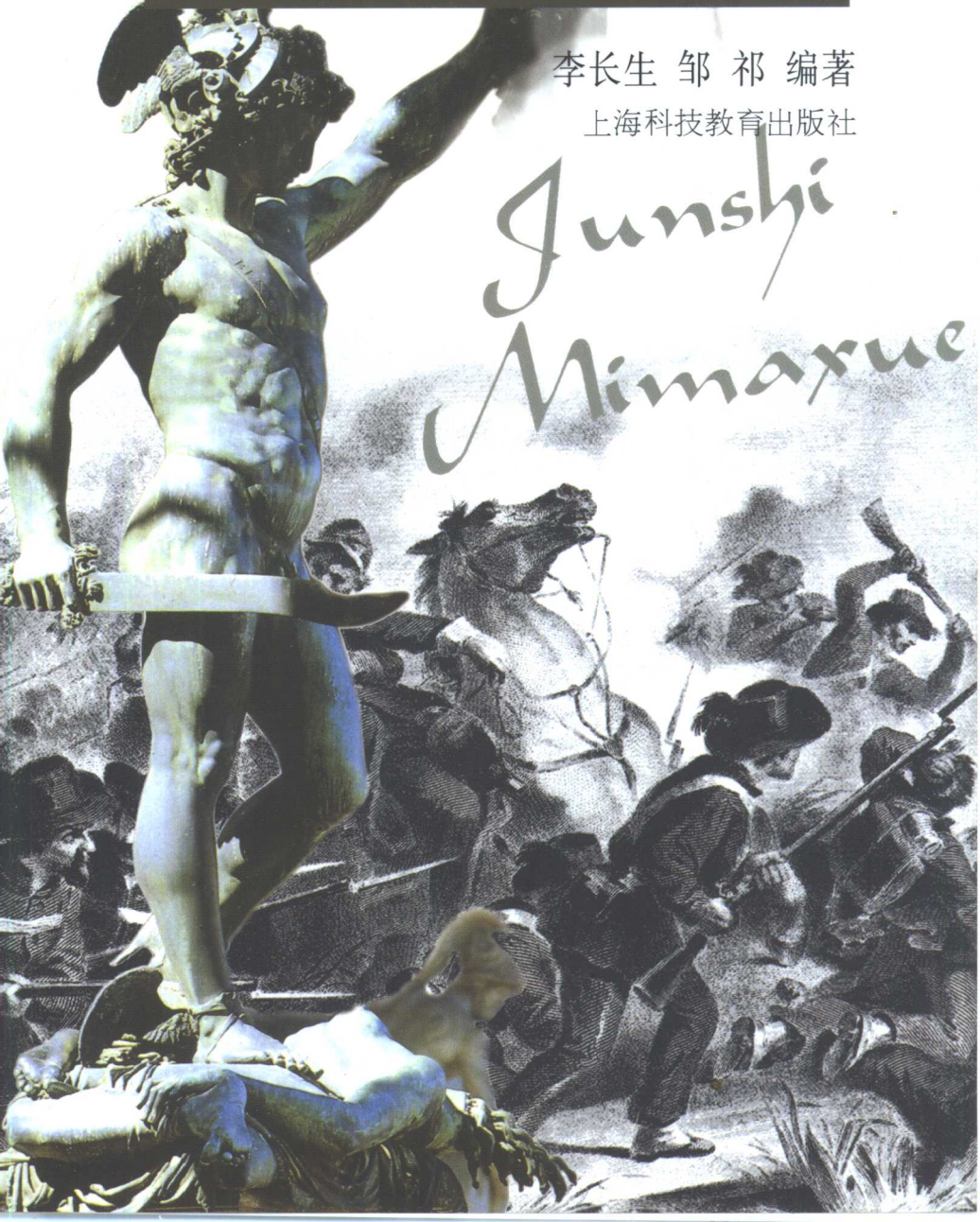
战争中的数学

军事密码学

李长生 邹 祁 编著

上海科技教育出版社

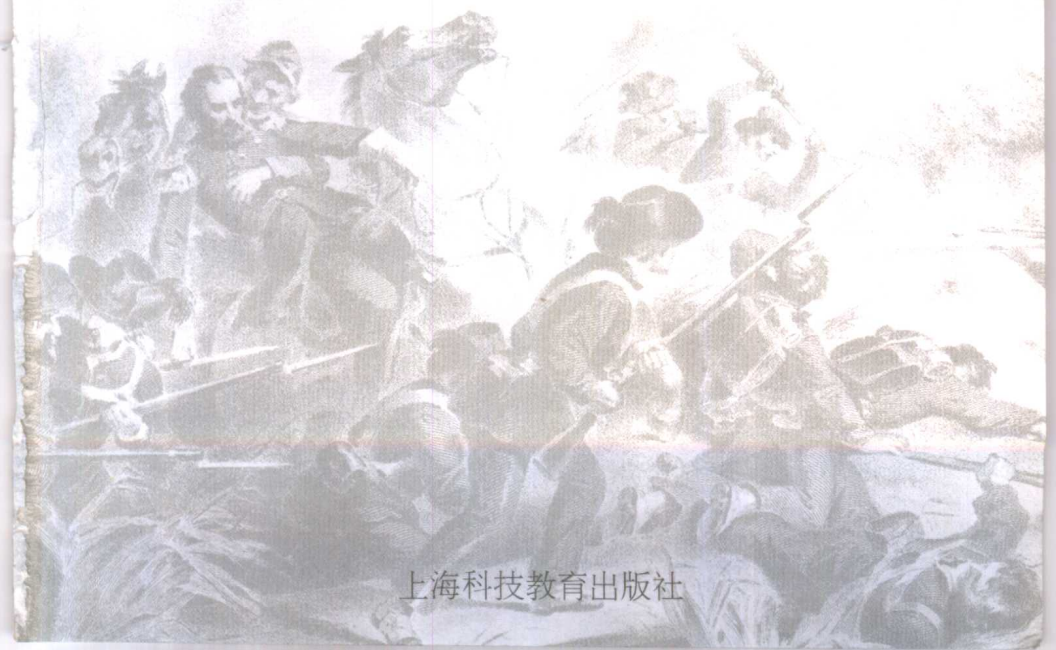
Junshi Mimaxue



战 争 中 的 数 学

军事密码学

李长生 邹 祁 编著



上海科技教育出版社

策划编辑　朱惠霖
责任编辑　朱惠霖
装帧设计　桑吉芳
版式设计　朱惠霖

·战争中的数学·
军事密码学
李长生　邹　祁　编著
上海科技教育出版社出版发行
（上海冠生园路 393 号　邮政编码 200235）
各地新华书店 经销　丹阳教育印刷厂印刷
开本 850×1168　1/32　印张 5.875　插页 1　字数 142 000
2001 年 9 月第 1 版　2001 年 9 月第 1 次印刷
印数 1－5 000
ISBN 7－5428－2469－4/O·275
定价：14.00 元

图书在版编目（CIP）数据

军事密码学/李长生，邹祁编著.—上海：上海科技教育出版社，2001.9

（战争中的数学）

ISBN 7-5428-2469-4

Ⅰ.军… Ⅱ.①李…②邹… Ⅲ.军事-密码-普及读物 Ⅳ.TN918.1-49

中国版本图书馆 CIP 数据核字（2000）第 73350 号

目　次

第一章　凯撒的密信　1

《高卢战记》1　译者的质疑2　凯撒密表3　芝麻开门5　密钥6　什么是密码8　道高一尺，魔高一丈10

第二章　从古埃及的神秘碑文说起　12

尼罗河畔的神秘碑文12　暗号和隐语13　卡尔达诺的漏格板17　“天书”20　还是凯撒24　圆盘与方表29　数学家的天下34　密码机40

第三章　与福尔摩斯共舞　46

《跳舞的小人》46　福尔摩斯的舞蹈49　密码破译的三大要素51　突破口之一：频率54　突破口之二：连接55　突破口之三：密钥漏洞59　破密“宝典”62　“合拍”现象64　重合指数67　三管齐下69　三条大路通罗马73

第四章　密码让历史拐了个弯　81

德国外长的密电81　两条通信电缆84　四十号房间85　“眨眼者”霍尔86　一石三鸟89　总统气昏了90　棋盘与换位93　两份头尾相同的密文96　还是频率统计99　愤怒的潘万101

第五章　太平洋上的情报战　107

"耻辱的日子"107　迟到的最后通牒110　"密码学之父"114
"紫密"117　"魔术"120　AF之谜124　山本五十六之死128

第六章　丘吉尔的"超级"情报　133

"鹰式行动"133　忍辱负重的道丁将军138　"不可思议的东西"139
聪明过头的德国人141　波兰人的成就148　布莱奇利庄园150
两条"鱼"154　捉拿"金枪鱼"160　"超级"保密165

第七章　秘密？公开？　169

公开的挑战169　一场"人民战争"171　DES简介172　把密钥也公开177

编著者后记　183

参考文献　184

兵者，诡道也。

——（春秋）孙武：《孙子》

第一章　凯撒的密信

《高卢战记》

公元前51年初，深冬。

高卢，毕布拉克德（现法国境内伯夫雷山），罗马军团冬令营，凯撒的营帐。

深夜。

罗马共和国高卢行省长官儒略·凯撒，正在一张羊皮上写着什么。他的身影被跳动的灯火映在帐篷上，高大而摇曳。他的脸略嫌狭长，但棱角分明，专注的神色中透着与生俱来的自负。他在写他的“随记”，也就是后来流传于世的《高卢战记》。

戎马倥偬的凯撒，本没有余暇来写什么随记。但是，过去的几年中，与他在高卢的显赫战绩相比，政治上的事态发展可不那么如意。罗马执政官克拉苏斯，在同帕尔提亚人（在今土库曼斯坦南部和伊朗东北部）的作战中被俘。熔化了的金液灌进了他的喉咙……这个当年残酷镇压斯巴达克斯起义的刽子手，如今

同他堵如生命的金子铸在了一起. 这对凯撒来说是一件好事——少了一个政敌,但更是一件坏事——罗马"三巨头"之间的平衡被打破了,活着的两巨头,他和庞培,不得不面临决斗. 凯撒从来没有看得起过克拉苏斯,这个只会献媚的小人,死不足惜. 但庞培绝不能小看. 不然的话,凯撒当年也不会把自己的女儿尤丽娅嫁给庞培,要知道,庞培比凯撒还要大 8 岁.

现在,尤丽娅已去世,他们之间除了你死我活,已无任何瓜葛. 庞培以罗马唯一执政官的地位优势,正在元老院里向他发动强大的政治攻势……

他必须宣传自己,他必须向元老院陈述自己的功绩,但同时又必须表现出一种谦逊、客观的态度,不能带有任何自吹自擂的痕迹. 为此,他在这部随记中,处处用第三人称称呼自己,通篇都用异常平静、简洁的笔调叙说战事的经过.

这时他正写到卷五. 说的是公元前 54 年,他的爱将西塞罗突然遭到维尔纳人的围攻,情况紧急,"于是,他以极大的酬报说服了一个高卢骑兵,送一封信去给西塞罗. 送去的信是用希腊文写的,免得它被敌人截住后,得知我军的计划. ……"写到这里,他停了一下,似在考虑更好的措辞. 一丝狡黠的微笑从脸上掠过,他继续写了下去……

译者的质疑

时间无情地飞驰,转眼就过了近 2000 年. 凯撒的《高卢战记》以其翔实的叙事、清纯的文风,成为研究罗马历史、拉丁文学和军事史不可或缺的学术资料. 1979 年,我国商务印书馆将《高卢战记》译成中文,作为"汉译世界学术名著丛书"中的一种出版,译者任炳湘先生.

打开这本中文译本,翻到第 124 页,我们看到了上面引述的那桩派人送信给西塞罗的事. 然而,治学严谨的译者在这里发

现了问题，他注道："言下之意，似乎高卢人不懂希腊文，即令书信被截去，也不会泄露自己的计划．但在本书卷一 25 节中曾说到在厄尔维几人营中发现用希腊文写的统计数字，又说高卢人无论公私文件都用希腊文书写，似乎有矛盾．"对此，译者的推测是："也许上面两节指的是高卢人用希腊字母书写自己的语言，这一节所说是真正的希腊文．"

译者的质疑可说是切中要害．然而，译者的推测却仍让人疑云难消．敌营中就没有一人认识真正的希腊文？他们就不能去找一个希腊人来识这封信（如果他们截住了这封信的话）？足智多谋的凯撒竟会不考虑这些明摆着的可能而铤而走险？

是不是可以有另外的解释？

确实有另外一种解释：如果让一位密码学家来进行推测，他会毫不犹豫地认为——凯撒送去的这封信是用密码写的！因为任何一本讲述密码学历史的著作，都会提到凯撒对军事密码学的贡献．凯撒在其军事行动中使用了密码，这在密码学界已不是密码．

凯撒用的是怎样的密码呢？

凯撒密表

古罗马随笔作家修托尼厄斯在他的作品中披露，凯撒常用一种"密表"给他的朋友写信．这里所说的密表，在密码学上称为"凯撒密表"．用现代的眼光看，凯撒密表是一种相当简单的加密变换，就是把明文中的每一个字母用它在字母表中位置后面的第三个字母代替．古罗马文字就是现在所称的拉丁文，其字母就是我们从英语中熟知的那 26 个拉丁字母．因此，凯撒密表就是用 D 代 a，用 E 代 b，……，用 Z 代 w，（注意！）用 A 代 x，用 B 代 y，C 代 z．这些代替规则也可用一张表格来表示（所以叫"密表"），如表 1.1 所示．

表 1.1 凯撒密表

明文字母	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
密文字母	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

例如,有这样一个拉丁文句子:

Omnia Gallia est divisa in Partes tres

(高卢全境分为三部分)

用凯撒密表加密后,就成为密文

RPQLD JDOOLD HVW GLYLVD LQ SDUWHV WUHV

你看,不掌握个中奥妙,不知道凯撒密表,简直不知所云.

那么,在公元前 54 年,凯撒就是用这种密码给西塞罗写信的吗? 有趣的是,密码界对这一点却持否定态度,因为密码学历史上还记载着凯撒使用的另一种加密方法:把明文的拉丁字母逐个代之以相应的希腊字母. 这种方法看来更贴近凯撒在《高卢战记》中的记叙. 显然,哪一个拉丁字母应该代之以哪一个希腊字母,事先都有约定,凯撒知道,西塞罗也知道. 不然的话,西塞罗收到密信后,也会不知所云.

凯撒的这种加密方法也可用一张表格表示. 比方说,用希腊字母代替拉丁字母,通常有如表 1.2 的代替规则.

表 1.2 另一种可能的"凯撒密表"

拉丁字母	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
希腊字母	α	β	ξ	δ	ε	φ	γ	η	ι	ϛ	κ	λ	μ	ν	ο	ρ	θ	ϟ	σ	τ	π	υ	ω	χ	ψ	ζ

我们写这本小册子的目的,当然不是考证当年凯撒派人送信给西塞罗时用的是什么保密的方法. 如果这一点具有考证价值,那就让历史学家去考虑吧. 我们讲述这个故事,是想借此带你来到密码学的大门口,并进一步迈进这扇大门.

芝麻开门

当阿里巴巴站在那四十一名大盗的山洞大门口，准备打开大门时，他必须知道一个咒语："芝麻开门"．当我们站在密码学的大门口，准备迈入时，必须要知道的则是一些基本概念．为此，让我们先把密码通信的几个要素总结如下．

在军事通信上，必须考虑要传送的秘密信息在传送的途中被除发信者和收信者以外的第三者（特别是敌方）截获的可能性．使载送信息的载体（如文本、无线电波等）即使在被截获的情况下也不会让截获者得知其中信息内容的通信方法或技术，称为**保密通信**．密码通信就是一种保密通信，它是把表达信息的意思明确的文字符号，用通信双方事先所约定的变换规则，变换为另一串莫名其妙的符号，以此作为通信的文本发送给收信者．当这样的文本传送到收信者手中时，收信者一时也不能识别其中所代表的意思，这时就要根据事先约定的变换规则，把它恢复成原来的意思明确的文字，然后阅读．这样，如果这个文本在通信途中被第三者截获，由于第三者一般不知道那变换规则，因此他就不能得知在这一串符号背后所隐藏的信息．当然，为了战争的目的，他会千方百计地努力弄到这个变换规则．一种努力就是对已截获的密文进行分析，有时结合从其他途径获得的有关信息，试图找出这个变换规则．

在密码学中，我们把要传送的以通用语言明确表达的文字内容称为**明文**，由明文经变换而形成的用于密码通信的那一串符号称为**密文**．把明文按约定的变换规则变换为密文的过程称为**加密**．收信者用约定的变换规则把密文恢复为明文的过程称为**解密**．敌方主要围绕所截获密文进行分析以找出密码变换规则的过程，称为**破译**．

如在上一节中，Omnia Gallia est divisa in Partes tres 就是一段

明文，凯撒密表就是一种变换规则．这段明文经凯撒密表加密后，就变成了密文 RPQLD JDOOLD HVW GLYLVD LQ SDUWHV WUHV．收信者收到这段密文后，就要进行解密．解密也是用凯撒密表，就是把凯撒密表的第二行中每一个字母用它头顶上第一行中的相应字母代替．

在这个例子中，加密和解密都在用凯撒密表，但严格地说，加密时所用的变换与解密时所用的变换是两个变换．这两个变换间的关系是它们互为逆变换．也就是说，对明文用其中一个变换进行加密产生密文后，若再用另一个变换对这密文进行解密，就会得到原来的明文．这种互逆的关系就如同我们所熟知的加法和减法互为逆运算的关系一样：加上一个数后再减去同一个数，就等于不加也不减．（后面我们将知道，用凯撒密表加密，就相当于模 26 加 3，而用它解密，就相当于模 26 减 3．）

密　钥

我们看到，密码的变换规则显然是至关重要的．一种变换规则一旦被敌方掌握，所有用这种规则加密的通信都将无密可言．因此，变换规则必须严加保密．但在密码的安全性与变换规则的安全性上，却有一个“怪圈”．

要提高密码的安全性，不让敌方轻易破译，就要把变换规则设计得尽量复杂，比方说，不是用字母代替字母，而是用字母组代替字母组；但变换规则复杂到一定程度，就变得难以记忆；而难以记忆，就需要用文字把它记录下来备查；而一有文字记录，其安全性就大打折扣．一是这种文字记录至少要为通信双方所拥有，于是就有多个复本，复本越多，安全性越差；二是这种文字记录与保管者可能分离，这就增加了被他人窃取复制的可能；三是变换规则需要经常更换，于是必须传送新的文字记录，但无论是古代的人工传送，还是现代的电子传送，显然都很不安全．

打破这个“怪圈”的方法是:在把变换规则设计得尽可能复杂的同时,设计出一个(或一组)“关键词”,根据这个(组)“关键词”,就可以把变换规则“推导”出来. 这个(组)“关键词”就称为**密钥**. 顾名思义,密钥就是打开密码之锁的钥匙.

例如,凯撒密表的密钥就是“后移3”,甚至可以更简单地表示为“3”. 记住这个密钥,在用凯撒密表进行加密或解密时,就不需要记住凯撒密表(表1.1)的具体内容了. 而对于表1.2,由于没有简短的密钥,我们只能把整个这张表作为密钥了. 好在表1.2并不是太复杂,记住它也不是太难. 但如果是一张庞大的密表(如中文的电报码本),而又没有较为简短的密钥,那么就不得不好好地在这张密表的保密工作上下一番功夫了. 虽然这样的密码在实际上也被人们所使用,但一般只用于具有相对固定的潜伏地点并伪装得较好的情报人员. 对于流动性较大的军事作战部门,这样的密码是不可取的. 因此在军事密码学中,我们只考虑有简短密钥的密码.

现在,我们可把一个密码的运作过程用图1.1表示.

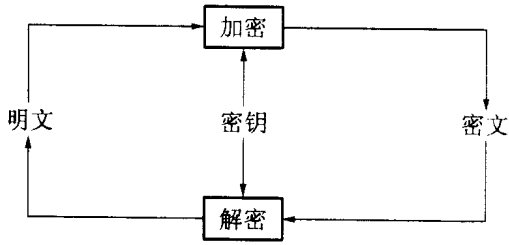


图1.1 一个密码的运作过程

在这张图中,我们只画了一个密钥,可同时用于加密和解密. 对此需要补充说明如下.

前面说过,加密变换和解密变换是互为逆变换的两个变换.

在几十年前，对这种区别一般不怎么强调．因为只要知道了其中一个变换，它的逆变换也就唾手可得了．但是到了20世纪70年代，这个观念被人打破了．有种变换，从一种状态变换到另一种状态的正变换其计算是十分容易的；但反过来，从另一种状态恢复到原来状态的变换，即逆变换，虽然在理论上可以从正变换得知，但其计算却十分复杂，即使用现代的电子计算机也要花去成千上万年的时间，这种计算已失去任何现实意义．如从两个很大的素数变换为它的积，这种变换就是做一个乘法，显然很容易；但是反过来，要把一个大整数分解成两个素数，一般没有有效的算法，计算十分困难．有人根据这一特点，设计了所谓“公开密钥密码”，简称“公钥密码”．在这种密码中，需要强调加密变换与解密变换之间在计算困难性上的巨大差异，并且相应地有两个(组)密钥，一个(组)是加密密钥(可予公开)，另一个(组)是解密密钥(必须保密)，分别用于加密和解密．关于这种密码，将在本书第七章介绍．目前我们还是暂时认为一个密码只需要一个(组)密钥．

什么是密码

我们已多次使用了“密码”这个词．对于它，似乎不需要多加解释．但密码学作为一门理论数学的应用分支，必须对每个概念作出明确的定义．对“密码”这个概念，也不例外．为此，让我们回顾一下我们在用这个词时所表达的意思．

从字面上看，“密码”应该是指密文中所用的符号，这自然不错．但这些符号若不代表着某种明文，那么它们也仅是符号而已，是不能被称为密码的．因此，“密码”应该是隐藏着明文的密文符号．但是，当我们说“这个密码与那个密码不同”时，是什么不同呢？难道仅是指密文所用的符号不同吗？当然不是，这里的“不同”，主要是指加密解密变换的不同．可见“密码”的内涵

中还有这两个变换. 但既有这两个变换,也就不能不联系到控制着它们的密钥.

我们以凯撒密表为例,具体地看一下上面提到的"密码"诸要素.

首先,凯撒密表必须有其加密的对象——明文集合,即所有用拉丁语明确表达的语句.

其次,任何明文经凯撒密表加密后变换成的密文,都是一个由拉丁字母组成的字符串. 这说明其密文集合就是由所有这样的字符串组成的.

第三,凯撒密表有密钥 3. 但是我们发现这个 3 并不是本质的,它也可以是 4,5,等等. 因此,这里可以有一个密钥集合,它的元素是 0,1,2,…,25. 集合中不同的密钥决定着不同的变换.

第四,密钥集合中各个密钥所决定的加密变换也组成了一个集合. 虽然这些加密变换是不相同的,但却有一个共同的算法——后移.

第五,同样,也有一个解密变换集合,相应地也有一个共同的算法——前移.

密钥集合中的一个密钥,比方说 3,作为加密的共同算法"后移"的一个参数,决定了一个具体的加密变换"后移 3". 同样,它也决定了一个具体的解密变换"前移 3". 这两个变换互为逆变换.

这样的 5 个要素,加上这些要素之间的必要关系,就形成了所谓的"移位密码",也称"凯撒密码".

一般地说,我们有如下的定义.

定义 所谓一个**密码体制**,是指由如下 5 个部分组成的一个系统:

(1) 明文集合 μ;

(2) 密文集合 π;

(3) 密钥集合 K;

(4) 加密变换集合 E 及其加密算法 e;

(5) 解密变换集合 D 及其解密算法 d.

K 中的任一个密钥 k,既作为加密算法 e 的参数决定了 E 中的一个加密变换 $e_k : \mu \to \pi$,同时又作为解密算法 d 的参数决定了 D 中的一个解密变换 $d_k : \pi \to \mu$. 并且 e_k 与 d_k 互为逆变换,即对明文集合中的任一个明文语句 M,恒有 $d_k(e_k(M)) = M$.

现在我们可以明确地说,所谓"密码",一般就是指"密码体制". 在不引起混淆的情况下,有时也指一个密钥已具体给定的密码体制.

道高一尺,魔高一丈

上面我们主要是从编制密码的角度来介绍的. 这部分内容的研究属于密码编码学. 但战争是一种对抗行为,有人在编制密码,就有人在设法破译密码. 研究破译密码的学科称为密码分析学. 而密码学,就是由密码编码学和密码分析学这两部分组成的.

密码编制学的任务是研制尽可能复杂的密码,尽量使得敌方不可能从截获的密文中得知密钥或明文. 这方面的数学理论比较完整和成熟,而且公开的文献也比较多.

与密码编码学的"防守型"研究不同,密码分析学的研究是"进攻型"的,因此也更具有挑战性. 但是,由于可以理解的原因,这方面公开的文献较少. 而且,与编制密码时所用的确定性方法不同,破译密码的方法虽然也有确定性的,但或多或少带有"尝试"和"凑巧"的成分. 在本书中,我们将介绍其中的一些经典方法,读者可从中领略到破译密码的艰辛和乐趣.

密码编制者在编制密码时,从实战的要求出发,必须假设密码分析者在着手破译一个密码时已具备了一些有利的条件. 根

据这些条件，可把破译密码的方法分为如下3类.

唯密文破译　即假设密码分析者仅掌握了一些密文(当然是由同一密钥加密的，下同)，他主要通过对这些密文的分析来推断出密钥. 显然，这样破译是比较困难的. 但反过来，对密码编制者来说，设计一个密码，使它不能被这类方法所破译，应该说是最低的要求了.

已知明文破译　即假设密码分析者不仅掌握了一些密文，还掌握了这些密文所对应的明文(比方说由情报人员窃得). 这显然没有像唯密文破译那样困难，但也并非是一件容易的事. 反过来，一个密码设计得能抵制这类破译方法，尚属差强人意.

选择明文破译　即假设密码分析者能够获得自己选择的任何明文所对应的密文(比方说，设计诱使敌方按照这些明文发出相应的密文电报，然后将这些电报截获). 由于明文是密码分析者自己选择的，它们及其所对应的密文应该提供更多的可供破译的信息. 因此，对密码分析者来说，有这样好的条件还不能破译，似乎说不过去. 但对密码编制者来说，设计的密码能抵制住这样的破译方法，应该说是很不错了.

好了，不知不觉中，我们已经迈进了密码学的大门，就要来到它的第一个展示厅了. 厅门上沿的大匾上，赫然写着："密码的历史". 让我们先进去，浏览一下琳琅满目的经典密码吧!