第一部分

基础知识

第 1 章

引子——从经典密码到量子密码

天地之化, 在高与深; 圣人之道, 在隐与匿。

——《鬼谷子 · 谋篇》

曾有人将密码学所研究的内容戏称为一部 "肥皂剧", 一部关于 Alice、Bob 和 Eve 三个人的故事[①]。故事中 Alice 和 Bob 相互发送信息, 而 Eve 则想方设法窃取这些信息。由于 Alice 和 Bob 都知道 Eve 的企图, 因此他们在发送信息的时候会竭尽所能地隐藏这些真实信息, 以防 Eve 的窃听。这部小小的 "肥皂剧" 贯穿了数千年的人类历史, 其演员下至平民百姓, 上至王公贵族、国家领导, 剧目的内容包括个人的生死与国家战争的胜败, 影响的领域遍及人们的日常生活、商业机密、军事行动和政治外交等。这部剧目中的双方斗智斗勇, 在这没有硝烟的战场上你追我赶, 相互促进发展。从利用个人智慧与想象力, 到引入系统性的数学分析, 再至依靠物理学原理。对抗双方的工作也从人工手动操作发展到计算机大规模搜索运算, 进而采用量子操作来完成。时至今日, 这部剧已经发展成为一门与人类日常生活息息相关的学科 —— 密码学。本章对密码学的基础知识做一简要概括。

1.1 什么是密码学

先来看一则关于 "美国密码之父" 雅德利[②] (Herbert Osborne Yardley, 1889—1958) 的故事, 该故事刊登在雅德利的著作《美国黑室》(*The American Black Chamber*) [2] 中。

雅德利在 1912 年受雇于美国国务院密码室, 破解密码是他的特别爱好。在第一次世界大战期间, 雅德利晋升为美国陆军部下属信号部队少尉, 并于 1917 年负责筹建和领导军事情报处第八科 (MI-8), 专门进行与密码破译有关的工作。

① 说法引自文献 [1]。Alice、Bob 和 Eve 为密码学研究中常用的三个人名。

② 雅德利照片 (图 1–1) 来自维基百科。

第一次世界大战期间，MI-8 成功地破解了超过 10000 份的国外电报，受到政府和陆军部的嘉奖。第一次世界大战结束后，MI-8 被解散，雅德利带领少数密码破译组的人员在纽约组建了新的密码局，专门负责破译外国政府的外交密码电报。由于该项行动是政府暗中提供资金支持的，因此被称为“美国黑室”。1929 年，雅德利的“美国黑室”被下令关闭，此后他出版了《美国黑室》一书以记录这段经历。雅德利在 20 世纪 30 年代末来到中国帮助国民政府建立“中国黑室”，致力于破解日本的密码。

图 1-1　美国密码学之父雅德利

在“美国黑室”成立不久，雅德利接到国务院转来的一个破译任务，是从一架飞往苏联的德国飞机上截获的 7 封密码信。其中一封的内容如下：

Fortsetzung 4.		27001.	enere	donea	zneie
stuna	ittft	velds	henrs	304.	ptlzz
tnadm	nsdti	uikgt	vrpit	eschs	agert
levwi	otnis	edsai	ahnao	tdoiu	ngetn
reros	anmrc	heeeg	nennn	etkkv	iucit
osbic	eiren	keaof	iehtg	ungsr	omtre
rnpie	esoek	eruhu	hlben	tdlkk	lotte
eoiae	lrasn	eeson	rerlh	rdtrs	rrbra
hhrpn	knlnr	zdmhe	tisri	drdes	ieebl
tanta	sehge	enare	uiish	gkdrh	gamio
rlhha	ebrac	gnaei	baikl	eces.	

密码信是该飞机在拉脱维亚迫降时被搜出的，由于拉政府没有能力破解，因此求助于美国政府。雅德利等人分析该密码信采用的是移位密码，即将原文的字母按照某种规律打乱顺序进行重排形成新的混乱文字，并通过分析辅音以及统计词频等手段成功地破解了该密码信。这些密码信是苏联间谍写给其上司的，密码信的语言是德语，破译后的原文为[①]：

1919 年 12 月 23 日快送钱来。意大利和法国急需钱。大珍珠在这里很好卖；蓝宝石在英国好卖。秘书处急需材料。在会议开始前，钱应该分配好，分钱需要通过这个中心点。11 月，保罗·莱维和布鲁斯基·翟克因尼史被选为秘书。秘书

① 密码信和译文的内容均摘自文献 [2]。

与荷兰有关系。共产主义资料已经在这里发行，我将出版俄文资料。

这些被破译的密码信引起了华府高度的重视，这是美国政府首次拥有苏联国际间谍活动的证据。在上述故事所描述的密码交锋中，存在两方势力：一方是苏联间谍和他的上司，他们试图彼此传递保密的情报消息，这就相当于小剧目中的 Alice 和 Bob；而另一方则是拉脱维亚政府、美国政府以及雅德利等扮演的窃听者 Eve 的角色，他们试图解读苏联间谍所传递的信息。苏联间谍及其上司的通信是采用书信的方式，存在被截获的可能。因此，为了避免截获者获取通信的内容，苏联间谍使用了一种特殊的移位加密方法，使得书信看起来杂乱无章，无法按正常的阅读语言来理解。由于其上司知道其使用的移位加密方法，因此可以对书信内容进行还原以获取信息。雅德利等人虽然事先并不知道该移位加密方法的具体方式，但是通过经验及对多封书信内容的分析，成功地破解了该移位加密方法，并完成了对全部书信的解密。

从这个故事中可以看出保密通信的一些特点：间谍在发送情报前假定其情报有被截获的可能，因此进行了加密以使情报内容难以理解；情报的接收方与发送方共有一些关键信息，可以帮助快速完成解密过程，以得到真正要传递的情报；破获情报后的解密行动可能由多人甚至多国完成，其用于解密的资源与力度可以说是十分强大的。

上述故事虽然只是无数使用密码的故事中的一个，但它依然能够忠实地反映出**密码学 (Cryptology)** 所研究的两个方面：

密码编码学 (Cryptography)，也称**密码术**。其所研究的是如何构建更加强大、更为难以破解的密码系统 (也称密码体制)，用以保护待传递信息的安全。上述故事中苏联间谍就是利用移位密码体制来保护待传递的情报。

密码分析学 (Cryptanalysis)。其所研究的是如何利用某一密码体制的缺陷、弱点来破解该密码体制，从而得到其保护的信息。上述故事中雅德利就是利用移位密码体制的权限通过词频统计等方法破解了密码信。

下面介绍一些密码编码学中的基本术语及常用代称 [3]：

(1) **消息 (Message)**：以某种方式记载或传递的有意义的内容，也称为信息。

(2) **明文 (Plaintext)**：未经过任何伪装或隐藏技术处理的消息。

(3) **加密 (Encryption)**：利用某种密码体制对明文进行处理使消息被隐藏的过程。

(4) **加密算法 (Encryption Algorithm)**：将明文加密成密文的规则或数学运算。

(5) **密文 (Ciphertext)**：被加密的消息。

(6) **解密 (Decryption)**：将密文恢复成为明文的过程。

(7) **解密算法 (Decryption Algorithm)**: 将密文解密成明文的规则或数学运算。

(8) **密钥 (Key)**: 进行加密和解密操作所需要的秘密参数或关键信息。

(9) **密码系统/密码体制 (Cryptosystem)**: 由明文空间、密文空间、密钥空间、加密算法、解密算法组成的一个五元集合体。其定义见定义 1.1 [4]。

(10) **Alice**: 常指代信息的发送方, 完成明文的加密过程。

(11) **Bob**: 常指代信息的接收方, 完成密文的解密过程。

(12) **Eve**: 常指代窃听者, 总是试图攻破密码系统, 获得消息明文。有时也称为**Oscar**。

定义 1.1 密码系统 密码系统是一个五元集合体 $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, 它满足以下条件:

(1) $\mathcal{P}$ 表示所有可能的明文组成的有限集合。

(2) $\mathcal{C}$ 表示所有可能的密文组成的有限集合。

(3) $\mathcal{K}$ 代表密钥空间, 由所有可能的密钥组成的有限集合。

(4) 对任意 $K \in \mathcal{K}$, 都存在一个加密算法 $e_K \in \mathcal{E}$ 和对应解密算法 $d_K \in \mathcal{D}$。且每对 $e_K : \mathcal{P} \mapsto \mathcal{C}$ 和 $d_K : \mathcal{C} \mapsto \mathcal{P}$ 均满足条件: 对每一个明文 $x \in \mathcal{P}$, 均有 $d_K(e_K(x)) = x$。

图 1-2 形象化地展示了一般密码系统的运行过程, 包含三个主要步骤:

(1) Alice 通过密钥 $K1$ 选择对应的加密算法 $e_{K1} \in \mathcal{E}$, 并使用之将明文 x 加密成密文 $y = e_{K1}(x)$, 并将密文通过信道发送给 Bob。

(2) Eve 可以在信道中获取传输的密文 y, 并试图通过之获得明文 x。

(3) Bob 通过密钥 $K2$ 选择对应的解密算法 $d_K \in \mathcal{D}$, 并在接到密文 y 之后对其进行解密, 得到明文 x。

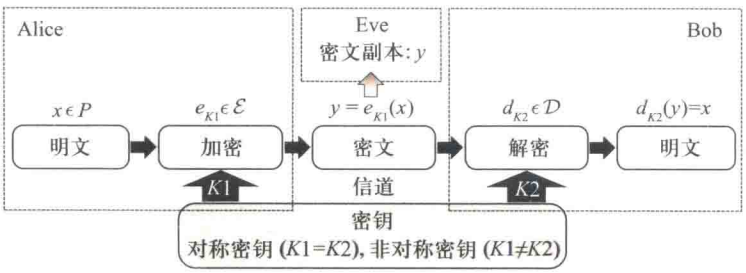


图 1-2 一般密码系统运行过程

根据 Alice 和 Bob 使用的密钥是否相同，可以将密码系统分为两类：一类是两密钥相同的**对称密码系统**；另一类是两密钥不同的**非对称密码系统**。对称密码系统出现较早，数千年前人们就开始使用各式各样的对称密码系统。而非对称密码系统出现相对较晚，20 世纪 70 年代左右才被提出。

美国通信专家香农 (Claude Elwood Shannon, 1916—2001) 在 1948 年创立的信息论中指出，一切人们所知道的文本、声音、图像、视频等都可以转换成数字形式 (经典的 0, 1 比特数据) 进行存储、传输，从而可以被计算机所处理。直到现在，通信理论并没有显著的飞跃，人们日常所需要面对与处理的信息仍是比特数据。因此，可以将密码系统的任务简化为保护 0, 1 比特数据的安全。早期密码系统设计主要利用数学复杂性，即破解一个密码系统或一段密文，相当于求解一个复杂的数学问题。这类利用数学复杂性的密码系统称为**经典密码系统**，与之相关的密码术和密码分析研究称为**经典密码学**。这里称之为经典，一方面是因为其出现时间早，研究深入，另一方面，因为其只利用到了数学，并未涉及物理原理，与本书将要介绍的量子密码学有所不同。

与经典密码学相对的是**量子密码学**，起源于 20 世纪 80 年代，其安全性基础并不依赖于数学复杂性，而是依赖于物理学中量子力学的基本原理，具有原理上的 "绝对安全性"。随着物理学与信息论的融合发展，诞生出了量子信息论 (Quantum Information Theory)，使得信息论的研究对象不再局限于经典比特数据，也包括了量子比特 (Quantum Bit, Qubit)[①]。因此，有时也将香农最初所创立的信息论称为信息论或传统信息论。在量子信息论中，信息的一种基本单元是量子比特，其可以是一个二能级量子系统中的任意量子态。量子信息也同样面临着如何保密存储、传输的问题，相对应的，就存在量子密码学。由于量子信息的存储、传输等均要受到物理学规律的限制，因此量子密码在原理设计上是从量子力学的原理出发，以物理原理来保证信息安全。其既可以用来保护比特数据的安全，也可以保护量子比特数据的安全。

下面首先简要介绍经典密码学的发展历程，与密码系统的安全性定义，而后简要介绍量子密码学。

1.2 经典密码学发展简介

人类对于密码的使用可以追溯至数千年前，在漫长的发展过程中，经典密码学经历了四个高速发展期，分别是文艺复兴时期、第一次世界大战期间、第二次世界大战期间、第二次世界大战后直至现在。其中，直至第二次世界大战结束，密码系统虽然越来越复杂，但其并无原理层面的本质突破，因此常被称为古典密

① 具体定义与介绍见后文。也存在其他基本单元，取决于所使用量子系统的维度。

码 (Classical Cryptography)。而从第二次世界大战时数学家开始广泛介入密码研究，到第二次世界大战结束后香农创立信息论，为密码学研究明确了数学基础开始，密码学才正式成为具有系统研究的学科。自此以后的密码常被称为是现代密码 (Modern Cryptography)，尤其是非对称密码 (也称公钥密码) 的出现，其从思想上与古典密码大不相同，拓宽了密码学的应用范围。

1.2.1 古典密码

保密通信的需求在人类社会诞生文字之后不久就产生了。无论是在中国或西方，密码学最早的系统性应用都是在军事领域。例如，中国古代军事著作《六韬》[①](又称《太公六韬》或《太公兵法》) 中前集第三卷《龙韬》中的《阴符》篇所述，以八种不同长度的 "阴符" 来表示两军交战的战果，而每种长度所代表的含义则由在外将领和君主事先约定好。

《龙韬 · 阴符》【原文】

武王问太公曰："引兵深入诸侯之地，三军猝有缓急，或利或害。吾将以近通远，从中应外，以给三军之用。为之奈何?"

太公曰："主与将，有阴符。凡八等：有大胜克敌之符，长一尺；破军杀将之符，长九寸；降城得邑之符，长八寸；却敌报远之符，长七寸；誓众坚守之符，长六寸；请粮益兵之符，长五寸；败军亡将之符，长四寸；失利亡士之符，长三寸。诸奉使行符，稽留者，若符事泄，闻者告者皆诛之。八符者，主将秘闻，所以阴通言语，不泄中外相知之术。敌虽圣智，莫之能识。"

武王曰："善哉!"

【译文】

武王问太公说："率领军队深入到敌国境内，三军突然遭遇紧急情况，战事可能顺利也可能失利。我想与远近各军相通，以国内策应国外，供给三军的需求，应当怎么办?"

太公答道："君主与主将之间使用秘密的兵符联系。阴符共分为八种：代表我军大获全胜、攻克敌军的阴符，长度为一尺；代表攻破敌军、擒杀敌将的阴符，长度为九寸；代表敌军投降、占领敌人城邑的阴符，长度为八寸；代表击退敌人、远报战况的阴符，长度为七寸；代表誓师率众坚守的阴符，长度为六寸；代表请求补给粮草、增加兵力的阴符，长度为五寸；代表军队失败、将领阵亡的阴符，长度为四寸；代表战斗失利、士卒伤亡大的阴符，长度为三寸。凡是奉命传递阴符的，如果延误时限，泄露、听到和传告机密的，都一律处死。这八种阴符，由君主和将

① 相传为西周太公望 (又名姜子牙，约公元前 1128—前 1015) 所著，以问答形式阐述军事理论。

帅秘密掌握，是一种暗中传递消息而不泄露朝廷和战场机密的通信手段。这样，即使敌人有十分高深的智慧，也无法识破它的奥秘。”

武王说：“很好!”

阴符的使用可以增加军情传递的安全性，且每次出征前君主和主将可以对不同长度符的含义进行重新的定义，以增加安全性。这种加密方法属于“替换法”，军情就是消息明文，符就是密文，事先约定好的符的长度与军情含义之间的关系就是密钥。显然，主将需要和君主掌握同样的密钥才能完成对军情消息的正确解读，因此阴符系统属于对称密码系统。

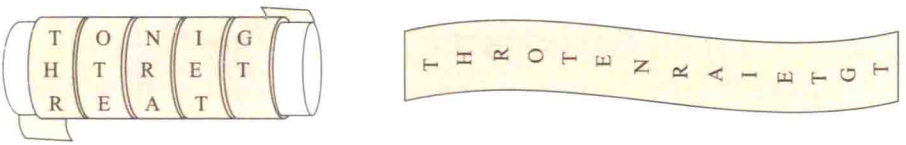
使用阴符来传递军情只有八种不同的情况，可以传递的信息量较小。后来人们发明了类似的可传递更多军情种类的加密方法，比如北宋时期官修的兵书《武经总要》中所述“字验”一节，在偏裨将出征前与主将约定好 40 种不同的军情与一首含 40 个不同字的诗中每一个字的对应关系，传送军情时只需写一封普通的书信或文件而在关键字之旁加印记即可。这 40 种军情为：

今约军中之事，略有四十余条，以一字为暗号：

请弓、请箭、请刀、请甲、请枪旗、请锅幕、请马、请衣赐、请粮料、请草料、请车牛、请船、请攻城守具、请添兵、请移营、请进军、请退军、请固守、未见贼、见贼讫、贼多、贼少、贼相敌、贼添兵、贼移营、贼进兵、贼退兵、贼固守、围得贼城、解围城、被贼围、贼围解、战不胜、战大胜、战大捷、将士投降、将士判、士卒病、都将病、战小胜。

宋代的“字验”方法后来发展为军事、外交中常用到的密码字典，极大地扩充了可加密的明文空间大小，使得可以安全传递的消息种类大大增加。

在西方，密码的使用同样有悠久的历史。大约在公元前 700 年，古希腊的军队使用一种叫作 Scytale 的圆木棍来进行保密通信 (见图 1-3)，其使用方法为：① 把用于书写情报的羊皮纸带紧密缠绕在一根圆木棍上，然后沿棍身横向书写



明文:
TONIGHT RETREAT
今晚撤退

密文:
THROTENRAIETGT
???

图 1-3 古希腊军队 Scytale 圆木棍加密法示意

(假设该木棍可写下三行单词 (为直观显示均写在了同一面)，则明文 “TONIGHT RETREAT” 在展开后的羊皮纸带上显示为无意义的 “THROTENRAIETGT”。)

需要传递的消息; ② 将羊皮纸带解下, 则顺着羊皮纸带方向的文字就显示为混乱无意义的单词, 将羊皮纸带传递给接收方; ③ 接收方使用相同直径的圆木棍将羊皮纸带缠绕上去就可以读出原始传递的信息。据传这种加密方式主要是古希腊城邦中的斯巴达人 (Sparta) 在使用, 因此又被称为 "斯巴达棒"。在 Scytale 这种加密方法中, 需要传递的语句就是明文, 羊皮纸带展开后的无意义的字母组合就是密文, 木棍的直径就是 "密钥"。该加密方法属于 "换位法", 前文中提到的苏联间谍使用的加密方法也属于 "换位法"。

另一个著名的例子是凯撒加密法。2100 年前, 古罗马的执政官和军队统帅凯撒 (Julius Caesar, 公元前 100—前 44) 发明了一种将所有字母按照字母表顺序循环移位的文字加密法。比如向后移动 5 位, 则将字母 a 写成 e, b 写成 f, ……, z 写成 d。按照此规则加密前面例子中的句子 "tonight retreat" 就会得到无法直接阅读的密文 "ytsnlmy wjywjey"。可以看出, 在此加密方法中, 要传递的语句是明文, 每个字母分别替换之后的无意义字母组合就是密文, 字母表的移位位数就是密钥。该方法与 "字验" 方法类似, 均属于替换法。后人为方便加解密, 根据凯撒加密法的原理制作了移位加密圆盘 (见图 1–4)。盘的内圈和外圈分别是两个字母表, 转动外圈圆环不同的格数, 就可以形成不同的移位值, 从而组成不同的凯撒替换密码表。

图 1–4 应用凯撒密码的移位加密圆盘

上述几个例子都是早期古典密码学的代表, 虽然结构简单, 但其基本思想却一直延续到第二次世界大战结束, 只是密码系统的结构变得更加复杂, 因此虽然直至第二次世界大战结束密码学的发展经历了三个高峰, 但都可以归为古典密码学的范畴。

与古典密码编码学相对立的密码分析学也发展迅速。据记载, 阿拉伯民族从公元 7 世纪开始就进行了关于密码的系统总结, 在中世纪的时候就广泛地将密码应用到国家事务当中。相应地, 其密码分析学也有系统性的发展。1987 年, 人们发现了公元 9 世纪伟大的阿拉伯哲学家、自然科学家肯迪[①] (公元 801—873) 所著的《解码手册》(*On Deciphering Cryptographic Messages*) 一书, 该书最早明确提出使用 "频率分析法" 来破解替换密码。书中相关的描述如下:

> 如果我们已经知道了一份密文所使用的语言, 要破解它的一种方法是找一份用同样语言写的明文, 大约有一页纸的长度。然后数其中每个字母出现的次数; 把出现频率最高的字母称为 "第一", 出现频率第二高的字母称为 "第二", 依此类推, 直到数完所有的明文字母。

① 全名 Abu Yūsuf Ya'qūb ibn 'Ishāq as-Sabbāh al-Kindī, 公认的阿拉伯第一位哲学家。

然后再看要破解的那份密文，对其中的符号同样根据出现频率进行排序。我们找到出现频率最高的那个符号并把它替换为明文统计中的“第一”字母，找到出现频率第二高的符号并把它替换为明文统计中的“第二”字母，依次将密文中的字母全部都完成对应的替换。

频率分析法是破解一般替换密码十分有效的方法。后来人们对多种日常使用语言进行了大量的频率统计，不仅是单个字母出现的频率，还包括双字母、三字母等。此外，对单词的特性也进行了大量总结，比如在一个英语单词中同一字母出现次数大于一的被称为模式词 (Pattern Word)，模式词的数量并不多，常被按照出现频率编辑成模式词列表以方便快速查询。

从历史上来看，西方密码学的后续发展比起中国要更为丰富与迅速，历史因素不断地促进着密码学的演进。古典密码学所迎来的第一个发展高峰是在文艺复兴时期。

在摆脱了漫长的中世纪黑暗之后，13 世纪末期，从意大利开始，欧洲近代三大思想解放运动之一的文艺复兴运动逐渐开始横扫西欧大陆。欧洲诸国开始进行现代意义上的外交活动，在他国建立大使馆并互派大使。由于身处异国的各国大使向国内传递信件大部分只能通过公共邮政系统，因此即便是涉及机密情报的信件也极有可能被人截获。事实上，各国情报机构也确实在肆意拆看这些外交信件。因此，各国驻外大使就需要想尽办法对要传递的信息进行加密，这就促进了密码编码学的发展；同时各国情报机关绞尽脑汁破解密信的行为也大大促进了密码分析学的发展。16 世纪，资本主义的发展使得资产阶级与封建统治和宗教神权的矛盾愈演愈烈，欧洲近代三大思想解放运动之二的基督教改革运动逐渐兴起。由于事涉敏感的教义问题，为避免宗教迫害，相关人士的书信往来也常使用加密方法，这也间接促进了密码学的发展。在这一时期，古典密码学迎来其发展的第一个高峰。

在密码编码学发展方面，为了应对频率分析法，人们提出了“**多字母表替换加密法**” (Polyalphabetic Substitution Cipher)。如前所述的凯撒移位密码等各种替换密码由于通篇加密过程同一个明文字母只会被替换为同一个密文字符，因此被称为“**单字母表替换加密法**” (Monoalphabetic Substitution Cipher)。而在多字母表替换加密法中，同一个明文字母在明文中不同位置按照规则可以被替换为不同的密文字符，如此则频率分析方法的效用大大降低。由于字母替换表和替换规则可以设计得十分复杂，因此这种方法一直到第二次世界大战之后还偶有使用。此类密码中早期比较著名的是维吉尼亚加密法 (Vigenère Cipher)，相传发明于 16 世纪。

图 1-5 给出了一个简单的维吉尼亚加密表的例子，表中第一行代表明文字母，其下面代表可能被替换的密文字符，可以看出，每一个字母有 26 种不同的替

换选择。第一列代表选择密钥，譬如密钥选择为 C 时，就用 C 这一行的字符来替换明文字母，即第一行字母和 C 这行字母组成了一个仅临时使用一次的“单字母替换加密表”。图 1-5 中所示的维吉尼亚加密表生成法是：每一行均是 26 个字母顺按照字母序循环排列得到，第 n 行的首字母就是第 n 个字母。维吉尼亚加密表的使用方法是：

	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
A	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
B	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	A
C	C	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
D	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
E	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	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

图 1-5　简单的维吉尼亚加密表

(1) 首先在通信前双方约定好密钥字母串，如单词 hello。

(2) 而后将密钥字符串重复若干次并顺序排列，直至超过要传递的信息长度。比如要传递的信息为 “tonight retreat”，则就将 hello 重复三遍。

(3) 将明文序列和密钥序列进行排序，每一个明文字母的加密密钥就是对应位置的密文字母，使用密文字母对应行的替换规则对明文字母进行替换。例如，第一个明文字母 t 对应的密文字母为 h，则在图 1-5 中找到 h 这一行，并查得字母 t 所对应的替换字母为 a，则将 t 替换为 a。如此则全部密文是无意义的字母序列：

密钥:	h	e	l	l	o	h	e		l	l	o	h	e	l	l
明文:	t	o	n	i	g	h	t		r	e	t	r	e	a	t
密文:	a	s	y	t	u	o	x		c	p	h	y	i	l	e

(4) 解密的时候进行相反的查找操作即可。

在维吉尼亚加密法中, 密钥包含两部分: 加密表和密钥字母串。图 1-5 中所展示的加密表仅是构造最为简单的一种, 事实上, 加密表并不限于只有 26 行, 只要是对明文字母的有效单字母替换表都可以成为维吉尼亚字母表的一行。密钥的选择也不仅是不断重复初始密钥这一简单方法, 更可以通过短的初始密钥生成长的更加无序的密钥序列, 甚至还可以将明文作为后续的密钥使用。由于可以不断地设计出更为复杂的加密表和密钥, 因此多表替换加密思想不断发展并被使用了很长时间。

在这一时期以维吉尼亚加密法为代表产生了许多新的加密方法, 密码设计更像一门艺术, 人们依靠自己的灵感, 各展才华。这为解密工作的进行造成了很大的困难。因此, 自 18 世纪起, 欧洲各国逐步建立起专门的解密机构, 专门截获和破解驻留本国的外交人员的密信。这些机构被称为黑室 (Black Chamber)。黑室的流程化截获、破解方式极大地提高了密码破解的效率, 据称以维也纳的黑室为最, 其典型的一天工作流程可概括如下[①]:

✓早上 7:00 当天寄给驻维也纳大使的邮件均被带到黑室中, 通过蜡烛将封口化开, 将信件取出交给专门负责抄写的人, 并同时记录信件的顺序, 当抄写完毕后将邮件以正确的顺序放回, 并用伪造的印章重新做好蜡封。而后于 9:30 将邮件送回邮局进行正常投送。

✓上午 10:00 经由维也纳寄往他国的邮件也会同样经历一番上面的待遇。下午 4:00 由驻维也纳的各国大使寄出的邮件同样要经历一番上面的待遇。

✓抄写的邮件由专人负责阅读分类, 所有欧洲的语言均有专人掌握。将加密邮件进行破解后, 根据内容通知相关的部门, 如警察、火车站等。一个 10 人组成的特殊队伍平均每天可以解读 80 ~ 100 封邮件。

密码学的第二个发展高峰是在第一次世界大战期间。经历了文艺复兴后欧洲密码学的发展热潮后, 密码的应用已经逐渐深入到欧洲诸国的各个角落, 大范围使用密码来保护信息的安全已经成为人们的常识。1837 年, 美国艺术家与发明家莫尔斯 (Samuel F. B. Morse, 1791—1872) 发明了有线电报, 使得信息可以莫尔斯码 (Morse Code) 的形式更为迅捷地传递。1896 年前后, 意大利发明家马可尼 (Guglielmo Marconi, 1874—1937) 发明了无线电报, 使得电报的发送脱离了线缆的束缚, 信息的及时传递变得更为灵活。有线和无线电报的发明改变了人们传递信息的方式, 使世界进入了电子通信时代。

"知己知彼, 百战不殆", 及时有效的军情传递是战场制胜的法宝。有线和无线电报发明后, 迅速成为了军事情报传递的主要方法。然而有线电报受限于预先铺设的线路, 很容易在线缆无人看管的地带被窃听或破坏, 如野外或是海底; 而无线电报虽然不受线缆的限制, 但它是一种广播性质的通信方法, 原则上任何

① 参见文献 [5] 第五节:The Era of the Black Chambers。

人都可以接收到无线电报的内容。因此，为了保证电报所传递的情报不被敌人所获取，电报内容的加密就十分重要。第一次世界大战波及面十分广，各国为了这场涉及生死存亡的战争的胜利，均大力发展密码学。

第一次世界大战期间的密码学虽快速发展，但其在理论上并未突破古典密码学的范畴，只是在形式、密钥复杂度方面不断加强。作战部队以及间谍常配有密码本，根据密码本定时更改密码系统的关键参数，以增加密码系统的复杂度，使之更难以破解。为了破解越来越复杂的密码，各国军队都设立了专门从事密码破解的部门，其中比较著名的有英国海军部的“40 号房间”和美国陆军部的“军情第八科”(MI-8，即前文中由雅德利所领导的“美国黑室”)。这些部门所破解的情报对协约国的胜利有着至关重要的作用。

1914 年，英国对德宣战的同时，英国海军就切断了德国穿越大西洋的海底电缆，使德军不得不依靠无线电报来对海外战场进行通信联系，从而使英军轻易地获得了德军大量的无线电报密文。为了使这些密文变为有价值的军事情报，英军于 1914 年 10 月成立了一个专门破解密码的小组，其办公所在地是英国旧海军大楼第 40 号房间，因此被称为“40 号房间”。在“40 号房间”成立前后，英军截获了多个德军的密码本以及大量与德军密码系统相关的资料，大大加速了英军对德军密码的破解。其中比较著名的是 1915 年 3 月，英国获得了在中东积极活动的德国外交官瓦斯慕斯所使用的德国外交部密码本，该密码本对英国破解德国外交部部长齐默尔曼 (Arthur Zimmermann，1864—1940) 的一封外交密电起到了重要作用，直接导致了美国的参战，加快了第一次世界大战的胜利进程。该次破解也被认为是历史上最为成功的一次密码破解案例。

德国外交部部长齐默尔曼于 1917 年 1 月 16 日发往德国驻美大使馆的电报被窃听之后送往了“40 号房间”，由于英国已经获得了德国外交部的密码本，因此该秘密电报很快便被破解。该电报要求德国驻美大使在合适的时候交给墨西哥总统。电报中称德国将进行“无限制海战”，用潜艇攻击包括美国等中立国在内的海上商运船，并希望墨西哥对美宣战以牵制美国，作为交换条件，承诺帮助墨西哥从美国手中夺回得克萨斯、新墨西哥和亚利桑那等州。这封电报成为了英国人将美国拖入战争的绝佳机会，但是为了不使德国知道英国已经破获了其在德国外交部本部使用的密码，英国故意等到德国驻美大使按照电报要求，将内容以另一套更为老旧的密码加密转发给德国驻墨西哥大使后，再次截获该电报并解密后才将内容透露给美国。美国在获悉德国的意图之后，于 1917 年 4 月 6 日正式对德宣战。美国的加入使德国在第二年就宣布投降。

据称，“40 号房间”在第一次世界大战期间共破译了超过 15000 份德国密电，对战争的胜利做出了巨大贡献。此外，据称雅德利领导的“美国黑室”在第一次世界大战期间也破获了超过 10000 份的外国密电，同样为战争胜利做出了

巨大贡献 [2]。

第一次世界大战期间虽然由于战争原因, 加密和解密技术的发展十分迅速, 加密系统更为复杂, 解密的投入力量也不断增强, 但作为一门学科, 其基本原理并无很大变化, 甚至在加解密的方式上都仍然靠手工进行。

第一次世界大战使各国进一步明白了密码的重要性, 没有什么比洞悉敌人的秘密能更有效地打击敌人, 也没有什么比保护自己的秘密更能确保己方的胜利。因此, 各国政府在密码系统和密码分析两方面都加大投入, 使得无论是在密码理论还是应用方面, 都发生了革命性的变化。

在技术方面, 基于机械和电气的加解密装置全面取代了以往的手工密码, 最著名的就是德国的 "隐谜" (Enigma)[①] 密码打字机和 "洛伦兹" (Lorenz) 密码电传机, 以及基于波兰数学家破解 "隐谜" 密钥理论而产生的各种 "炸弹" (Bomba)[②] 破译机, 后来甚至电子计算机也开始介入。在密码学理论方面, 大量的数学和统计学知识被应用于密码的分析和破解, 越来越多的数学家不断加入密码队伍, 以更为严谨的数学分析代替以往的个人灵感成为密码战场上的主力军。这一时期由于大量使用机械和电气装置来进行加解密, 其效率远远超过手工处理能力, 因此被称为机器密码阶段。

德国的 "隐谜" 密码打字机主要包括四部分 (见图 1–6)。

(1) 键盘: 包括 26 个字母, 没有标点符号, 用于明文 (或密文) 的输入。

(2) 指示灯面板: 该面板上有 26 个可以亮起的字母, 当敲击键盘上的某个字母时, 对应的加密 (或解密) 后的字母就会亮起。

(3) 转轮组和反射器: 转轮组是整个加密机中最为重要的组成部分, 共由 3 个独立的圆形转轮组成 (见图 1–7), 转轮处于整个机器的内部, 仅露出部分齿状边缘, 可以看到上面的数字或字母。每个转轮的边沿是齿状的, 方便从外部拨动位置, 且齿状边沿旁边有 26 个字母或是数字, 用以确定当前转轮的位置。每个转轮代表一个单字母替换表, 多个转轮代表多个单字母表替换加密法的级联。因此, 当 3 个转轮中的任何一个转动的时候都会使得总字母替换表变化, 形成新的替换加密。反射器置于转轮组的一侧, 是一个字母对换表, 其最大的作用是使加密与解密过程是对称的。

(4) 插孔板: 插孔板位于键盘下方, 上面有 26 个插孔, 代表 26 个字母。当使用一根电线将插孔板的 2 个字母相连时, 代表对这两个字母做了对换。例如, 将 B 和 C 连起来, 按 B 键时代表的是 C, 按 C 键时就代表 B。密码机工作时需连接若干不同的插孔对字母进行对换, 如连接 5 对字母。

---

① 也有音译为 "英格玛" "恩尼格玛" 的, 为德国电气工程师谢尔比乌斯 (Arthur Scherbius) 于第一次世界大战后所发明。

② 波兰发明的 "炸弹" 机称为 Bomba, 英国发明的 "炸弹" 机则称为 Bombe, 两者的原理并不同。

图 1-6 “隐谜”密码打字机

图 1-7 “隐谜”密码打字机中的转轮

在“隐谜”密码打字机中，决定最终总的加密函数的因素有：转轮的数量、每个转轮所代表的单字母替换表、反射器所代表的字母对换表、各转轮的位置、插孔板中对换字母对的数量及如何对换。而在加密时，每敲击一下键盘，最低位的转轮就转动一下，每当低位的转轮转动一圈，其相邻的高位转轮就转动一下。而任一转轮的转动就代表着加密函数的变化，不难想象，设计良好的“隐谜”密码打字机就相当于一个拥有非常多行的维吉尼亚加密表，且密钥的长度也足够长，使得加密规则的循环周期相当长。以 3 个转轮和 5 对插孔板对换字母对的机器为例：

3 个转轮组的位置排列可能数目：$3! = 6$。

3 个转轮组的初始位置可能数目：$26^3 = 17576$。

插孔板上 5 对对换字母可能数目：$C_{26}^{10} \times C_{10}^{5} \times A_5^5 \times 1/2^5 = 5019589575$。

3 个转轮组转动的复位周期数目：$26^3 = 17576$。

除去加密表复杂多变这一优势，“隐谜”密码打字机还具有以下优势：转轮的数量、每个转轮所代表的单字母替换表、反射器所代表的字母对换表等都可替换，使得生产不同型号的密码系统变得十分容易；由于反射器的存在，使得加解密操作是完全对称的，即通过键盘敲击明文则得到密文，而敲击密文则可以直接得到明文，此对称的加解密方式大大增加了加解密的速度，提高了实用性。

由于“隐谜”密码打字机具有如此多的优势，使其深受德军重视，并在部队中进行了全面列装，为德国在第二次世界大战前期带来了巨大优势。但是对“隐谜”密码打字机安全性的迷信，使德军忽略了其并不是不可破解的密码系统这一事实，导致其在战争后期频频受创。对“隐谜”密码打字机的破解主要归功于数学分析和具有大规模计算能力的破解机 (后续发展出了电子计算机)。由于并非本书的主要目的，因此在此简化数学细节，仅对人们对破解“隐谜”所做努力

做简要介绍。

事实上, 随着科技水平的整体进步, 密码系统越来越复杂, 依靠个人能力进行手工破解也就越来越不现实。依靠数学分析来寻找密码系统的设计缺陷, 并借助计算机的搜索计算能力进行密码系统的破解, 也是密码分析学势在必行的选择。

最先引入数学家参与到密码破解行动的是波兰军方的密码局, 早在 1919 年时就曾有波兰数学家参与破译了苏联人的密码。因此, 当 1928 年波兰密码局发现德国使用了全新的 "隐谜" 密码打字机后, 1929 年波兰波兹南大学数学系就秘密开设了 "密码学" 这门课程。在层层筛选之下, 三名优秀的年轻人被留了下来, 他们是雷耶夫斯基 (Marian Rejewski, 1905—1980)、齐加尔斯基 (Henryk Zygalski, 1908—1978) 和鲁日茨基 (Jerzy Różycki, 1909—1942)。这三位年轻的数学家对破解德国 "隐谜" 密码打字机起到了至关重要的作用[①]。他们将 "隐谜" 密码看作数学上的对 26 个字母进行不断的置换, 利用 "隐谜" 密码打字机本身的结构特性 (字母间是对换的) 以及德军密电的格式缺陷 (转轮位置总是发送两遍), 提出了破解方法, 并设计出回转机 (Cyclometer) 来制作查找表, 以提高破解速度。在查找表已知的情况下, 只需要每天监听到足够多的密电, 将关键信息统计后通过查表就可以得到当天的转轮初始位置和次序设定; 再通过一些语言学分析得到插孔板置换的信息, 就完成了当天 "隐谜" 密码的破解!

虽然后来德国改变过发送密电的格式, 也增加过转轮的个数, 但是其映射是对换这个弱点从来都未改变。后来波兰人又设计出了 "炸弹" 机, 是回转机的改进版, 相当于将 6 台 "隐谜" 密码打字机连在一起, 其只需要 2 h 就可以计算出转轮的位置和插孔板的连线方式。

波兰沦陷后, 英国密码专家们接过了继续破解德军 "隐谜" 密码的任务, 在布雷契莱 (Bletchley) 庄园成立了 "政府密码学校"。在布雷契莱庄园中, 著名的现代计算科学开创者图灵 (Alan Mathison Turing, 1912—1954) 发现了 "隐谜" 的另一个缺陷: 不能将一个字母映射为自己。针对此缺陷, 图灵设计了破解 "隐谜" 的 Crib 方法。据统计, 使用该方法大约只需要 30 个字符长的已知明文就可以完成对 "隐谜" 的破解。为了获得尽可能长的已知明文, 除了有时可利用德军密电的一些特殊格式, 如日期、天气等之外, 英军会故意散布一些虚假情报或刻意做出某些军事安排, 使得德军向上级汇报的密电中包含特定的关键词[②]。图灵方法的好处在于不针对任何特殊电文格式, 无论德军如何修改密电发送方式都不会影响此方法的有效性; 其缺陷是依靠人力无法完成这个任务。因此英国人设计了新的 "炸弹" 机: 1940 年第一台 "炸弹" 机完成, 相当于 36 台 "隐谜" 密码打字机的组合, 1941 年 "炸弹" 机的数量增加到 16 台, 1943 年增加到 49 台,

① 对这三位波兰数学家破解 "隐谜" 密码打字机的较详细介绍可以参考文献 [1] 第四章。

② 这种获取特定明文的方法被称为 "种花" (Gardening), 参考文献 [1]。