)新登字 063 号

## 内 容 简 介

这是一本介绍现代密码学——计算机密码学的实用教程，该书详述了密码学的协议（简单协议、复杂协议到深奥协议）、密码技术（密钥生成、密钥存储、密钥管理等等）和密码算法（包括数学基础、数据加密标准 DES、对称算法、公钥算法、单向哈希函数、流密码等）。编程人员通过应用密码技术对信息加密和解密来维护计算机数据的私有性，在计算机系统和网络通信中建立安全保障，以免信息被未授权用户掠夺与破坏。书中大量算法都给出了 C 语言实现函数，以便读者应用。

本书可作为从事计算机软件、网络通信、网络安全、电子信息和密码学等专业的学生、教师、工程师以及计算机爱好者的学习参考。

**图书在版编目(CIP)数据**

计算机密码学/冯晖等编. —北京：中国铁道出版社，1999.6
ISBN 7-113-03358-X

Ⅰ.计… Ⅱ.冯… Ⅲ.电子计算机-密码-理论 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(1999)第 27707 号

**书　　名**：计算机密码学
**著作责任者**：冯　晖　来凤琪　王绍银　章　群
**出版·发行**：中国铁道出版社(100054，北京市宣武区右安门西街 8 号)
**策划编辑**：殷小燕
**责任编辑**：殷小燕
**封面设计**：李艳阳
**印　　刷**：北京彩桥印刷厂
**开　　本**：787×1092　1/16　印张：16.5　字数：408 千
**版　　本**：1999 年 7 月第 1 版　1999 年 7 月第 1 次印刷
**印　　数**：1—2000 册
**书　　号**：ISBN7-113-03358-X/TP·366
**定　　价**：30.00 元

# 前　言

数字化和因特网(Internet)的普及变革着我们的学习方式、工作方式、娱乐方式，总之改变了我们的世界。“信息的基元，比特(Bit)”正在迅速取代原子而成为人类生活中的基本交换物。看着孩子们自如地在浩瀚的数字世界中漫游和寻奇猎取，可以想像不远的将来由于年轻一代的影响，分布式的工作心态将会弥漫社会，中央集权式的生活观念将成过去；地理束缚的大解放，使地球村内的友谊、合作将会大大加强；摆脱了许多传统偏见的人们将被吸引到一个更加和谐的世界之中。在信息急剧增加，一再地冲破时空局限的同时，大量属于个人私有的，或举足轻重和价值昂贵的数据，如何实现安全保密的问题也日见重要。有人担心未来10年中隐私权的遭受侵犯将是计算机科学技术带来的一个黑暗面。然而有矛必有盾，密码学这一古老(指传统的密码术)而又年轻(指计算机密码学)的学科将会担当起防卫窃听和攻击的任务，使信息的安全保密成为可能，未来数字世界的前景是乐观的。

密码学除了它在古埃及的形成初期，一些墓碑上的铭文，是用神秘性来表达庄严和权威之外，它总是与军事、外交和情报领域联系在一起。它涉及国家利益因而是政府责任部门的要务。诚然，这些概念目前仍未过时，但是新技术的出现，新世纪的到来，“保密”已出现在大众化的生活之中。当你用信用卡在网上购物时，你不会不考虑信用卡口令的保密和安全。当你将个人的医疗信息送往远处名医诊断，或当你收到治疗意见和处方时，你不会不担心遭受攻击和篡改的可能。至于广为使用的电子邮件，如有保密软件给它套上安全的“信封”，则将倍受欢迎。尽管至今从事密码学研究的人员中，秘密进行研究的人数远远超过公开研究的人数，政府控制的研究重于民间自发的研究，但广泛公开研究密码学的历史已持续了十多年，有一天密码学作为政府特权的看法将会改变。

但是密码学本身却是以极其枯燥的纯数学作为基础，读起来会感到十分苦涩。惟有志于这一领域的研究者才会有嚼橄榄的感觉。本书详述了编程人员如何使用密码学——对信息加密和解密的技术——来维护计算机数据的私有性，以免被未授权用户掠夺与破坏。本书的特点除介绍了实用密码技术的最新发展之外，还用大量篇幅填补了在密码技术与程序实现上的空白，使设计计算机应用程序、网络和存储系统的编程人员知道如何在计算机软件和系统中建立安全保障。

全书分为四个部分。

第一部分(第2章至第6章)介绍密码学的协议。涉及的协议从简单到复杂再进入深奥阶段。

第二部分(第7章和第8章)讨论密码技术。第7章关于密钥，为达到安全，密钥应有多长，如何生成密钥，如何存储以及如何管理密钥等等。第8章讨论使用密码算法的不同途径，以及如何为通信、数据存储等选择算法。

第三部分(第9章至第16章)转向讨论算法。第九章是数学基础。第10章讨论数据加密标准。第11章介绍其它对称算法。第12、13章讨论公开密钥算法。第14章叙述单向哈希函数。第15章关于随机数生成和流(序列)密码。最后，第16章讨论了实现第一部分中部分协议

的特殊方法

第四部分(第17章)介绍这些算法和协议在现实世界中的实现。

为配合本书的教学,所有的算法程序另出一张软盘,有需要的读者请与中国铁道出版社联系。联系电话010－63549447。

本书大部分取材于Bruce Schneier的"Applied Cryptography"第一版和第二版,编写工作是远程医疗基础研究的一部分。它得到了上海铁道大学负责医工结合的王文浩副教授、孙章教授、陈保权副教授的支持和帮助,在此深表感谢。

最后,但却是必不可少的是由于中国铁道出版社和殷小燕编辑的支持和帮助,本书才能献予读者。

《计算机密码学》一书可作为计算机网络、通信、电子信息和密码等专业的高年级本科生和研究生有关课程的教材,也可供从事远程医疗,电子商贸等有关技术人员学习参考。

编　者

1999.3

# 目　录

# 第1章 基 础

## 1.1 术 语

**发送者和接收者**

在信息传送过程中，主动提供信息的一方称发送者，得到信息的一方称接收者。发送者要确保信息安全传送，使窃听者不能盗取信息。

**信息和加密**

原始信息是清楚明白的文本，它又称明文。以隐藏信息实质内容的方式伪装信息的过程就是加密，加密后的信息称为密文。把密文转回明文的过程称解密。所有这一切均表示在图1.1中。

保持信息安全的科学技术称为密码术(Cryptography)，它是密码员的工作内容。揭示密文伪装的科学技术称为密码分析或密码破译(为行文方便，本书两种称呼叠用)，它是密码破译员(或密码分析员)的工作内容。兼有密码术和密码破译两方面内容的数学分支就是密码学(Cryptology)，这是密码学家的研究领域。密码学学科要求近代密码学家应具有理论数学方面的训练。

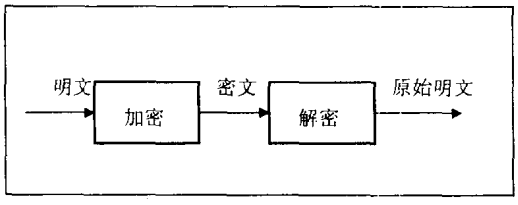


图1.1 加密和解密

明文信息用M(Message)或P(Plaintext)表示。它是比特流、一个文本文件、一个位信息图、数字化语音流、或数字化视频图像等类似物。只要联系到计算机，M就是简单的二进制数据。

密文用C(Ciphertext)表示。它也是二进制数据。有时与M等长，有时大于(压缩再加密，C可能会小于M，然而，单加密通常不能做到这样)。加密函数E作用于M产生了C，数学表示为：

$$E(M)=C$$

逆操作，解密函数D作用于C产生了M：

$$D(C)=M$$

因为加密和解密信息的全过程是恢复原始明文，下列表达式必须成立：

$$D(E(M))=M$$

**认证，完整性和不许抵赖**

密码术除了提供机密性之外，还要求做以下工作：

认证：信息接受者应有可能核查信息来源，任何闯入者无力装扮成原有的发送者。

完整性：信息接收者应有可能验证信息在传播中未经修改，闯入者无力用假信息代替合法的原有信息。

不可抵赖：发送者在发送出信息后无法抵赖他所发出的信息。

这些计算机上进行社交的要点也类似于人们面对面交流时的要求。某人讲他是何许人时

就需用证件(不管是工作证,驾驶执照或护照)来证实。这些表示某人身份的证件确能代表其人。认证,完整性和不可抵赖提供的就是这类服务。

**算法和密钥**

密码算法,称为加密算法,是用来加密和解密的数学函数。为给明文信息加密,用加密算法函数。为给密文信息解密,用解密算法函数。

如果算法的安全性基于算法工作的保安,这是一个受约算法。受约算法只是历史上曾被注意,可惜不适合今日的要求。大的或变动着的用户团体不能使用它们,因为每次一个用户离开了,团体中的每一个人必须改换不同的算法。如果团体中某个人偶然泄漏了秘密,其他每一个人也必须更换算法。

更糟的是受约算法无质量控制和标准。每一个用户团体必须有他们自己独特的算法。他们不能用现成的硬件或软件产品,因为窃听者可以购买同一商品并弄清算法,从而不得不设计自己的算法并付之实现。如果该团体中没有很好的密码员,他们将不清楚所用的算法是否安全。尽管这样,对低安全性的应用来讲,受约算法还是非常有效的。Zenith 的视频编码技术是一个加密算法的例子。

近代密码术用密钥来解决安全性问题。密钥用 K 表示,它可以是任何一个大数。这个密钥能取许多值中的一个。密钥的取值范围称为密钥空间。

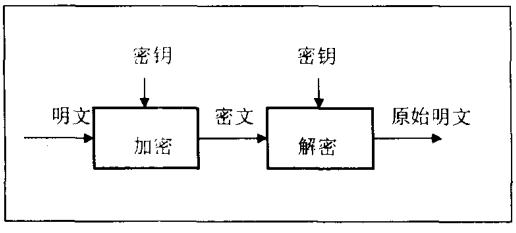



图 1.2 具有相同加密和解密密钥的系统

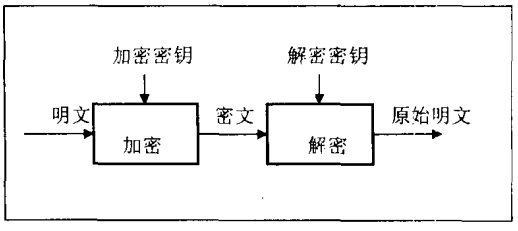



图 1.3 具有二个密钥的加密和解密系统

密钥可同时用于加密和解密,那么加密和解密函数表示为:

$$E_K(M)=C$$

$$D_K(C)=M$$

如果加密密钥和解密密钥是相同的,则这两个函数具有以下性质:

$$D_K(E_K(M))=M$$

如图 1.2 所示。

某些算法用不同的加密密钥和解密密钥(见图 1.3)。即,加密密钥 $K_1$,解密密钥 $K_2$。在这种情况下:

$$E_{K1}(M)=C$$

$$D_{K2}(C)=M$$

$$D_{K2}(E_{K1}(M))=M.$$

密钥决定了这些算法的安全性,而不是算法的内容。所以人们尽管可以发表和分析算法,用算法可以制造大量商品,即使窃听者知道算法,但若不知特有的密钥仍不能读取信息。一个密码系统应包括算法以及所有可能的明文、密文和密钥。

**对称算法和公开密钥算法**

基于密钥的算法有两种一般形式:对称的和公开密钥。对称算法,也称常用算法,是加密密

钥能从解密密钥求得或解密密钥能从加密密钥求得的算法。在许多对称系统中，加密密钥和解密密钥是相同的。这种算法，也称为保密密钥算法、单密钥算法或一密钥算法，需要发送者和接收者在他们通信之前协商密钥。这种密钥必须保密。对称算法的安全性依赖于密钥；泄密的密钥意味着任何人在这个加密系统中能加密和解密信息。

用对称算法的加密和解密表示为：

$$E_K(M)=C$$

$$D_K(C)=M$$

对称算法能划分为两类。一类称为流算法或流加密算法，另一类则是按组进行，在明文中每次操作一组比特。这些比特组称为块。这类算法称为块算法或块加密算法。对计算机上实施的算法，典型的块大小为 64 比特，大到可阻止破译，小到易于操作。在块和流算法中，加密和解密中使用相同的密钥（在用计算机之前，算法对明文通常每次操作一个字符。可认为这是字符流操作算法，也可认为 8 比特块的块操作算法。）。

公开密钥算法也称不对称算法。他们的设计使得应用于加密的密钥不同于应用解密的密钥。进而，解密密钥不能（至少不能在有限计数之内）从加密密钥中计算出。因为加密密钥为公开的，所以称为公开密钥系统：一个完全陌生的人能使用加密密钥加密信息，但仅拥有相应解密密钥者才能解密信息。在这个系统中，加密密钥常称为公开密钥，简称公钥。而解密密钥称为私有密钥或秘密密钥，简称私钥。

使用公钥 K 加密表示为：

$$E_K(M)=C$$

尽管公钥和私钥是不同的，但具有相应私钥的解密表示为：

$$D_K(C)=M$$

有时，信息将用私钥加密和用公钥解密，如数字签名。尽管可能混淆，这些操作仍分别表示为：

$$E_K(M)=C$$

$$D_K(C)=M$$

**密码破译**

密码术的主要目的是考虑到窃听者能完全拾取收发二者之间的通信信息情况下，实现安全信息传送。

密码破译则是无须取得密钥而能将密文信息恢复成明文的科学。密码破译成功，不仅恢复明文也可得到密钥。并且发现密码系统中导致上述结果的弱点。

一次破译也称一次攻击。破译中的基本假设是保安性全取决于密钥而破译员了解加密算法和实现的全部细节。实际上并非完全如此，这只是理想的假定。

有四种一般类型的攻击方法。当然他们中的每一种都假定破译员已有所用加密算法的全部知识。

1. 仅知密文攻击

在这种攻击中，密码破译员有几个信息的密文，所有的信息使用相同加密算法加密。为将相同密钥加密的信息解密，密码破译员会尽可能多地恢复信息的明文，或者更好地是导出用于加密信息的密钥。

已知：$C_1=E_k(P_1), C_2=E_k(P_2), \cdots C_i=E_k(P_i)$

导出：$P_1、P_2\cdots P_i、k$

或导出从 $C_{i+1}=E_k(P_{i+1})$ 得知 $P_{i+1}$ 的算法

2. 已知明文攻击

密码破译员不但利用几个信息的密文，而且有这些信息的明文。导出用于加密信息的密钥或用相同的密钥加密任何新的信息的解密算法。

已知： $P_1,C_1=E_k(P_1),P_2,C_2=E_k(P_2),\ \cdots\ P_i,C_i=E_k(P_i)$

导出： k 或导出从 $C_{i+1}=E_k(P_{i+1})$ 得知 $P_{i+1}$ 的算法

3. 选择明文攻击

密码破译员不但利用密文和涉及到的信息的明文，而且能选择加密的明文。这比已知明文攻击更强有力，因为密码破译员能选择专用的明文块加密，可能产生更多关于密钥的信息。导出用于加密信息的密钥或用相同的密钥加密任何新的信息的解密算法。

已知： $P_1,C_1=E_k(P_1),P_2,C_2=E_k(P_2),\ \cdots\ P_i,C_i=E_k(P_i)$

其中密码分析者选择 $P_1$、$P_2$ … $P_i$

导出： k 或导出从 $C_{i+1}=E_k(P_{i+1})$ 得知 $P_{i+1}$ 的算法

4. 自适应选择明文攻击

这是选择明文攻击的一个特例。密码破译员不但选择加密的明文，而且能依据以前加密的结果修改选择。在选择明文攻击中，密码破译员可以选择一大块明文加密；在自适应选择明文攻击中，选择一个较小的明文块，然后依据第一次的结果选择另一块，等等。

5. 选择密文攻击

密码破译员能选择不同的将要解密的密文和已解的明文，将它们放入一个自动解密的分解判别的工具箱中，导出密钥。

已知： $C_1,P_1=D_k(C_1),C_2,P_2=D_k(C_2),\ \cdots\ C_i,P_i=D_k(C_i)$

导出： k

这种攻击主要应用于公开密钥加密系统。选择密文攻击有时对对称算法一样有效。

6. 选择密钥攻击

这种攻击并不意味破译员能选择密钥。只不过破译员对不同密钥之间的关系有所了解。它较新奇和含混但并不实用。

7. 牛皮筋式破译

破译员威胁、写黑信或折磨某人直至给出密钥，或用金钱收买，所以也称购买密钥攻击，这已不是科学技术的内容了，但在现实社会中却也常有奏效。

已知明文和选择明文攻击比想象中用得更普遍。许多信息有密码破译员熟知的标准开始和结尾。源代码加密后仍易受攻击，因为规则地出现一些关键词如 #define、struct、else、return。加密可执行代码也有同样问题，如函数、循环结构等等。已知明文攻击成功的例子，在二次大战时对日本和德国的作战中都有记录。

讨论攻击时不要忘记我们的基本假定，破译员是熟知算法的。把密码系统的强度建立在算法保密上的想法是错误的。最好的算法，被世界级破译员攻击多年而仍未攻破的算法都已公开，还有什么可值得保密的算法呢？

密码破译员并不总有获得算法的机会，如二次大战中美国破译日本外交代码 purple 就是这样，但他们经常会得到算法。如果算法是使用在商业的保密程序中，花钱买反汇编程序就可揭开算法。如果算法是用于军事通讯系统，也很简单，花钱买设备或窃听然后恢复算法。

那些因暂时未被破译就简单地宣布拥有不可破译密码的人，不是天才就是傻瓜，不幸世界

上多是后者。夸耀算法优点但又拒绝公开，相信自己的算法万能的人，要当心。好的密码员会依靠同行评论区分出好的和坏的算法。

**算法安全性**

算法根据攻破的难易标定了不同的安全程度。如攻破某算法的费用大于加密数据的代价，该算法认为是安全的。如攻破某算法的时间长于数据的保密期，该算法也认为是安全的。同样如攻破某算法所需的数据量多于密钥加密的数据量，该算法仍认为是安全的。以上所说的安全并非绝对，因为在密码破译中新的攻破机遇频频发生，另一方面大部分数据的价值会随时间流逝而贬低。所以，安全的要点是数据的价值要继续保持低于攻破安全屏障所花的代价。

Lars Knudsen 按攻破算法难易的递降顺序，分类如下：

- 全攻破，密码破译员找到密钥 K，于是解密 $D_K(C)=M$。
- 全局推导，密码破译员找到另一算法 A，无须知道 K，因为 A 等价于 $D_K(C)$而解密。
- 局部推导，密码破译员找到窃听来的密文的明文而解密。
- 信息推导，密码破译员得到关于密钥信息或是有关明文格式的信息。利用这些信息而解密。

如果无论破译员有多少密文，仍无足够信息能恢复明文，这样的算法是无条件安全的。事实上只有一次一用的密码本是不可攻破的。其它所有密码系统在惟密文攻击下都是可以攻破的。简单的做法就是尝试所有可能的密钥，然后判断明文的意义，这也称蛮力攻击。

密码术更关心密码系统不能被计算机攻破，一算法认为是“计算”性地安全，指在有效资源下，无论现在或将来都是不能攻破的。后文将解释什么是“有效资源”。

也可以不同方式度量攻击的复杂性：

- 数据复杂性，为攻击所需数据的攻击量。
- 处理复杂性，执行攻击所须的时间，又称工作因子。
- 存储需求，做攻击所须的存储量。

攻击的复杂性取这些因素中的最小值。某些攻击涉及到三个因素的平衡折衷。较快的攻击往往花费较大的存储需求。

复杂性往往用数量级表示，如果算法处理的复杂度为 $2^{128}$，则攻破算法需要 $2^{128}$次操作，假定计算速度为 100 万次/秒，并由 100 万个这样的处理机来并行处理，还须 $10^{17}$年才能揭示密钥。这是宇宙年龄的 10 亿倍。

然而攻击复杂性是恒定的，而计算能力却不同，在本世纪的后半世纪它有着显著的进步而且没有理由认为会停止。平行机很适合用来作密码破译攻击。攻击任务被分成亿万个小片，处理机间不需交互作用。总之，简单地将因为现有技术的局限而未能攻破的算法宣称为绝对安全算法是危险的。设计好的密码系统时，必须预期计算能力经若干年的发展后，仍然是不可破译。

## 1.2 密写术

密写术是把密件隐藏在其它信息中而不觉察存有秘密的书写方法。一般发送者用一大片无关信息写在纸上然而把密件隐藏其中。过去采用过的技巧有不可见墨水，在选用的字符上带小针孔，手写字符间的微小差异，打印出来的字符上用铅笔做标记，格孔密写卡（将它覆盖在一张纸上从格孔中写入密件，然后在纸上余下部分填入其它字句，使它像一般信件）等等。

近来人们常把密件藏于图形、图像中，将图像信息每一字节的最低位替换成密件信息位。这样加工后的图像并无肉眼可知的变化，而密件却能安全地到达接受方。一个 1024×1024 灰度级的图像用这样的方法能存储 64K 字节的信息。有一些公开的用来做这种密写的加工程序。

Peter Wayner's 模拟函数(mimic functions)可将密件信息搅乱,这些函数修饰密件,使其统计面貌相似报纸分类内容,莎士比亚的剧本,互联网络的新闻。这种密写方法只对计算机扫视信息时奏效,而不能蒙混人眼。

## 1.3 替代加密和转移加密

在计算机出现之前,密码学包含的是基于字符的各种算法。不同的密码算法或是一字符替代成其他字符,或是一字符转置成其他字符。较好的算法则二者都进行并多次反复。

目前,事情更为复杂,但道理是一样的。主要的变化是算法实施于每一个二进位而不是一个字符。实际上这不过是"字母表"的大小有所变化:26 个元素变成 2 个元素。多数好的加密算法仍是把元素结合成一定大小进行替代和转置。

**替代加密算法**

替代加密算法是明文中的每一个字符用另一个字符替代形成密文。除接受者外其他人不理解其间的替代。接受者对密文作反向替代后恢复成明文。

在经典密码学中,替代加密算法有四种基本类型:

1. 简单替代加密算法或称单字符加密,明文每一字符被替代成密文中的相应字符。新闻密电就是用这种方法。

2. 同音替代加密算法,类似于简单替代加密算法,但明文中的单一字符能对应密文中的几个字符。例如"A"可能相应于 5、13、25 或"B"可能相应于 7、19、31 或 42 等等。

3. 多元替代加密算法,成块的字符加密成一组其它字符。如"ABA"相应于"RTQ","ABB"相应于"SLL"等等。

4. 多字母替代加密算法,由多次简单替代加密组成。例如用 5 次不同的简单替代加密,具体所用的次数随每一字符在明文中的位置而变化。

著名的凯撒加密算法是将每一明文字符用右移三位并以 26 为模的字符所替代(A 用 D 替代,B 用 E……W 用 Z、X 用 A、Y 用 B、Z 用 C 替代)。它是一个简单的加密算法。

ROT13 也是一个简单加密程序,通常可在 Unix 系统中找到它,每一字符移动 13 个位置,如 A 用 N 替代,B 用 O 替代等等。

用 ROT13 两次加密一个文件,则恢复成原文件。

M=ROT13(ROT13(M))

ROT13 并不着眼于安全性,它常用在网上公布一些带有冒犯性的文章以费人猜疑。

简单替代加密易于攻破,因为加密算法并不涉及明文不同字母的隐藏次数。密码破译者重建明文对每一个字母大约要试的是其它 25 个字母。

早在 1401 年,曼图亚的 Duchy,就采用了同音替代加密算法。它们比简单替代加密算法复杂得多,因而更难破译。但因为仍然没隐藏明文所有的统计特性,用已知明文攻击方法,很容易被攻破;用仅知密文攻击,会难一些,但对计算机也是几秒钟的事情。

多元替代加密算法将字母按组进行加密,例如英国在一次世界大战中采用的 playfair 算法。它是 1854 年发明的,一次加密一对字母。Hiu 算法也是一种多元替代加密算法。有时用 Hoffman 编码进行加密,那是不安全的多元替代加密。

在 1568 年,Leon Battisfa 发明的多字母替代加密算法,曾在美国内战中被北方军使用。尽管这种加密很容易被攻破,许多商业计算机安全产品都使用这种形式的算法(如 Word Perfect)。Vigenere 和 Beaufort 算法也是多字母替代加密算法的例子。

多字母替代加密算法有多个单字母密钥，每个密钥用来加密明文中的一个字母，第一个密钥加密第一个字母，第二个密钥加密明文中的第二个字母，依此类推。所有密钥用完之后，再循环使用。如果有 20 个单字母密钥，那么每 20 个字母将用相同的密钥加密。这称为密码的周期。在经典密码学中，周期长的密钥比周期短的密钥更难破译，但采用计算机技术，周期非常长的替代加密也能很容易被攻破。

运行密钥加密算法是这类算法的另一个例子。它用一个文本来加密另一个文本。尽管这样使密码的周期长达一个文本，但破译仍是轻而易举。

**转置加密算法**

转置加密后的密文有相同的字符长度，只是字符的次序改变了。简单的圆柱转置加密算法是将明文横着写在一张宽度固定的图纸上，然后垂直地读出即成密文，解密只不过是将密文竖着写在一张同样宽度的图纸上，垂直读出明文。如图 1.4 所示。

```
明文: COMPUTER GRAPHICS MAY BE SLOW BUT AT LEAST IT' S EXPENSIVE

                COMPUTERGR
                APHICSMAYB
                ESLOWBUTAT
                LEASTITSEX
                PENSIVE

密文: CAELP OPSEE MHLAN PIOSS UCWTI TSBIU EMUTE RATSG YAERB TX
```

图 1.4　圆柱互换加密算法

因为密文和明文的字母完全一样，对密文的频率分析表明每个字母出现的可能性几乎相同。根据这个很好的提示，密码破译员用各种技术试探出字母的真正排列，从而获得明文。将密文再转置一次，会大大提高安全性。但无论多复杂的转置加密，计算机几乎都能攻破译。

在第一次世界大战中，德国采用的 ADFGX 加密算法，是一种转置加密算法，它同时又采用了简单的替代加密。当时这已经是一个复杂的算法了，但还是被一名法国的密码破译员 Georges Painvin 攻破。尽管许多现代加密算法都采用转置加密，费事的是它需要大量存储空间。但有时要求信息只有一定长度。因而替代加密更为普遍。

**旋转机器**

在 20 世纪 20 年代，为完成自动加密，各种机械加密装置应运而生。它们根据旋转的概念，用机械旋转来完成一般的替代。

旋转机器由一个键盘和一组旋子组成来实现 Vigenere 加密算法。每一个旋子有 26 个位置，刚好是字母表的一个任意排列，完成一个简单的替代。例如，一个旋子用“F”替换“A”、“U”替换“B”、“L”替换“C”等等。同时，一个旋子的输出端栓在另一个旋子的输入端。

比如，一个旋子机器由四个旋子组成，第一个旋子将“A”替换成“F”，第二个将“F”替换成“Y”，第三个将“Y”替换成“E”，最后一个将“E”替换成“C”，那么 C 就是输出的密文。如果，某几个旋子转动一下，下一次的替代又将不同于前一次。

旋子与齿轮的转动使得机器安全运行，因为每一个旋子的不同转速转动，由 n 个旋子组成的机器周期为 $26^n$，有些旋转机器的每一个旋子上位置的数量不同，这样更让密码破译员伤透脑筋。