国外计算机科学经典教材

Data Privacy and Security

数据保密与安全

(美) David Salomon 著
蔡建 梁志敏 译

清华大学出版社

国外计算机科学经典教材

数据保密与安全

(美) David Salomon 著

蔡 建 梁志敏 译

清华大学出版社

北 京

Data Privacy and Security
David Salomon
EISBN: 0-387-00311-8

图书在版编目(CIP)数据

数据保密与安全/(美)萨洛蒙(Salomon，D.)著；蔡建，梁志敏译.—北京：清华大学出版社，2005.6
书名原文：Data Privacy and Security
(国外计算机科学经典教材)
ISBN 7-302-10444-1

Ⅰ. 数… Ⅱ.①萨… ②蔡… ③梁… Ⅲ. 密码术 Ⅳ. TN918

中国版本图书馆 CIP 数据核字(2005)第 009212 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969
组稿编辑：曹　康　　**文稿编辑**：徐燕萍
封面设计：康　博　　**版式设计**：康　博
印 刷 者：北京鑫海金澳胶印有限公司　　**装 订 者**：北京市密云县京文制本装订厂
发 行 者：新华书店总店北京发行所
开　　本：185×260　**印张**：23.5　**字数**：602 千字
版　　次：2005 年 6 月第 1 版　2005 年 6 月第 1 次印刷
书　　号：ISBN 7-302-10444-1/TP・7094
印　　数：1～4000
定　　价：42.00 元

前　言

1917 年 1 月 17 日，英国政府截获了一份德国的加密电报，随后这份电报按程序被送往英国密码署进行解密。大致浏览过电报内容后，英国的密码分析专家意识到这份电报可能是通过一种用于高级外交通信的密码进行加密的，于是他们立即着手进行解密工作。借助于过去得到的相似解密经验，数小时后，密码破译人员完成了对部分报文的解密。虽然只破译了部分报文，但是这部分内容已经清晰地说明了德国的一个秘密阴谋：计划阻止美国参加战争(即第一次世界大战)。随着这份电报的完全解密与美国政府和公众的关注，美国最终决定参加战争，因此，该电报极大地影响了世界历史。

这个事件在今天被称为“Zimmermann 电报事件”，该事件示例说明了密码术的重要性以及成功的加密和解密能够影响历史的发展。[Tuchman 85]和[Friedman 00]中详细讲述了 Zimmermann 电报的故事，不过在此我们只会简要介绍一下这个故事。

第一次世界大战于 1914 年 4 月爆发，当时的交战双方都希望在几个月内就能结束战争，但是这场战争最终却演变成为一场持续四年之久的世界大战，它夺去了成千上万人的生命，并且改变了世界的格局。在战争中的某个阶段，形势似乎变得对德国及其盟国有利，因此英国和法国试图说服美国加入对德国的战争。所有人都明白，凭借着美国强大的人力和物质资源，就能够确保打败德国，但是美国总统 Woodrow Wilson 却犹豫不决。Wilson 并不希望美国士兵为远在欧洲的战争付出生命，并且希望继续扮演调停者的角色并保持中立。甚至，在 1915 年 5 月发生了 Lusitania 客轮沉没事件，虽然有 1100 多人丧生(包括 124 名美国人)，但是美国仍然不愿意卷入这场战争。

然而，尽管美国一直保持中立，德国却越来越感觉到战争的不利因素，只有迅速击败英国才能赢得整个战争。因此，1917 年 2 月，德国政府决定对英国展开非常规的海战，也就是说使用潜水艇对英国海岸线附近出现的任何船只进行攻击。虽然这个决定并没有使美国卷入战争，但是德国仍然认为无论如何都要阻止美国在之后会加入这场战争，这正是 Arthur Zimmermann 计划考虑的问题。作为德国的首相，Zimmermann 提出了一个怂恿墨西哥从南部、日本从西部攻击美国的计划，他希望这些攻击能够使美国只能忙于保护自己国家的安全，从而保证德国能够主导并赢得在欧洲的战争。

Zimmermann 的计划是说服墨西哥总统 Venustiano 在德国的帮助下向美国发动夺回新墨西哥、德克萨斯和亚利桑那领土的战争，以及要求日本进攻美国。Zimmermann 相信，只要这份计划能够成功地付诸实施，就能够阻止美国向欧洲发兵和提供补给，这样德国及其盟国就能快速包围英国并取得胜利。

由于没有更加安全的传输通道，Zimmermann 只能通过电报来传送自己的计划。这份加密的电报从瑞典发送给在华盛顿的驻美德国大使 Johann von Bernstorff，并要求他再转送给驻墨西哥的德国大使 Heinrich von Eckhardt。德国人相信自己的密码是无法破译的(我们将看到这种想法是大错特错的)，但是英国人却轻易地破译了德国的密码，从而在整个战争期间截获了德国的许多消息，包括上面提及的这份电报。

在破译的电报内容被送给美国政府后，该电报通过舆论让美国公众了解到德国的阴谋。不过，人们当时对这份电报的真实性还有所怀疑，但是 Zimmermann 本人很快就给出了答案。当柏林新闻界向 Zimmermann 提出这个问题时，他承认了这份电报的真实性："是的，我无法否认。"美国舆论与国会立刻一片哗然，终于导致美国于 1917 年 4 月 6 日向德国宣战。随后，战争又持续了一年时间，最后双方在 1918 年 11 月 11 日签订了全面停战协议。

图 0-1 显示了这份加密的 Zimmermann 电报，下面是该电报的英文译文：

Berlin, January 19, 1917

On the first of February we intend to begin submarine warfare unrestricted. In spite of this, it is our intention to endeavor to keep neutral the United States of America.

If this attempt is not successful, we propose an alliance on the following basis with Mexico: That we shall make war together and together make peace. We shall give general financial support, and it is understood that Mexico is to reconquer the lost territory in New Mexico, Texas, and Arizona. The details are left to you for settlement.

You are instructed to inform the President of Mexico of the above in the greatest confidence as soon as it is certain that there will be an outbreak of war with the United States and suggest that the President of Mexico, on his own initiative, should communicate with Japan suggesting adherence at once to this plan; at the same time, offer to mediate between Germany and Japan.

Please call to the attention of the President of Mexico that the employment of ruthless submarine warfare now promises to compel England to make peace in a few months.

Zimmerman
(Secretary of State)

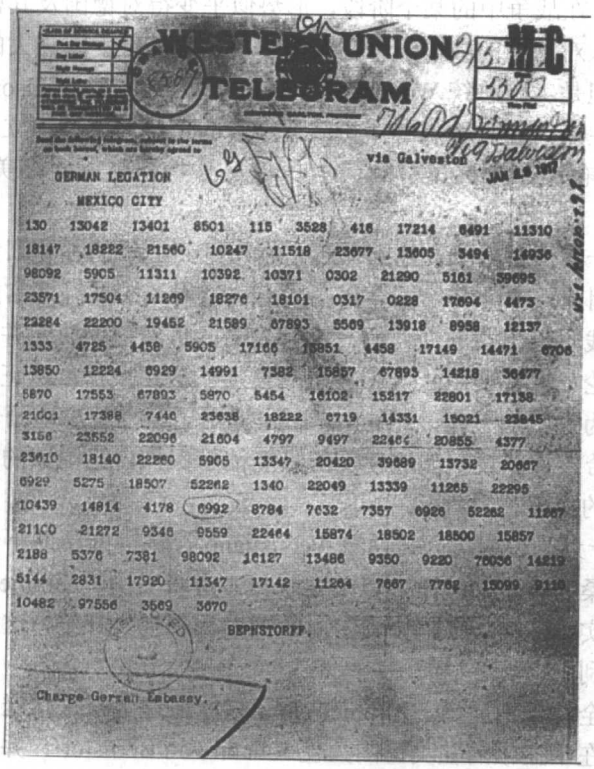

图 0-1 加密的 Zimmermann 电报

这是一个 Joam Dacosta 和他的人民都不希望看到的意外事件。实际上，正如那些没有忘记故事开始一幕的人们所意识到的那样，这份文档使用了密码术众多系统当中的某个系统进行了加密。

但是，究竟使用的是哪一个系统呢？

发现这个问题的答案需要运用人类的全部智慧。

——Jules Verne，Eight Hundred Leagues on the Amazon (1881)

0.1 基本概念

密码学(cryptology)是处理秘密记录和消息的学科，密码学以某种方式处理秘密记录和消息后，非授权的人要读懂这些记录和消息是非常困难的，甚至是不可能的。密码学分为密码术(cryptography)和密码分析学(cryptanalysis)，密码术是编写秘密消息或与数学锁和密钥相关的学科，密码分析学是破译加密消息的学科。在密码学的这两个分支中，从事具体工作的人分别被称为密码学家(cryptographer)和密码分析学家(cryptanalyst)。

隐写术(steganography)可以隐藏信息，而密码术则可以加密信息，密码术隐藏的是信息的含意，而不是信息本身。我们可以将密码术看作是用于公开秘密记录的学科，将隐写术看作是用于隐蔽秘密记录的学科。

术语“密码术”与“密码学”由希腊词汇 $\kappa\rho\upsilon\pi\tau o\varsigma$(意为“隐藏”)、$\gamma\rho\alpha\phi\iota\alpha$(意为“编写”)和 $\lambda o\gamma o\varsigma$(意为“消息”)衍生而来。术语“密码术”是由英国物理学家 Thomas Browne 在 1658 年首先提出的。

密码分析学的重要性在于密码术的一个基本定律，也就是任何安全的编码在通过暴露其所有弱点和错误的大型公开测试与跟踪之前都被认为是不安全的。

密码术具有以下四个主要要素：

- 机密性(confidentiality)。任何未授权者都无法理解经过加密的消息。
- 完整性(integrity)。可以检测存储介质或传输过程中对加密消息的任何更改或讹误。
- 不可抵赖性(nonrepudiation)。发送方不能抵赖先前生成或发送了加密消息。
- 身份验证(authentication)。发送方和接收方能够彼此确认对方的身份以及消息的起源和目的地。

本书的 8.8 节将详细讨论上述 4 个要素。

对于商人、统治者、将领以及他们的对手来说，安全的编码通常是同样重要的。政府发送给各地的消息必须预先进行加密，以防止泄露机密；同样，将领们发出的命令和公司高级职员发送的便函也需要先经过加密。不过从另一方面来说，对手总是会试图破译安全的编码。这样一来，经过密码学家(密码生成者)与密码破译者的共同努力，安全的编码不断得到发展和完善。在历史上不断出现新的安全编码，这些安全的编码又不断被破译，这就需要开发更新、更复杂的加密方法。进入 20 世纪以来，安全编码的发展更加迅猛，这是因为：(1) 两次世界大战；(2) 数学的发展；(3) 计算机的发展。

由于无线电通讯的快速发展，因此在现代生活中经常会遇到安全编码的问题。电话交谈有时会通过通信卫星进行传输，电子邮件消息在到达目的地之前可能会通过许多计算机，这样一来，我们的私人通信信息很容易被截获。因此，我们总是希望在进行私人通信时使用密码。商业和其他贸易企业主要依赖于发送和接收消息，所以它们同样需要安全的通信。另一方面，安

全代码的广泛使用也困扰着执法机构，这是因为一旦犯罪分子(有组织的或没有组织的)和恐怖分子开始意识到保密通信的用途，他们也可能会使用安全的编码。

压缩和密码术之间存在一个鲜为人知的连接。生成密码的一个古老而传统的方法是密码本(codebook)。密码本由一个常用词汇和短语列表组成，这些词汇和短语分别与其编码的某个保密短字相关联。密码本在加密消息的同时也会压缩消息。用短词汇替代长词汇甚至整个短语非常重要。在电报被普及使用的时期，发送一份电报的花费是由电报中的词汇或字母数决定的。一个使用定制代码本的大型贸易企业能够显著地节省在电报上的开支。随着计算机的出现与发展，压缩变得更加重要。加密压缩的消息可以加快消息的传输速度，并且还会使密码破译者难以破译这些消息。即使密码分析学家知道或怀疑到消息的加密方式，甚至是能够知道或猜测出使用的正确密钥，对加密消息进行解密后得到的结果仍然是难以理解的，无法达到预期目的的攻击者还可能放弃实际上正确的攻击方式。

如图 0-2 所示，密码术被分成编码和密码。术语“编码(code)”指的是替代词汇、短语或整条消息的代码，而术语“密码(cipher)”则指的是替代每个符号的代码。例如，军队可能约定使用代码字“green”来表示“attack at dawn”，约定使用代码字“red”来表示“retreat immediately”。在这里，词汇“green”和“red”就是编码。如果经过仔细的设计和使用，编码可能无法被破译，不过由于编码必须对所有可能的偶然性做出一致性的约定，因此编码的使用存在局限性。另一方面，密码是一个规则，这个规则讲述了对消息中每个字母进行编码的方法。例如，如果我们约定使用字母表中每个字母后面的第 2 个字母来代替原始的这个字母，那么消息“attack at dawn”就会被编码为“cvvcem cv fcyp”或更秘密的“cvvcemcvfcyp”。密码是通用的，不过却比编码更容易被破译。在实际运用中，我们使用的是术语“code”和“codebreaker”，而不是更为准确的术语“cipher”和“cipherbreaker”。

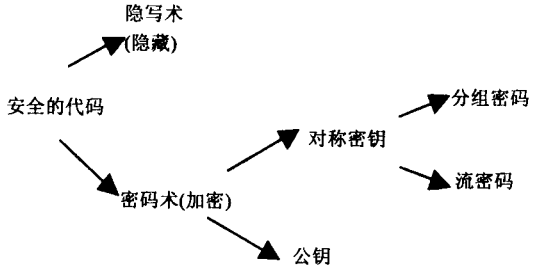

图 0-2　安全编码的术语

此外，编码和密码也可以组合在一起，这样的组合被称为代码本(nomenclator)。消息的一部分可以使用编码进行加密，不存在编码的剩余部分则使用密码进行加密。

任何加密算法都必须容许解密，而解密又必须是惟一的(不过本书 8.4 节介绍了一个罕见的特例)。加密通常也是惟一的，不过也存在一些特例，其中一个特例是本书 1.7 节将要介绍的同音替代密码(homophonic substitution cipher)。

术语“字母表(alphabet)”指的是消息中包含的符号集合，它可以是比特集合(0 和 1 这两个值)，可以是 26 个字母的集合，可以是 26 个字母加上空格、一组字母、数字和标点符号的集合，可以是 128 个 ASCII 码的集合，可以是 256 个字节值的集合，还可以是其他任何形式的集合。

加密算法将消息作为明文(plaintext)输入，并以密文(ciphertext)输出消息。明文和密文可以

使用相同的字符(它们可能使用相同的字母表)，也可以使用不同的字符集合(例如明文使用字母集合，而密文则可能包含数字)。

传统的编码用户在加密明文之前会删除明文中的空格和标点符号。删除空格有时会导致模糊，如删除“week nights”和“wee knights”中的空格，删除“the rapists”和“therapists”中的空格。同样，删除连接号也可能会导致模糊，如短语“four thousand year old mummies”可以被解释为“four-thousand-year-old mummies(有4000年历史的木乃伊)”、“four-thousand year-old mummies(4000个有一年历史的木乃伊)”和“four thousand-year-old mummies(四个有千年历史的木乃伊)”。

此外，以五个符号为一组来书写密文也是一个传统的方法，这个传统方法起源于某些基于五字符组的老式电报系统。

为了描述发送秘密消息的加密/解密算法，通常使用一般的名字Alice和Bob来代替收发秘密消息的A和B；如果加密/解密算法涉及到防范偷听者，通常将偷听者称为Eve。这已经成为一个惯例。[Conceptlabs 01]中介绍了对Alice和Bob的描述(该书的第195页还提供了方框图)。

有一个非常流行的说法：第一次世界大战是化学家的战争(这是因为首次大规模使用了毒气)，第二次世界大战则是物理学家的战争(这是因为原子弹的使用)。同样地，第三次世界大战(我们希望不要爆发)可能会是数学家的战争，这是因为，要赢得战争，最终可能取决于安全代码的使用和破译。

在遍及全球的大学和研究所中，研究员们公开完成了一些编码的开发和破译([Flannery 01]介绍了一个与众不同的示例)，这些工作通常是得到同意的。不过，编码开发和破译领域的大多数工作是由政府机构秘密进行的，其中，最著名的两个机构是美国的国家安全局(National Security Agency，简写为NSA)和英国的政府通信总局(Government Communication Headquarters，简写为GCHQ)。

对消息进行加密涉及两个组成部分：算法和密钥。目前存在许多知名的加密算法，不过每种算法的结果都取决于所选择的密钥。最简单的加密算法示例可能是字母移位。这种算法非常简单，加密消息时，我们会使用字母表中每个字母后面的第n个字母(循环移位)来代替这个字母，此时密钥就是数值n。下面列出了n=3的一个示例(注意Y被替换为A)：

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ␣
DEFGHIJKLMNOPQRSTUVWXYZ␣ABC
```

其中，第一行是明码字母表(plain alphabet)，第二行则是密码字母表(cipher alphabet)。

0.2 Caesar密码

前面刚刚介绍的这种简单移位密码被称为Caesar密码，这是因为Julius Caesar在他的作品*Gallic Wars*(高卢战记)中首先介绍了这种密码。Caesar密码是一个替换算法示例，在替换算法中，每个字母都被替换为不同的字母(有时可能不变)。许多加密算法都基于某种替换类型。一个非常保密的简单替换算法示例是图书密码(book cipher)，这种密码会选定一本图书，并随机选定一页作为密钥，这页上的单词被编上号码，并提供了一个表格，该表格列出了每个单词的第一个字母以及这个单词的号码，随后这个编码表可以被用于加密消息，方法是使用编码表中的号码来替换每个字母。例如，选定页中存在下面一段话：“[1]numbered [2]and [3]a [4]table [5]is [6]prepared,

[7]with [8]the [9]first [10]letter [11]of [12]each [13]word [14]and [15]the [16]word's [17]number. [18]This [19]code [20]table [21]is [22]later [23]used [24]to [25]encrypt [26]messages [27]by [28]replacing [29]each [30]letter [31]of [32]the [33]message [34]with [35]a [36]number [37]from [38]the [39]table。”，消息“NOT NOW”可以被编码为 36|31|20|17|11|13(也可以被编码为其他形式)。如果消息较短，并且每条消息都使用不同页，这种简单的编码就非常保密，不过我们必须预先约定不同的页码号，这在许多情况下又显得不合时宜。

> Cicero 与其同党也使用 Caesar 密码来传递机密消息，也就是改变字母的顺序使其他人无法理解消息的含义。如果要破译和理解这些机密消息，就必须使用字母表中的第 4 个字母 D 来替代字母 A，依此类推。
>
> ——Seutonius，*Lives of the Caesars*，LVI

ROT13(Rotate 13 的简写)是密钥为 13 的 Caesar 密码，它在 1984 或 1985 年被引入到 Internet 社区中。ROT13 被用于暂时隐藏难题的答案或模糊违禁的素材(如幽默新闻组中的黄色笑话)。选择 13 作为密钥是因为 13 恰好是英语字母表的一半长度，也就是说加密和解密 Rot13 是完全相同的。下面列出了明码字母表和 Rot13 字母表：

明码字母表　　ABCDEFGHIJKLMNOPQRSTUVWXYZ
Rot13 字母表　　NOPQRSTUVWXYZABCDEFGHIJKLM

使用 Rot13 时，消息“AND THE ANSWER IS RED”会被加密为“NAQ GUR NAFJRE VF ERQ”。

0.3 仿射密码

Caesar 密码被认为是一种加法密码，这是因为对一个字母进行编码时，我们会对该字母的数字值和常数 *a*(即密钥)进行以 26 为模的加法。此外，还可以使用乘法密码，在乘法密码中，通过对明文字母的数字值和密钥 *m* 进行以 26 为模的乘法，明文字母就会被转换为密文字母。

要分析密钥 *m* 的作用非常容易。假定为 26 个字母指派从 0(用于 A)到 25(用于 Z)的数字值。如表 0-1 所示，当每个字母都与密钥 *m*=2 进行以 26 为模的乘法时，某些字母会在结果中出现两次，而其他字母则不会在结果中出现；当每个字母都与密钥 *m*=3 进行以 26 为模的乘法时，得到的密文中含有每个字母，这些字母只出现一次。因此，对于密钥 *m* 来说，值 2 是一个不太好的选择，而值 3 则是一个好的选择。通常，好的 *m* 值都与 26 互质(relatively prime)，也就是以下 12 个数值：1，3，5，7，9，11，15，17，19，21，23 和 25。术语“互质”指的是两个整数不含有公共的质因子，或者说二者的最大公约数(greatest common divisor，简写为 gcd)为 1。

表 0-1　乘以 2 和乘以 3 后得到的字母值

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

练习 0.1：很显然，所有乘法密码都会将“a”转换为“A”。在乘法密码中，还有其他哪些字母仍然会被转换为自身，其原因何在？

我们可以将乘法密码表示为 $y=x \cdot m \bmod 26$，并且存在 12 种这样的密码(包括没有多大价值的、$m=1$ 的乘法密码)。接下来，我们将加法密码和乘法密码组合为仿射密码(affine cipher)，这个仿射密码被定义为 $y=[(x*m)\bmod 26+a]\bmod 26$，根据模数函数的属性，它可以被进一步定义为 $y=(x*m+a)\bmod 26$。因为加法密码的密钥 a 可以取从 0～25 的 26 个值，所以仿射密码的总数为 $12\times26=312$，虽然这个总数并不是很大，但是如果不算上节假日，在一年中的每一天应用一种密码都显得绰绰有余。仿射密码的密钥是密钥对(m, a)。

(在几何学中，空间的仿射变换将直线变换为直线和一个 $y=mx+a$ 的直线关系式，这就是“仿射密码”名称的来源。)

如果一个整数 n 的质因数分解为 $P_1^{e1}P_1^{e2}\cdots P_e^{ek}$，那么 Euler 函数 $\Phi(n)$可以计算与 n 互质的整数个数：

$$\Phi(n)=\Pi_{i=1}^{k}\left(P_i^{e_i}-P_i^{e_i-1}\right)$$

例如，整数 126 的质因数分解为 $2*3^2*7$，因此 $\Phi(126)=(2^1-2^0)(3^2-3^1)(7^1-7^0)=36$。同样地，$\Phi(26)=(2^1-2^0)(13^1-13^0)=12$。对于给定的一组要加密的 n 个符号来说，仿射密码的总数就是 $n*\Phi(n)$。

练习 0.2：在定点仿射密码中，某些字母被加密后保持不变。对于 26 个字母的使用来说，有多少密钥生成的仿射密码不是定点仿射密码？

模运算具有许多有意思且有用的属性，其中一个属性是等同性(identity)，即

$$([(x\times m+a)\bmod 26]\times n+b)\bmod 26=[x(m\times n)+(a\times n+b)]\bmod 26$$

等同性意味着使用两种仿射密码进行两次加密的效果只相当于进行一次加密的效果。

要解密仿射密码，需要使用 Euclid 算法来计算两个整数的最大公约数。给定两个不同的整数 r_0 和 r_1，Euclid 算法会计算 $\gcd(r_0,r_1)$。下面将要介绍的示例可以轻易地说明 Euclid 算法。如果 $r_0=20$ 和 $r_1=6$，就会执行下列步骤：

$$20=3*6+2 \rightarrow \gcd(20,6)=\gcd(6,2)$$
$$6=3*2+0 \rightarrow \gcd(6,2)=\gcd(2,0)=2$$

Euclid 算法可以被总结为下面的步骤：

输入 r_0、r_1

$$r_0=q_1\times r_1+r_2,\ \gcd(r_0,r_1)=\gcd(r_1,r_2)$$
$$r_1=q_2\times r_2+r_3,\ \gcd(r_1,r_2)=\gcd(r_2,r_3)$$
$$\vdots$$
$$r_{m-2}=q_{m-1}\times r_{m-1}+r_m,\ \gcd(r_{m-2},r_{m-1})=\gcd(r_{m-1},r_m)$$
$$r_{m-1}=q_m\times r_m+0,\ \gcd(r_0,r_1)=\gcd(r_{m-1},r_m)=r_m$$

其中，余数为 0 表示是最后一个步骤。

接下来，我们要研究这种算法的扩展。扩展的 Euclidean 算法能够解决这样的问题：给定两个整数 r_0 和 r_1，找出另外两个整数 s 和 t，使 $s*r_0+t*r_1=\gcd(r_0,r_1)$。这种扩展的算法利用了 Euclid 算法每次迭代中的当前余数 r_i 的表示形式：$r_i= s_i*r_0+t_i*r_1$。最后一次迭代被表示为 $r_m= \gcd(r_0,r_1) = s_m*r_0+t_m*r_1=s*r_0+t*r_1$。扩展的 Euclidean 算法可以被递归表示为：

$$s_0=1，\ t_0=0$$
$$s_1=0，\ t_1=1$$

在 $i=2，3，\cdots$ 时，重复执行 $s_i=s_{i-2}-q_{i-1}s_{i-1}$，$t_i=t_{i-2}-q_{i-1}t_{i-1}$。

例如，在 $r_0=126$ 和 $r_1=23$ 时，我们可以计算扩展的 Euclidean 算法如下：

$$126 = 5*23+11，\ t_0=0$$
$$23 = 2*11+1，\ t_1=1$$
$$11 = 11*1+0，\ t_2=0-5*1=-5，\ t_3=1-2*(-5)=11$$

只要记住这种扩展的 Euclidean 算法，解密仿射密码就非常容易。根据等式 $y=(x*m+b) \bmod 26$，可以得出 $x=[m^{-1}(y-b)] \bmod 26 =[m^{-1} \bmod 26][(y-b) \bmod 26]$，此时扩展的 Euclidean 算法能够被用于计算 $m^{-1} \bmod 26$。

练习 0.3：查找用于等式 $y=x*23+7 \bmod 126$ 的解密规则。

图 0-3 显示了一个用于仿射密码的 Matlab 函数。如果调用“affine ('home sweet home', 3, 1)”，则会生成“wrln dpnng wrln”。

```
function msg=affine(msg,m,a)
l=length(msg);
for i=1:l,
  x=msg(i);
  if((x>='a')&(x<='z')),
    x=x-'a';
x=rem(x*m+a,26);
if(x<0) x=x+26; end;
msg(i)=x+'a';
  end
end
```

图 0-3 一个用于仿射密码的 Matlab 函数

0.4 一次一密

一次性密码是一种理想的密码，并且是绝对安全的。但是，由于分配长密钥相当困难，因此一次性密码的使用具有局限性。当然，保证密码的绝对安全非常重要，所以本节将讨论术语“绝对安全(absolutely secure)”的含义。首先，我们将介绍密码系统的概念。

密码系统由一种算法、用于该算法的所有可能密钥以及所有可能的明文和密文组成。通常，明文的数量是无限的，不过我们总是认定一个密码系统具有有限的明文数。一个简单的示例是练习 0.2 介绍的具有 168 个密钥的定点仿射密码：我们可以选择任何书籍作为密文，其中，每本书是一个明文；对于每个明文来说，都存在 168 种密文。

为了便于讨论，我们选定 x、y 和 z 作为明文，选定 a、b、c 和 d 作为密文。明文和密文的集合被分别表示为 P 和 C，并且这两个集合的大小被分别表示为$|P|$和$|C|$。随后，我们还设定加密算法 f 具有三个可能的密钥 k_1、k_2 和 k_3。这个密码非常简单，通过列出每个明文使用不同密钥得到的相应密文，我们可以完整地描述该密码。表 0-2 显示了所有可能的加密操作(或映射)。

表 0-2　一个简单的密码系统

k_1	$x \rightarrow a$	$y \rightarrow b$	$z \rightarrow c$
k_2	$x \rightarrow a$	$y \rightarrow d$	$z \rightarrow b$
k_3	$x \rightarrow a$	$y \rightarrow c$	$z \rightarrow a$

此外，也可以使用函数记号来表示一个映射。例如，$f_1(x)=a$ 表示使用密钥 k_1 将明文 x 加密为密文 a。在这个示例中，对应于三个不同的密钥，存在三种映射：f_1、f_2 和 f_3。所有映射的集合被表示为 F。

显而易见，密码系统必须具有惟一解密消息的能力。从数学的角度来说，这意味着 f 必须具有可逆的 f^{-1}，这样对于 P 中的任何明文 w 来说，$f_i^{-1}(f_i(w))=w$。理解这一要点后，我们可以用三元组(P, C, F)来表示密码系统 S，其中 F 是可逆函数集合。惟一解密的需求指的是对于给定的一个密钥来说，C 中的任何一个元素都只能是 P 中一个元素的密文；另一方面，两个不同的密钥可以将 P 中的同一个元素映射为 C 中的不同元素。因此，集合 C 会大于集合 P(如上面的示例所示)。

一旦掌握了密码系统的概念，我们就可以考虑如何保证系统的绝对安全。从表面上看，术语“绝对安全”意味着即使有足够的时间和资源，密码分析学家仍然无法获取密码系统的知识(无法检查每个密钥)。这里会使用到概率知识，首先要讨论的概念是明文的概率。我们将明文 t 的概率表示为 $p(t)$，并通过一些示例来阐述 $p(t)$的意义。

在第一个示例中，明文集合 P 由 26 个字母组成，由于每个字母都是一个明文，因此明文“a”的概率就是字母“a”的概率(即表 1.1 中给出的 7.6%)。在第二个示例中，明文是字母组，明文“th”的概率 p(th)就是这个双字母组合的概率(3.7%)。上述数值是广为人知的，并且是这些明文的先验(priori)概率(该概率是理论值)。

试图解密特定的密文 c 时，密码分析学家原则上可能会比较每个明文 t，并且计算或估计出 c 是明文 t 通过某种特定加密算法所得加密结果的概率。我们使用 $p_c(t)$来表示这些概率，这些概率被称为后验(posteriori)概率(该概率是测量值)。接下来将介绍一些示例。

先来看第一个示例。我们假定明文是 26 个字母，并且使用 Caesar 密码进行加密操作。Caesar 密码具有 26 个可能的密钥，因此任何给定的密文 c 可能对应于 26 个明文 t 中的任一个明文。图 0-4 显示了三个明文(“s”、“t”和“y”)使用不同密钥分别得到的 26 个密文(每个箭头上的数字表示所使用的密钥)。

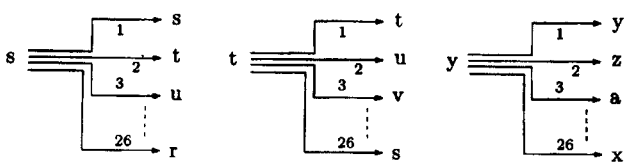

图 0-4　一个简单的密码系统

在这个示例中，每个密文 c(单个字母)可以是任何明文的加密结果。此外，密文 c 是“a”、“b”或其他明文加密结果的几率是相同的。这样一来，因为“a”在明文中出现的概率是 7.6%，所以“a”的加密结果密文 c 的概率也应当是 7.6%。因此，在第一个示例中，如果给定密文 c，对于任何明文 t 来说，$p_c(t)=p(t)$始终成立。

在第二个示例中，每个明文由一本未指定书籍某页上的前 100 个字母组成，明文$|P|$的大小等于这本书的页数，加密算法同样是 Caesar 密码。与图 0-4 相当的这个密码系统具有$|P|$部分，每一部分对应于一个明文。每个明文的概率是 $1/|P|$。每个明文具有与之相对应的 26 个密文，每个密文同样也是 100 个字母的分组。给定一个密文 c，通过简单地比较该密文与 P 中所有明文的字母分布情况，就能够轻易地确定具体的明文 t。如果密文 c 是特定明文 t 的加密结果，则 $p_c(t)=1$，但是如果明文 $q\neq t$，则 $p_c(q)=0$。因此，我们可以得出这样的结论：在这个示例中，$p_c(t)\neq p(t)$。

从第二个示例得出的结论非常简单。给定一个密文 c，密码分析学家会检查许多明文 t。对于某个明文 t 来说，如果发现 $p_c(t)>p(t)$，密码分析学家就会知道需要进一步分析密文 c 和明文 t 之间可能的对应关系；另一方面，如果发现 $p_c(t)<p(t)$，密码分析学家就能够确定这个特定明文 t 与指定密文 c 相对应的概率非常小，从而不需要进一步的分析。在上述两种情况下，密码分析学家都能够获取与这个密码系统相关的有用信息。这样一来，我们就可以认定：$p_c(t)=p(t)$的情况无法为密码分析学家提供任何有用的信息，这样的密码系统是最安全的密码系统。因此，我们规定满足 $p_c(t)=p(t)$条件(也就是对于任何密文 c 和明文 t 来说，先验概率和后验概率相等)的密码系统是绝对安全的。

每个明文都是单个字母的示例满足 $p_c(t)=p(t)$条件，所以它是绝对安全的。给定一个密文字母 c，我们无法能够确定相应的明文字母 t。

对于判断密码系统是否绝对安全来说，上述标准是一个充分条件，但是却很难识别任何给定的密码系统。在实际运用中，我们需要必要或充分、并且易于识别的标准，这样的一组标准能够轻易地确定给定的密码系统是否绝对安全。第一个标准显而易见：如果规定密码系统 S 绝对安全，那么任何明文都可以使用不同的密钥被加密(映射)为 S 中的所有密文。我们可以对图 0-4 稍作修改，左边的每个明文都必须与右边的所有密文存在对应关系(每个密文至少对应一个明文)。

我们很容易看出这个标准是必要标准的原因。假定密文 c 和明文 t 属于某个绝对安全的密码系统 S。因为 S 是绝对安全的，所以它满足 $p_c(t)=p(t)$条件。$p(t)=0$ 的情况意味着 t 并不存在，因此 $p(t)$必须为正，同样，$p_c(t)$也必须为正，也就是说至少存在一个密钥能够将明文 t 映射为密文 c。

因此，对于给定的密码系统 S 来说，如果观测到某个明文 t 不能使用任何密钥被映射为密文 c，我们就可以确信 S 是绝对安全的。

第二个标准规定：如果 S 绝对安全，那么$|F|\geq|C|\geq|P|$。前面已经介绍过，$|C|$总是大于$|P|$。为了理解 S 同样必须满足$|F|\geq|C|$的条件，我们将重点介绍一个特定的明文 t。第一个标准规定通过使用不同的密钥，明文 t 应当被映射为每一个密文 c。由于存在$|C|$个密文，因此我们也需要同样数目的密钥来映射明文 t。其他密文可能使用相同的密钥，不过也可能需要更多的密钥，因此密钥数$|F|$必须大于或等于密文数$|C|$。

第三个标准是充分条件，这个标准规定：在密码系统 S 中，如果$|F|=|C|=|P|$、所有密钥的使用概率相等，并且对于任何明文和密文对来说，都只存在一个密钥将 t 映射为 c，那么 S 就是

绝对安全的。图 0-5 示例说明了一个这样的密码系统。

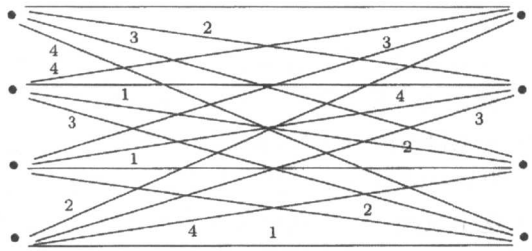

图 0-5　一个简单的密码系统

一次一密就是针对上述这些讨论提出的，一次一密是一个重要的、实用的和绝对安全的密码系统。假定每个明文都是 n 个字母的字符串，集合 P 由所有 26^n 这样的字符串组成。选择 P 作为密钥集合，也就是说$|F|=|P|$并且每个密钥都是 n 个字母的字符串。我们以相等的概率从 26^n 个密钥中选择其一。加密规则是：逐字母地读取明文和密钥。使用密钥字母 k_i 对明文字母 a_i 进行加密时，需要转动字母表使其从 k_i 开始，同时选中在原始位置 a_i 发现的字母。例如，如果当前的明文字母和密钥字母分别为“m”和“d”，就需要将字母表向左转动三个位置生成如下所示的新字母表，同时将“m”加密为字母“p”(“m”右移三个位置即为“p”)：

```
defghijklmnopqrstuvwxyzabc
```

上述这个密码满足了第三个标准，这是因为：(1)三个集合 F、C 和 P 是相同的；(2)所有密钥的使用概率相等；(3)对于任何明文和密文对(t,c)来说，都只存在一个密钥将 t 映射为 c。鉴于选中每个密钥字母的方式，因此密钥是独特的。如果在位置 i 的明文字母和密文字母分别为“m”和“p”，那么密钥字母 k_i 在字母表中的位置应当是字母“m”和字母“p”之间的位置差异，这个位置差异为 4，所以 k_i 是字母表中的第四个字母“d”。

练习 0.4：说明如何解密这个密码系统中的消息。

接下来，我们将介绍“一次一密”的概念。一次一密是 G. Vernam 在 1917 年首先提出的，因此有时也被称作 Vernam 密码(请参看附录之后的“密码术时间表”)。过去，人们会在纸上写满随机的字母，每页纸被用于只对消息进行一次加密(在接收方则用于解密)，随后这页纸会被销毁。对 n 个字母组成的明文进行加密操作时，这些明文字母被替换为密钥中后续有效的 n 个随机字母，密钥中的剩余部分则继续用于加密其他明文。这是一个非常安全的密码系统，不过它要求大密钥的安全分发，而且在许多情况下不太实用。例如，第二次世界大战期间，在布莱切利公园(Bletchley Park)工作的密码破译人员使用一次一密将破译的德国情报发送给白金汉宫里的英国政府机关(参见 5.4 节)。Shannon 在他的经典论文([Shannon 49]和[Shannon 51])中已经验证了一次一密所提供的绝对安全性。

在现今的计算机时代中，这个密码操作的是比特(而不是字母)，此时用于加密和解密的规则更加简单(参见 6.2 节)。通过使用移位寄存器生成很长的伪随机比特序列，人们已经解决了密钥分发问题。

> 人类一定能够解决编造的密码所存在的问题。
>
> ——Edgar Allen Poe

0.5 Kerckhoffs 原则

密码术完全基于一个重要的假定：某些信息能被安全地保存和传播，并且只有授权用户才能访问这些信息。这些信息就是加密算法所使用的密钥(key)。

荷兰语言学家 Auguste Kerckhoffs von Nieuwenhoff 提出了一个密码术中的重要原则(参见[Kerckhoffs 83])，该原则声明加密消息的安全性应当取决于密钥的秘密性，而不是取决于算法的秘密性。人们普遍接受了这个原则，该原则意味着一个算法应当具有许多可能的密钥，这个算法的密钥空间(key space)必须非常大。例如，由于只存在从 1～26 的 26 个密钥，移位 27 次就会得到原始明文，并且移位 27+n 次相当于移位 n 次，因此 Caesar 密码非常脆弱。需要注意的是，大密钥空间是必要条件而不是充分条件。在某些情况下，一种算法可能具有极大的密钥空间，但是实际上可能仍是脆弱的。

Kerckhoffs 原则

我们应当假定对手知道加密数据所使用的方法，数据的安全性应当取决于密钥的选择。这并不是说必须公开加密方法，而是因为加密方法在其出现时已经是公开的。

——Auguste Kerckhoffs

使用穷举方法可能破译一种密码。意图明确的密码破译者可以简单地搜索整个密钥空间中的所有可能密钥！但是，有两个因素会使这种穷举搜索方法变得不实用和存在局限性。第一个因素是大量的密钥，另一个因素则是通过猜测密钥识别出正确明文的问题。表 0-3 列出了检查密钥长度为 n 的全部密钥所花费的时间，这张表显示了一秒钟检查 1M 或 1G 个密钥所耗用的时间。显然，密钥长度每增加一位，密钥总数会增加两倍。事实上，对于 n 比特长度的密钥来说，密钥总数为 2^n，并且随 n 的变化呈指数变化。识别出正确的明文并不容易。如果明文是文本，那么通过查找字典中的词汇，我们使用一个程序还可能识别明文。如果人为地在文本中插入许多无意义的词汇，这种方法就会毫无用处，更不必说明文可能是压缩数据，可能是含有可执行机器代码的文件，还可能是图像、视频或音频数据。实际上，上述这些类型的明文几乎是无法识别的。

表 0-3 某些密钥长度所提供的安全性

密钥长度	近似密钥总数	测试所有密钥的时间	
n 比特	(十进制)	每秒测试 1M 个密钥	每秒测试 1G 个密钥
32	4.3×10^9	4096 秒	4 秒
40	1.1×10^{12}	291 小时	1024 秒
56	7.2×10^{15}	2179 年	777 天
64	1.84×10^{19}	557845 年	545 年
128	3.4×10^{38}	10^{25} 年	10^{22} 年

练习 0.5：密码学家经常会反驳这样的观点："只要搜索整个密钥空间，就总是能够破译加密的消息。借助于一台高速的计算机，我们可以非常容易地检查所有 64 比特长度的密钥。

除此之外，第一次完整的检查就能够取得成功。”使用现实生活中的示例说明这种观点的谬误之处(参见练习 7.5)。

最后，我们要列出一些与密码和隐写相关的资源。首先，我们为普通读者提供了一份书籍清单，这些书大部分是介绍密码术的通俗读物，另外一些则重点讨论特定的主题。需要注意的是，目前介绍密码术及相关主体的书籍过于泛滥，因此这里列出的清单代表了作者的观点。除了这些书籍之外，我们还应当提及一个专业出版社：[Aegean Park 01]，该出版社专门出版与密码术相关的书籍。

- [Kahn 96]：非常全面地回顾了从古代到 20 世纪 50 年代的密码术历史。原作已经绝版，不过最新的修订版简略地介绍了 20 世纪 50 年代以后密码术的发展概况。
- [Bauer 00]：介绍密码术的通俗读物。该书假定读者只具备初等数学知识，并且介绍了密码学历史上许多扣人心弦的、有趣的故事。
- [Gaines 56]：介绍较早的密码术方法(不借助于计算机)的通俗读物。该书包括提示、示例以及许多表格，这些表格说明了不同语言的字母频率、首字母和末字母频率以及最常用的英语词汇。这是原版(1939 年)的 Dover 版本。
- [Hinsley and Stripp 92]：记录了第二次世界大战期间在布莱切利公园(Bletchley Park)工作的密码破译人员所叙述的 27 个故事。该书从非技术的角度描述了密码破译的一些故事。
- [Johnson et al. 01]：讲述了数据隐藏和标识技术、隐写术和水印信息的破译方法以及防范此类攻击的对策。
- [Katzenbeisser et al. 01]：介绍信息隐藏(隐写术和水印)的优秀读物，该书覆盖了大量的主题。
- [Levy 01]：讲述了现代密码术的故事。这本书籍收录了 20 世纪后期从事密码术工作的相关人员的访谈记录。该书条理清晰，适于阅读，并且勾勒了整个密码术领域及其主要人物的全景图，其中最引人深思的描述是个别密码学家与不同政府之间的冲突。
- [Newton 97]：是一本百科全书。这本专论提供了根据字母顺序排列的 550 个条目，概述了从古代历史到现代电子媒体的编码技术。这些条目有的只有很短一个句子，有的则有几页篇幅。
- [Konheim 81]：针对不大了解密码学的读者而编写。该书篇幅不长，提供了密码分析学领域的基本知识。
- [Savard 01]：用于安全代码的联机参考手册。
- [Schneier 95]：通俗易懂，从实际出发详细介绍了现代密码术的所有主题。它是非常优秀的、具有 1500 多个条目的详细文献目录。
- [Schneier 02]：Bruce Schneier(一位重要的安全专家)负责编著的，与计算机安全性相关的时事通讯月刊。
- [Sinkov 80]：以详细、通俗易懂的方式讨论密码术的基础知识。该书每一章中的示例和练习为读者提供了所介绍概念的实践指南。
- [Stallings 98]：这是一本介绍密码术的优秀书籍，它重点讲述了算法(而不是密码破译)。该书详细讨论了公钥加密方法。

下面列出了一些重要的负责密码和密码术的政府部门：

- 英国的政府通信总局(Government Communication Headquarters[GCHQ 01])。

- 美国国家安全局(National Security Agency[NSA 01])。
- 澳大利亚的防御信号理事会(Defense Signals Directorate[DSD 01])。
- 加拿大的通讯安全局(Communications Security Establishment[CSE 01])。
- 俄罗斯的联邦安全局(Academy of Federal Agency for Government[AFAG 01])。

有兴趣的读者还可以访问以下资源：

- NSA 主管的 National Cryptologic Museum[NCM 01]。
- 密码爱好者的团体：The American Cryptogram Association[ACA 01]。
- 专业季刊：Cryptologia[Cryptologia 01]。
- 专业季刊：The Journal of Cryptology[Cryptology 01]。
- 关于密码学问题的电子期刊：The Journal of Craptology[Craptology 01](您大可不必在意这个资源)。