密　码　学

—— 理论和实践

[美] D. R. 斯廷森　著

张文政　译

国防科学技术保密通信重点实验室

密 码 学

——理论和实践

[美] D.R. 斯廷森 著

张文政 译
谯通旭等 校
刘村友 总校

国防科学技术保密通信重点实验室

1997 年 · 成都

前 言

我写这本书的主要目的是出一本一般的综合性教科书，它涉及密码学中所有重要的领域。虽然近几年来已经出版了许多关于密码学方面的专著，但它们主要是讲述密码学中的某一特定领域。另一方面，由于过去 15 年间密码学研究的快速扩展，现存的许多教科书已变得过时了。

我在 Nebraska—Lincoln 大学为计算机科学方面的研究生教授密码学课程，但我知道，在数学系、计算机科学系和电子工程系中本科生和研究生都开设了密码学课程，这样我就打算写一本在密码学的更广领域中使用的足以普遍适用的书籍。

当然，要吸收这样广泛的读者会有许多困难，但基本上我打算以适当的方式来完成这些事。我提供了所需要的数学知识，我对各种密码体制给出了一个非形式化的描述及更精确的伪编码描述，因为我认为这两种方式可以相互加强。同时这里也有许多例子来解释这些算法的工作原理，并且在每种情况下，我都解释了它的数学结构，因为在没有理解基本的数学理论之前来理解一个密码体制是如何工作的，我认为是不可能的。

这本书分成三个部分：第一部分（第 1 章—第 3 章）包含私钥密码体制；第二部分（第 4 章—第 9 章）涉及到公钥密码的主要课题；第三部分（剩下的 4 章）介绍了密码学中的四个实际研究领域。

第一部分包括下列内容：第 1 章是对简单的“经典”密码体制的基本介绍；第 2 章包含了密码学的仙侬方法的主要部分，包括完全保密的概念和信息论在密码学中的应用；第 3 章是对 DES 的较详细的讨论，包括差分分析。

第二部分包括下列内容：第 4 章涉及到 RSA 公钥密码体制、素性测试和因子分解的数论背景；第 5 章讨论了其他一些公钥密码体制，最重要的是基于离散对数的 ElGamal 体制；第 6 章讨论了签名规则，如数字签名标准，包括各种特定类型的签名方案，如不可否认签名和失败—停止签名方案；第 7 章是散列函数；第 8 章综述了密钥分配和密钥共识协议的许多方法；第 9 章描述了身份识别方案。

第三部分的各章包括了精选的几个研究课题：鉴别码、秘密共享方案、伪随机数发生器和零知识证明。

这样，我试图综合介绍密码学的各“核心”领域，同时也提供了关于特定领域的一

些更新的章节。然而在任何给定的领域中，我试图挑选几个具有代表性的系统，然后以适当的深度讨论它们，这样就覆盖范围来讲本书就不是一本百科全书。

当然，这本书比一学期（或两学期）所包含的内容更多，但我希望这本书可以作为几个不同类型的学期课程的基础。一般性的介绍可以包括第 1 章以及第 2 章～第 5 章的精选部分，第二学期或研究生课程可以更完整的方式包含这些章节，以及从第 6 章到第 9 章的知识。进而我认为任何一章将成为进一步研究该“主题”的一个适当基础。

但除了它的原始目的是作为教课书外，我还希望密码学中的研究人员和实际工作者能发现对他们可能并不熟悉的领域，本书可以提供一种入门介绍。鉴于这个想法，对讨论的许多主题我都提供了进一步阅读的参考文献。

写这本书最困难的事情之一是确定要引入多少数学知识。密码学是一个十分广泛的课题，它需要几个领域的数学知识，包括数论、群、环、域，线性代数，概率论和信息论，并且熟悉计算复杂性、算法和 NP—完全性理论也有好处。我没有假定需要这么多的数学知识，对于大部分章节仅讲述了它们需要的数学工具，这对熟悉基本的线性代数和模算术的读者肯定有好处。另一方面，一个更专业化的课题，如信息论中熵的概念，顺便作了介绍。

我也将向任何不同意副书名“理论和实践”的人道歉，我承认这本书包含了比实践更多的理论。我的意思是在这本书中我将选择同时包括理论兴趣和实际重要性这两个基本方面的资料。所以，书中可能包括了一些不实用的体制，不管它们是数学上一流的还是能解释一个重要的概念或技术的。但另一方面，我描述了最重要的在实际中使用的体制，如 DES 和其他美国密码标准。

D. R. 斯廷森

（蒋继红　校）

目　次

第1章　经典密码学

1.1　引言：一些简单密码体制

密码学的基本任务是使通常称为 Alice 和 Bob 的两个人在不安全的信道上进行通信，而他们的敌人 Oscar 不能理解他们正在通信的内容。比如，这个信道可能是电话线或计算机网。Alice 打算发送给 Bob 的消息，我们称为“明文”，它能够是英文文本、数字数据或任何其他东西——它的构造是完全任意的。Alice 用预先确定的密钥加密明文，同时在信道上发送产生的密文，在信道上通过截听而能看到密文的 Oscar 不能确定明文是什么，但知道加密密钥的 Bob 能解密密文从而重构明文。

这个概念更形式化的描述是使用下列数学记号。

定义 1.1：一个密码体制是一个五元组 (P,C,K,E,D)，这里下列一些条件要满足：

(1) P 是可能明文的有限集；

(2) C 是可能密文的有限集；

(3) 密钥空间 K 是可能密钥的有限集；

(4) 对每一个 $K\in K$，有一个加密规则 $e_K\in E$ 和相应的解密规则 $d_K\in D$，每一个 $e_K: P\to C$ 和 $d_K: C\to P$ 是一个函数，它满足 $d_K(e_K(x))=x$，对每一个明文 $x\in P$。 ∎

主要特性是特性(4)，它是说如果一个明文 x 使用 e_K 加密，加密后的密文接着用 d_K 解密，那么原来的明文将得到恢复。

Alice 和 Bob 利用一个特定的密码体制将使用下列协议，首先他们选择一个随机密钥 $K\in K$。当他们在同一个地方能够完成这件事同时不能让 Oscar 观测到；或另一种方法，当他们在不同的地方而能进入一个安全信道来完成。然后假设 Alice 在不安全信道上打算发送给 Bob 报文，我们假设这个报文是下列串

$$\mathbf{x}=x_1x_2\cdots x_n,$$

对某一整数 $n\geqslant 1$，这里每一个 $x_i\in P$，$1\leqslant i\leqslant n$。每一个 x_i 通过预先确定的密钥 K 和加密规则 e_K 来加密，这里 Alice 计算 $y_i=e_K(x_i)$，$1\leqslant i\leqslant n$，同时结果的密文串为

$$\mathbf{y}=y_1y_2\cdots y_n,$$

在信道上发送，当 Bob 接收到 $y_1\ y_2\cdots\ y_n$ 后，他使用解密函数 d_K 来解密，获得原来的明文串 $x_1x_2\cdots x_n$。通信信道示于图 1.1。

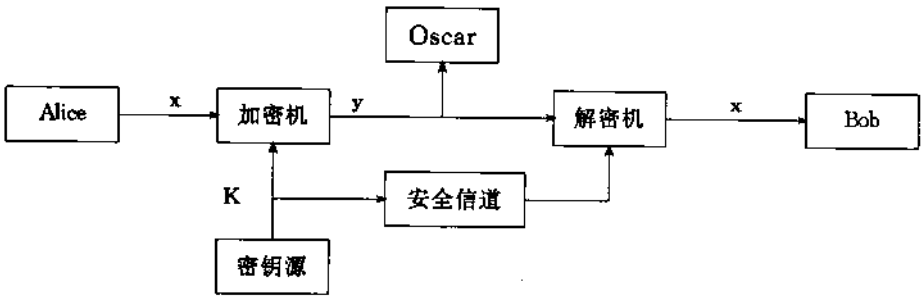

图1.1　通信信道

很明显，每一个加密函数 e_K 必定是一个单射函数(即一对一)，否则，无法完成无岐义的解密。例如，如果

$$y=e_K(x_1)=e_K(x_2),$$

这里 $x_1\neq x_2$，Bob 无法知道 y 将解密成 x_1 还是 x_2。注意如果 $P=C$，它要求每一个加密函数是一个置换，即，如果明文和密文集是相同的，那么每一个加密函数刚好重排(或置换)明文集的元素。

1.1.1 移位密码

在这一节，我们将描述基于模算术的移位密码，但首先我们复习模算术的一些基本定义。

定义 1.2：假设 a 和 b 是两个整数，m 是一个正整数，那么我们写 $a\equiv b(\mathrm{mod}\ m)$，如果 m 整除 $b-a$，这个短语 $a\equiv b(\mathrm{mod}\ m)$读作 "$a$ 同余于 b 模 m"，这个整数 m 称为模。 ▌

假设 a 和 b 被 m 除，获得整数商和余数，这个余数在 0 至 $m-1$ 之间。即 $a=q_1m+r_1$ 和 $b=q_2m+r_2$，这里 $0\leqslant r_1\leqslant m-1$，$0\leqslant r_2\leqslant m-1$。那么不难看到 $a\equiv b(\mathrm{mod}\ m)$，当且仅当 $r_1=r_2$。我们使用记号 $a \bmod m$(没有括号)来标记 a 被 m 除时的余数，即上面的 r_1。这样 $a\equiv b\ (\mathrm{mod}\ m)$，当且仅当 $a \bmod m=b \bmod m$。如果我们用 $a \bmod m$ 来代替 a，我们说 a 是被模 m 约简的[①]。

现在我们能够定义模 m 的算术：Z_m 是一个集合 $\{0,1,\cdots,m-1\}$，它有两种运算＋和×。在 Z_m 中的加法和乘法，除了将结果被模 m 约简外，刚好像实数加法和乘法。

例如，假设我们打算计算在 Z_{16} 中的 11×13，作为整数，我们有 $11\times13=143$，为了约简 143 模 16，我们只须完成普通的长除法：$143=8\times16+15$，所以 $143 \bmod 16=15$，因此，在 Z_{16} 中 $11\times13=15$。

在 Z_m 中的加法和乘法满足大部分算术规则，现在不加证明地列出这些规则：

(1)加法是封闭的，即对任何 $a,b\in Z_m$，有 $a+b\in Z_m$；

(2)加法是可交换的，即对任何 $a,b\in Z_m$，有 $a+b=b+a$；

(3)加法是可结合的，即对任何 $a,b,c\in Z_m$，有 $(a+b)+c=a+(b+c)$；

(4)0 是加法单位元，即对任何 $a\in Z_m$，有 $a+0=0+a=a$；

(5)对任何一个 $a\in Z_m$ 的加法逆元是 $m-a$，即对任何 $a\in Z_m$ 有 $a+(m-a)=(m-a)+a=0$；

(6)乘法是封闭的，即对任何 $a,b\in Z_m$，有 $ab\in Z_m$；

(7)乘法是可交换的，即对任何 $a,b\in Z_m$，有 $ab=ba$；

(8)乘法是可结合的，即对任何 $a,b,c\in Z_m$，有 $(ab)c=a(bc)$；

(9)1 是乘法单位元，即对任何 $a\in Z_m$，有 $a\times1=1\times a=a$；

(10)乘法在加法上是可分配的，即对任何 $a,b,c\in Z_m$，有 $(a+b)c=(ac)+(bc)$，且 $a(b+c)=(ab)+(ac)$。

规则(1)、(3)～(5)是说 Z_m 关于加法操作形成了一个称为群的代数结构，因为特性(2)也成立，这个群被说成是阿贝尔的。

事实上在 Z_m 中的规则(1)—(10)是说 Z_m 形成一个环。在这本书中我们将看到群和环的许多其他例子，一些环的类似例子包括整数 Z，实数 R 和复数 C。然而这些都是无限环，而我们的注意力仅限制在有限环上。

因而在 Z_m 中存在加法逆元，所以我们也能够在 Z_m 中完成减法。我们定义在 Z_m 中的 $a-b$ 是 a

---

① 许多计算机程序语言定义 $a \bmod m$ 是一个在 $-m+1$ 到 $m-1$ 之间的与 a 有相同符号的余数。例如 $-18 \bmod 7$ 将是 -4，而不是我们上面定义的 3。但对我们的目的，定义 $a \bmod m$ 始终是一个非负整数更方便。

$+m-b \bmod m$。等价地，我们能计算 $a-b$，然后通过模 m 来约简它。

例如，为计算 Z_{31} 中 11－18，我们能计算 11＋13 mod 31＝24。等价地，我们首先从 11 中减去 18 得到－7，然后计算－7 mod 31＝24。

在图 1.2 中我们提供了移位密码。

设设 $P=C=K=Z_{26}$。对 $0 \leqslant K \leqslant 25$，定义

$e_K(x)=x+K \bmod 26$

同时

$d_K(y)=y-K \bmod 26$

$(x,y \in Z_{26})$。

图 1.2　移位密码

虽然它可以定义在任何模 m 上，而这里它是定义在 Z_{26} 上，因为这里有 26 个英文字母，很容易看到移位密码形成了上述定义的密码体制，即对每一个 $x \in Z_{26}$ 有 $d_K(e_K(x))=x$。①

我们通过建立在字母和模 26 的剩余之间的如下对应：A↔0，B↔1，…，Z↔25，使用移位密码（模 26）来加密英文正文。因为我们将在几个例子中使用这个对应，为了将来的使用我们记下它。

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

用一个小例子来解释。

例 1.1：假设移位密码的密钥 K＝11，明文是

wewillmeetatmidnight.

我们首先使用该规定的对应把明文转变成整数序列如下：

22　4　22　8　11　11　12　4　4　19

0　19　12　8　3　13　8　6　7　19

其次，对每一个值我们加上 11，通过模 26 约简每一个和：

7　15　7　19　22　23　23　15　15　4

11　4　23　19　14　24　19　17　18　4

最后，我们把整数序列转变成字母，获得密文：

HPHTWWXPPELEXTOYTRSE.

为了解密密文，Bob 首先把密文转变成整数序列，然后从每一个值中减去 11（模 26 约简），最后转变整数序列到字母。②　∎

如果一个密码体制是可实际使用的，它将满足某些特性，我们非形式化地枚举出这些特性中的

① 对一特定的密钥 $K=3$，这个密码体制称为 Caesar 密码，它是由 J. Caesar 使用的。

② 在上面的例子中为了改进可读性，我们对密文用大写字母，明文用小写字母，除非另外声明我们将一直这样做。

两个：

(1)每一个加密函数 e_K 和每一个解密函数 d_K 将能有效地计算；

(2)看到密文串 y 的敌人将不能够确定出正在使用的密钥 K 或明文串 x。

第二个特性是以非常不明确的方式来定义“安全”的思想，给定密文串 y 来试图计算密钥 K 的过程称为密码分析(后面我们将使这些概念更精确)。注意，如果 Oscar 能确定 K，那么他就能像 Bob 一样使用 d_K 来解密 y，因此确定 K 至少与确定明文串 x 一样困难。

我们观察到移位密码(模 26)是不安全的，因为它能通过穷举密钥搜索这个明显的方法来进行密码分析，因为这里仅有 26 种可能密钥，它很容易来试每一个可能的解密规则 d_K 直到获得一个“有意义”的明文串。可通过下列例子来解释这一点。

例 1.2：给定密文串

JBCRCLQRWCRVNBJENBWRWN.

我们连续地试解密密钥 d_0，d_1 等等，将获得下列字母串：

jbcrclqrwcrvnbjenbwrwn
iabqbkpqvbqumaidmavqvm
hzapajopuaptlzhclzupul
gyzozinotzoskygbkytotk
fxynyhmnsynrjxfajxsnsj
ewxmxglmrxmqiweziwrmri
dvwlwfklqwlphvdyhvqlqh
cuvkvejkpvkogucxgupkpg
btujudijoujnftbwftojof
astitchintimesavesnine

在这点上，我们确定了明文同时我们能够停下来，这个密钥是 $K=9$。 ▮

平均一个明文将在试 26/2=13 次解密规则后而确定。

上面的例子指出，一个密码体制是安全的必要条件是穷举密钥搜索将是不可行的，即密钥空间将是非常大的。像可能希望的那样，一个大的密钥空间并不足以保证安全性。

1.1.2 替换密码

另一个众所周知的密码体制是替换密码，这个密码体制已经使用几百年了。报纸上的“密报”难题是替换密码的一个例子，这个密码定义在图 1.3 中。

设 $P=C=Z_{26}$，K 是由 26 个符号 0,1,…,25 的所有可能置换组成，对每一个置换 $\pi\in K$，定义

$$e_\pi(x)=\pi(x),$$

且

$$d_\pi(y)=\pi^{-1}(y),$$

这里 π^{-1} 是 π 的逆置换。

图 1.3 替换密码

实际上，在替换密码的情况下，我们也可取 P 和 C 都是 26 个字母的英文字符，在移位密码中我们使用 Z_{26} 是因为加密和解密是一个代数运算，但在替换密码中可以更方便地认为加密和解密是

由字母的置换构成。

这里有一个由加密函数组成的"随机"置换 π。(像前面一样,明文字母是小写,密文字母是大写。)

a	b	c	d	e	f	g	h	i	j	k	l	m
X	N	Y	A	H	P	O	G	Z	Q	W	B	T

n	o	p	q	r	s	t	u	v	w	x	y	z
S	F	L	R	C	V	M	U	E	K	J	D	I

这样 $e_\pi(a)=X$,$e_\pi(b)=N$,等等。解密函数是一个逆置换,它首先是写第二行,然后以字母顺序排序,就获得了下列的逆置换:

A	B	C	D	E	F	G	H	I	J	K	L	M
d	l	r	y	v	o	h	e	z	x	w	p	t

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	g	f	j	q	n	m	u	s	k	a	c	i

因此,$d_\pi(A)=d$,$d_\pi(B)=l$,等等。

作为练习,读者可以利用解密函数解密下列密文:

MGZVYZLGHCMHJMYXSSFMNHAHYCDLMHA.

替换密码的密钥刚好是由 26 个字母的置换组成,这些置换的数目是 26!,它大于 4.0×10^{26},是一个非常大的数。这样甚至对计算机来说穷举搜索密钥是不可行的,然而,后面我们将看到替换密码很容易通过其他方法来破译。

1.1.3 仿射密码

移位密码是替换密码的一个特例,它仅包含了 26 个元素的 26! 种可能置换中的 26 个。替换密码的另一个特例就是我们现在描述的仿射密码,在仿射密码中我们限制加密函数是下列形式

$$e(x)=ax+b \bmod 26,$$

$a,b\in Z_{26}$。这个函数称为仿射函数,因此该密码体制命名为仿射密码。(当 $a=1$ 时,它是移位密码。)

为了可能解密,它必须要求仿射函数是一个单射,换句话说,对任何 $y\in Z_{26}$,我们要求同余式

$$ax+b\equiv y \pmod{26}$$

有唯一的解 x。这个同余式等价于

$$ax\equiv y-b \pmod{26}.$$

现在当 y 在 Z_{26} 上变化时,$y-b$ 也将在 Z_{26} 上变化,故研究同余式 $ax\equiv y \pmod{26}$ $(y\in Z_{26})$ 就足够了。

我们断言这个同余式对每一个 y 有唯一地解当且仅当 $\gcd(a,26)=1$(这里函数 gcd 表示它的变元的最大公约数)。首先假设 $\gcd(a,26)=d>1$,那么同余式 $ax\equiv0 \pmod{26}$ 至少有两个 Z_{26} 中的不同解。即 $x=0$ 和 $x=26/d$,在这种情况下 $e(x)=ax+b \bmod 26$ 不是单射函数,因此它不是一个

有效加密函数。

例如，因为 $\gcd(4,26)=2$，可证明 $4x+7$ 不是一个有效加密函数：对任何 $x\in Z_{26}$，x 与 $x+13$ 将加密成相同的值。

其次，我们假设 $\gcd(a,26)=1$，假设对某个 x_1 和 x_2 有

$$ax_1\equiv ax_2 \pmod{26},$$

则

$$a(x_1-x_2)\equiv 0 \pmod{26}.$$

这样

$$26 \mid a(x_1-x_2).$$

现在我们使用除法特性：如果 $\gcd(a,b)=1$，且 $a\mid bc$，那么 $a\mid c$。因为 $26\mid a(x_1-x_2)$，$\gcd(a,26)=1$，因此必有

$$26 \mid (x_1-x_2),$$

即

$$x_1\equiv x_2 \pmod{26}.$$

至此我们已证明，如果 $\gcd(a,26)=1$，那么 $ax\equiv y \pmod{26}$ 形式的同余式在 Z_{26} 中有唯一解。因此，我们让 x 在 Z_{26} 上变化，那么 $ax \bmod 26$ 将取遍模 26 的 26 个不同值。即，它刚好取每一个值一次，可证明对每一个 $y\in Z_{26}$，同余式 $ax\equiv y \pmod{26}$ 对 x 来说有唯一解。

在这个关于数 26 的讨论中没有什么特别的，下面这个结果能以类似的方式来证明。

定理 1.1：同余式 $ax\equiv b \pmod{m}$ 对每一个 $b\in Z_m$ 有唯一解 $x\in Z_m$ 当且仅当 $\gcd(a,m)=1$。▌

因为 $26=2\times 13$，满足 $\gcd(a,26)=1$ 的 $a\in Z_{26}$ 的值有 $a=1,3,5,7,9,11,15,17,19,21,23,25$，参数 b 可能是 Z_{26} 中的任何元素。因此仿射密码有 $12\times 26=312$ 个可能密钥（当然，对安全性来说它是一个太小的数目）。

现在让我们考虑一下模是 m 的一般性的设置，我们需要数论中的另一个定义。

定义 1.3：假设 $a\geqslant 1$，$m\geqslant 2$ 是整数，如果 $\gcd(a,m)=1$，我们就说 a 和 m 互素。在 Z_m 中与 m 互素的整数的数目通常记为 $\Phi(m)$（这个函数称为欧拉函数）。 ▌

数论中一个众所周知的结果是利用 m 的素因子幂次的分解式给出 $\Phi(m)$ 的值（一个整数 $p>1$ 是一个素数，如果除开 1 和 p 之外，它没有其他正的因子，每一个 $m>1$ 的整数能以唯一的方式分解成素数幂的乘积。例如 $60=2^2\times 3\times 5$，$98=2\times 7^2$）。

我们采用下列定理来记下 $\Phi(m)$ 的公式。

定理 1.2：假设 $m=\prod_{i=1}^{n} p_i^{e_i}$，这里 p_i 是不同的素数，$e_i>0$，$1\leqslant i\leqslant n$，那么

$$\Phi(m)=\prod_{i=1}^{n}(p_i^{e_i}-p_i^{e_i-1}).$$ ▌

可以证明 Z_m 上仿射密码的密钥数目是 $m\Phi(m)$，这里 $\Phi(m)$ 由上述公式给出（这里加密函数是 $e(x)=ax+b$，b 的选择数目是 m 个，a 的选择数目是 $\Phi(m)$ 个）。例如，$m=60$，$\Phi(m)=2\times 2\times 4=16$，因此仿射密码的密钥数目是 960。

现在让我们考虑一下在仿射密码中模 26 的解密操作。假设 $\gcd(a,26)=1$，为了解密 x，我们需要解同余式 $y\equiv ax+b \pmod{26}$，像上面已讨论的那样，同余式将在 Z_{26} 中有唯一的解，但它没有给出一个有效的算法来找到这个解。我们需要的是有一个算法来完成，幸运地是模算术中的一些进一步的结果给我们提供了一个我们正寻找的有效解密算法。

我们需要乘法逆元的思想。

定义 1.4：假设 $a\in Z_m$，a 的乘法逆元是一个元素 $a^{-1}\in Z_m$，满足 $aa^{-1}\equiv a^{-1}a\equiv 1 \pmod{m}$。▌

通过上面这些类似地讨论，可证明，a 有模 m 的乘法逆元当且仅当 $\gcd(a,m)=1$，且如果乘法逆元存在，它必定是唯一的，同时也可观察到如果 $b=a^{-1}$，那么 $a=b^{-1}$。如果 p 是一个素数，那么 Z_p 中每一个非零元素有乘法逆元。每一个非零元素有乘法逆元的环就称为域。

后面，我们将描述对任何 m 计算 Z_m 中乘法逆元的一个有效算法，然而在 Z_{26} 中逐个尝试方法足以找到与 26 互素的每个元素的乘法逆元：$1^{-1}=1, 3^{-1}=9, 5^{-1}=21, 7^{-1}=15, 11^{-1}=19, 17^{-1}=23$ 和 $25^{-1}=25$。（这些能容易验证，如 $7\times15=105\equiv1 \bmod 26$，所以 $7^{-1}=15$。）

考虑我们的同余式 $y\equiv ax+b \pmod{26}$，它等价于

$$ax\equiv y-b \pmod{26}.$$

因为 $\gcd(a,26)=1$，a 有模 26 的乘法逆元，同余式的两边同时乘以 a^{-1}，我们得到

$$a^{-1}(ax)\equiv a^{-1}(y-b) \pmod{26}.$$

通过模 26 的乘法结合律，有

$$a^{-1}(ax)\equiv(a^{-1}a)x\equiv 1x\equiv x.$$

结果，$x\equiv a^{-1}(y-b) \pmod{26}$，对 x 来说这是一个显式公式，即解密函数为

$$d(y)=a^{-1}(y-b) \pmod{26}.$$

所以最后仿射密码的完整描述给在图 1.4 中。

设 $P=C=Z_{26}$，

$K=\{(a,b)\in Z_{26}\times Z_{26}:\gcd(a,26)=1\}$

对 $K=(a,b)\in K$，定义

$e_K(x)=ax+b \bmod 26$

和

$d_K(y)=a^{-1}(y-b) \bmod 26$

$x,y\in Z_{26}$.

图 1.4　仿射密码

让我们举一个小例子。

例 1.3：假设 $K=(7,3)$，注意到 $7^{-1}\bmod 26=15$，加密函数是

$$e_K(x)=7x+3,$$

相应的解密函数为

$$d_K(y)=15(y-3)=15y-19.$$

这里所有运算是在 Z_{26} 中进行的，它很容易验证对每个 $x\in Z_{26}$，$d_K(e_K(x))=x$，在 Z_{26} 中计算，我们有

$$\begin{aligned} d_K(e_K(x)) &= d_K(7x+3)\\ &= 15(7x+3)-19\\ &= x+45-19\\ &= x. \end{aligned}$$

为了解释这个，让我们加密明文 hot，我们首先转换字母 h，o，t 到模 26 的剩余，它们分别是 7，14 和 19，现在，我们加密

$$7\times7+3 \bmod 26=52 \bmod 26=0;$$

$$7\times14+3 \bmod 26=101 \bmod 26=23;$$

$$7\times19+3 \bmod 26=136 \bmod 26=6.$$

所以三个密文字母是 0,23,6 相对应的字母串 AXG。对读者来说我们留下解密作为练习。 ▌

1.1.4 维吉尼亚密码

移位密码和替换密码两者都是一次选择一个密钥，每一个字母都映射成唯一的一个字母。由于这个原因，这些密码体制称为单表密码体制。现在我们提供的图 1.5 中的密码不是单表密码，而是著名的维吉尼亚密码，这个密码是以生活在 16 世纪的 B. de. Vigenere 名字命名的。

设 m 是某一固定的正整数，定义 $P=C=K=(Z_{26})^m$，对一个密钥 $K=(k_1,k_2,\cdots,k_m)$，我们定义

$$e_K(x_1,x_2,\cdots,x_m)=(x_1+k_1,x_2+k_2,\cdots,x_m+k_m)$$

和

$$d_K(y_1,y_2,\cdots,y_m)=(y_1-k_1,y_2-k_2,\cdots,y_m-k_m),$$

这里所有运算在 Z_{26} 中完成。

图 1.5 维吉尼亚密码

使用前面已描述过的映射 A↔0,B↔1,…,Z↔25，我们能够使每一个密码 K 与长度为 m 的称为密钥字的字符串相关联。维尼吉亚密码每次加密 m 个字母：每一个明文元素等价于 m 个字母。

让我们举一个小例子。

例 1.4：假设 $m=6$，密钥字是 CIPHER，密钥 K 相对应的映射是 $K=(2,8,15,7,4,17)$，假设明文是串

thiscryptosystemisnotsecure.

我们转换这些明文元素到模 26 的剩余，以长度为 6 的组写下它们，然后“加上”模 26 的密钥字，过程如下：

19	7	8	18	2	17	24	15	19	14	18	24
2	8	15	7	4	17	2	8	15	7	4	17
21	15	23	25	6	8	0	23	8	21	22	15

18	19	4	12	8	18	13	14	19	18	4	2	20	17	4
2	8	15	7	4	17	2	8	15	7	4	17	2	8	15
20	1	19	19	12	9	15	22	8	25	8	19	22	25	19

这样密文串的等价字母是

VPXZGIAXIVWPUBTTMJPWIZITWZT.

为了解密，我们能够使用相同的密钥，但我们将用模 26 的减来代替模 26 的加法。 ▌

观察到维吉尼亚密码中长度为 m 的可能密钥字的长度是 26^m，甚至对于一个小的 m 值，穷举密钥空间将需要大的时间，例如，$m=5$，密钥空间超过 1.1×10^7，这个已经大到足以阻止手工的穷举密钥搜索(但不能阻止计算机)。

在维吉尼亚密码中密钥字长度是 m，一个字母能够映射成 m 个可能字母中的一个(假设密钥字包含 m 个不同的字母)，这样的密码体制称为多表密码体制，一般情况下对多表密码体制的密码分析比单表困难。

1.1.5 Hill 密码

在这一节，我们将描述另一个多表密码体制，它称为 Hill 密码，这个密码是 L. S. Hill 于 1929 年发明的。设 m 是一个正整数，定义 $P=C=(Z_{26})^m$，它的思想是取一个明文元素的 m 个字母的 m 个线性组合，这样产生一个密文元素中的 m 个字母。

例如，$m=2$，我们能够写明文元素 $x=(x_1,x_2)$和密文元素 $y=(y_1,y_2)$，y_1 将是 x_1 和 x_2 的线性组合，y_2 也是，我们可取

$$y_1=11x_1+3x_2,$$

$$y_2=8x_1+7x_2.$$

当然，这也可以矩阵形式写成更简洁的形式

$$(y_1,y_2)=(x_1,x_2)\begin{pmatrix}11 & 8\\ 3 & 7\end{pmatrix}.$$

一般，我们将取 $m\times m$ 的矩阵 K 作为我们的密钥，如果 K 中第 i 行和第 j 列的元素是 k_{ij}，那么我们写 $K=(k_{ij})$。对 $x=(x_1,\cdots,x_m)\in P$ 和 $K\in K$，我们能计算 $y=e_K(x)=(y_1,\cdots,y_m)$如下：

$$(y_1,y_2,\cdots,y_m)=(x_1,x_2,\cdots,x_m)\begin{pmatrix}k_{1,1} & k_{1,2} & \cdots & k_{1,m}\\ k_{2,1} & k_{2,2} & \cdots & k_{2,m}\\ \vdots & \vdots & & \vdots\\ k_{m,1} & k_{m,2} & \cdots & k_{m,m}\end{pmatrix}$$

换句话说，$y=xK$。

我们说密文是明文通过线性变换而获得的，我们必须考虑怎样进行解密，即 x 怎样能从 y 中计算出来，熟悉线性代数的读者将使用矩阵的逆 K^{-1}来解密，密文是通过公式 $x=yK^{-1}$来解密。

这里有一些线性代数的必要概念的定义，如果 $A=(a_{i,j})$是 $l\times m$ 的矩阵，$B=(b_{j,k})$是 $m\times n$ 的矩阵，那么我们通过下列公式定义矩阵的乘积 $AB=(c_{i,j})$：

$$c_{i,k}=\sum_{j=1}^{m}a_{i,j}b_{j,k}.$$

这里，$1\leqslant i\leqslant l$ 和 $1\leqslant k\leqslant n$。即 AB 的第 i 行第 k 列元素是取 A 的第 i 行和 B 的第 k 列的相应元素相乘，然后相加而得到的。注意 AB 是 $l\times n$ 的矩阵。

矩阵乘积的定义是可结合的(即$(AB)C=A(BC)$)，但一般情况下，不满足交换律(甚至对方阵 A 和 B，并不是总能成立 $AB=BA$)。

$m\times m$ 的单位矩阵记为 I_m，它是一个主对角线为 1，其它元素为 0 的 $m\times m$ 的矩阵，这样，2×2 的单位阵是

$$I_2=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}.$$

因为对任何 $l\times m$ 的矩阵 A 有 $AI_m=A$，对任何 $m\times n$ 的矩阵 B 有 $I_mB=B$，I_m 是一个单位阵。现在如果 $m\times m$ 的矩阵 A 的逆矩阵为 A^{-1}(如果存在)，它满足 $AA^{-1}=A^{-1}A=I_m$。并不是所有的矩阵都有逆矩阵，但如果逆矩阵存在的话，它必定唯一。

有了这些事实，很容易推导出上面给出的解密公式：因为 $y=xK$，两边同时乘以 K^{-1}，得到

$$yK^{-1}=(xK)K^{-1}=x(KK^{-1})=xI_m=x.$$

(注意利用了结合律。)

我们能验证上述加密矩阵在 Z_{26}中有逆矩阵