第5章 密码分析基础

一天，老板 Alice 发现一份急需的商业文件的解密密钥丢失了，于是找来 Bob 解决密钥丢失问题。当拿到密文文件时，Bob 需要做的工作是如何破译这份密文文件，此时 Bob 要进行密文分析将面临以下问题。

（1）能否选取一部分密文进行分析，进而破解出加密的密钥？此时可以利用破译的信息较少，是否有更多的信息用于破译呢？

（2）进一步分析，是否有一些密文对应的明文是知道的或者是可以猜测出来的？

（3）更进一步分析，在已知的明文和其对应的密文片段中，能否找到有利于破译的片段，或者知道加密算法？

（4）如果既知道一些有利于破译的明文-密文片段，又知道加密算法，就可能推出加密的密钥或者等效密钥。

从上述几个问题可以看出，这几个问题的破译难度是从难到易的，也是一个密码破译的分析过程。

本章将开启密码算法的破解之路。首先学习密码分析的概念和目标、攻击者类型以及密码分析方法，其次学习古典密码的分析方法及实例，最后介绍密码设备的侧信道攻击方法。

密码学包括密码编码学和密码分析学两部分。密码编码学是研究设计构造一个符合规定安全要求的密码系统，即如何设计相应的加密和解密算法、密钥和安全协议，使得密码系统能够达到所需要的安全性。密码分析学是研究在解密密钥和密码体制未知的情况下如何恢复明文的科学。这两部分既对立又统一，正是这两者的对立和统一推动了密码学的发展。密码分析学的具体内容涉及很多数学和计算机的知识，本章将从密码分析的概念、基本原理及方法等进行阐述。

5.1 密码分析介绍

本节主要介绍密码分析的基本原理和概念等。密码分析也称密码破译，是密码分析人员在系统密钥未知的情况下设法破解系统的密钥或者获取明文的过程。一个成功的密码分析不仅能够恢复明文消息和密钥，而且能够发现密码体制的弱点，从而控制通信。加密与破译始终是一对“孪生”的问题，随着密码技术的出现，也出现了各种试图对密码进行

破译的技术和方法。原则上，密码分析是攻击者为了窃取机密信息所做的事情，但是这同时也是密码体制设计者的工作。当然，设计者的目的是分析体制的弱点，提高密码体制的安全强度。密码技术就是在与密码破译技术的对立矛盾中不断发展、前进的。此外，密码分析在外交、军事、公安、商业等方面都具有重要作用，也是研究历史、考古、古语言学和古乐理论的重要手段之一。

如果密码分析者可以仅由密文推出明文或密钥，或者可以由明文和密文推出密钥，那么就称该密码系统是可破译的。相反，则称该密码系统是不可破译的。

密码设计和密码分析是共生的，又是互逆的，两者密切相关但追求的目标相反。两者解决问题的途径有很大差别。密码设计，特别是在现代密码体制中，主要利用数学构造密码。密码分析除依靠数学、工程背景、语言学等知识外，还要靠经验、统计、测试、眼力、直觉判断能力等，有时还靠运气。

一个密码体制是安全的，其前提是假设密码分析者已经知道了密码体制的具体算法，即密码体制的安全性仅应依赖于对密钥的保密性，而不应依赖于对算法的保密，符合柯克霍夫原则。这一原则是密码系统设计的重要原则之一，是荷兰密码学家柯克霍夫于 1983 年在著名的《军事密码学》中提出的一个重要原则：密码系统法即使为密码分析者所知，也应该难以从截获的密文中推导出明文和密钥。只有在假设攻击者对密码算法有充分的研究，并且拥有足够的计算资源的情况下仍然安全的密码，才是安全的密码系统。总之，“一切秘密寓于密钥之中”。

5.1.1　密码分析的目标

密码分析的目标是研究发现、开发和纠正密码算法本身的弱点，根据这些弱点不但可以对密码进行破译，还有助于设计更好的密码算法。密码攻击的目标有不同的层次，可以分为如下 4 种。

1. 完全攻破(Total Break)

发现密码系统所用的密钥，使得所有密文均可破译，并且攻击者可以按照自己的需要产生假冒的密文。

2. 全局演绎(Global Deduction)

攻击者找到解密算法的一个等价算法，无须密钥便可进行解密。

3. 局部演绎(Local Deduction)

攻击者发现一个或多个密文所对应的明文，这将为发现实际使用的密钥提供线索，对有些算法还可实施完整性攻击。

4. 信息演绎(Information Deduction)

密码分析者发现了与实际系统使用的密钥或明文有关的信息，如密钥的部分、明文的格式甚至是一些关键词等，这些信息将有助于进一步进行密码分析。

5.1.2　密码分析的攻击者类型

开展密码分析研究是遵循柯克霍夫原则的，且以获取密码算法的密钥为目标。在信

息的传输过程中，除了信息合法的接收者，还可能存在通过各种手段截获信息的第三方窃听(截获)者。他们虽然不知道密码系统的加密密钥，但通过分析手段可能会从截获的密文推断出原来的明文，这一行为称为密码分析或密码攻击。

根据密码分析者破译时对密码系统的明文、密文等数据资源的掌握程度，通常密码分析的攻击者类型分为以下 4 种。

1. 唯密文攻击(Ciphtext-Only Attack)

唯密文攻击是指攻击者只有一段或几段由相同密钥和加密系统加密的密文信息，记为 $c_1,c_2,\cdots,c_n$。密码分析的任务是从这些密文信息中获得相应的明文，记为 $p_1,p_2,\cdots,p_n$；或者破译出加密系统或算法 E_k 相应的密钥或等效的密钥，记为 k。这种类型的密码分析攻击可表述为

已知：$c_1=E_k(p_1),c_2=E_k(p_2),\cdots,c_n=E_k(p_n)$。

目标：推导出 $p_1,p_2,\cdots,p_n$ 或密钥 k。

由于密码分析者所能利用的数据资源仅为一些密文，因此可用的信息量较少，这是对密码分析者最不利的情形。

2. 已知明文攻击(Plaintext-Known Attack)

已知明文攻击是指攻击者不但获取了一些密文，还有这些密文对应的明文，即一些“明文-密文对”，分别记为 $p_1,p_2,\cdots,p_n$ 和 $c_1,c_2,\cdots,c_n$。密码分析的目标是利用“明文-密文对”推出加密系统或算法 E_k 的密钥或等效密钥 k，并对新的密文信息进行解密。这种类型的攻击常常是合理的，其表述为

已知：p_1 和 $c_1=E_k(p_1),p_2$ 和 $c_2=E_k(p_2),\cdots,p_n$ 和 $c_n=E_k(p_n)$。

目标：推导出密钥 k，或获得从新截获的密文 c_{n+1} 推出对应明文 p_{n+1} 的算法即通过 $c_{n+1}=E_k(p_{n+1})$ 推导出 p_{n+1}。

3. 选择明文攻击(Chosen-Plaintext Attack)

在选择明文攻击中，密码攻击者不仅可得到“明文-密文对”，还可以选择对破译有利的一些“明文-密文对”，明文记为 $p_1,p_2,\cdots,p_n$，密文记为 $c_1,c_2,\cdots,c_n$。密码分析者的目标也是利用“明文-密文对”p_1-c_1,p_2-$c_2,\cdots,c_n$-p_n 推出加密系统或算法 E_k 的密钥或等效密钥 k，且可对新的密文消息进行解密。这种类型的密码分析攻击可表述为

已知：p_1 和 $c_1=E_k(p_1),p_2$ 和 $c_2=E_k(p_2),\cdots,p_n$ 和 $c_n=E_k(p_n)$，其中 $p_1,p_2,\cdots,p_n$ 可由密码分析者选定。

目标：推导出密钥 k，或获得从新截获的密文 c_{n+1} 推出对应明文 p_{n+1} 的算法，即通过 $c_{n+1}=E_k(p_{n+1})$ 推导出 p_{n+1}。

与已知明文攻击相比，选择明文攻击更有效，因为攻击者可以选择一些特殊的明文进行加密，这些明文可以暴露出更多与密钥有关的信息。在日常的计算机文件系统和数据库系统中，此类攻击最容易遇见，原因是用户可以任意选择明文并获得相应的密文文件和密文数据库。

4. 选择密文攻击(Chosen-Ciphertext Attack)

选择密文攻击是指攻击者可以选择一些有利于破译的密文信息及相应的明文，分别

记为 $c_1,c_2,\cdots,c_n$ 和 $p_1,p_2,\cdots,p_n$。密码分析者的目标是利用选择的 p_1-c_1，p_2-c_2，…，c_n-p_n推出加密系统或算法 E_k 的密钥或等效密钥 k。这种密码分析主要用于攻击公钥密码体制。例如，攻击者可以通过访问该密码系统的自动解密装置，产生任何密文所对应的明文。这种类型的密码分析攻击可表述为

已知：c_1 和 $p_1=D_k(c_1)$，c_2 和 $p_2=D_k(c_2)$，…，c_n 和 $p_n=D_k(c_n)$，其中 $c_1,c_2,\cdots,c_n$ 可由密码分析者选定。

目标：推导出密钥 k。

选择明文攻击和选择密文攻击经常一起使用，被称为选择文本攻击。在以上密码分析攻击中，对攻击者来说，唯密文攻击是最困难的，因为分析者可利用的信息最少，因此攻击的强度最弱，其他攻击强度依次递增。一般认为，如果一个加密系统无法抵御唯密文攻击，该系统就无任何安全性可言；如果该加密系统能够抵御选择密文攻击，那么它当然能够抵御其余 3 种攻击。最常见的是已知明文攻击和选择明文攻击。

事实上，攻击者要得到一段明文或加密一段选择好的明文并不困难。例如，对程序源代码的加密，其中都包含一些关键字，攻击者可以利用这些代码关键字等。攻击者利用类似源代码这样的具有标准的头部、尾部的关键字，更容易解密。从技术角度看，对密码破译者较为有利且容易具备的条件是选择明文攻击。因此，一个好的密码算法必须满足能够抵抗选择文本攻击。

5.1.3　密码分析方法的评价

在现代密码分析学中，衡量一种密码攻击方法是否有效的标准，除了能成功获取密钥或等效密钥外，还要确保其攻击复杂度比穷举攻击的计算复杂度低。针对一种密码攻击方法的有效性和复杂性，主要从时间、空间、数据等几个方面的指标综合衡量，具体如下。

(1) 时间复杂度：完成攻击所需要的时间，包括数据采集时间和分析处理时间，为统一不同设备运算频率的不同，一般用加解密的次数进行衡量。

(2) 空间复杂度：用进行攻击所需要的存储空间大小进行衡量。

(3) 数据复杂度：用攻击者所需要收集的数据总量进行衡量。

(4) 成功概率：攻击者实施攻击后成功恢复密钥的概率。

攻击的复杂性取决于以上因素的最小复杂度，在实际实施攻击时往往要考虑这种复杂性的折中，如存储需求越大，攻击可能越快。此外，计算复杂度越高也表示加密系统的安全性越好。在密码分析中，计算复杂度或攻击复杂度通常是指时间复杂度和空间复杂度。

5.2　密码分析

针对密码分析，本节主要从密码分析方法以及这些分析方法在古典密码分析、密码算法分析等方面阐述，具体介绍如下。

5.2.1 密码分析方法

目前，密码分析方法主要有穷举攻击、统计分析、线性密码分析、差分密码分析及侧信道攻击，具体介绍如下。

1. 穷举攻击

穷举攻击方法也称为暴力攻击，是从事密码分析方法研究者的一个基本参考点。这种攻击方法是对截获到的密文尝试遍历所有可能的密钥，直到获得一个有意义的明文；在公钥密码体制中，使用已知或公开的密钥对所有可能的明文进行加密，直到其计算出的结果与截获的密文一致。

穷举攻击的基本思想：假设密钥长度为 n，密钥空间的复杂度为 2^n，如果穷举所有可能的密钥，理论上就可以攻破密码算法，分析的时间复杂度为 2^n。显然，穷举攻击方法的破译代价与密钥空间的大小成正比，攻击者只要有充足的计算资源，该方法总是可以成功的。穷举攻击所花费的时间等于尝试次数乘以一次解密所需的时间。对于任何已知密码算法的密码，只要攻击者有足够多的计算资源，此种方法就是可以成功的。所以，穷举攻击是一种进行密码分析研究所依赖的最基本的密码系统攻击方法。

对穷举攻击的优化方法是：首先将密钥空间分割成很多块，然后将它们分配到多个处理器或计算机，这是对穷举攻击唯一的实际优化，其本质是利用了并行处理的思想。例如，第 1 个处理器尝试破译所有前 4 位为 0000 的密钥，第 2 个处理器破译所有前 4 位为 0001 的密钥……直到第 16 个处理器尝试破译所有前 4 位为 1111 的密钥。

1997 年 6 月 18 日，美国科罗拉多州以 Rocke Verser 为首的一个工作小组宣布，通过互联网利用数万台微机历时 4 个多月，采用穷举攻击破译了 DES 密码算法，这是穷举攻击的一个很好的例证。穷举攻击的一个主要特点是：它总是保证经过一段时间后正确的密钥可以被找到，这一点对其他分析技术来说不一定成立，特别是基于统计方法的密钥恢复技术。另一个优点是它易于执行，这带来了一些额外的好处，比如易于优化。对抗穷举攻击的方法有增加密钥长度、增强加密算法的计算复杂度、增加冗余明文-密文对等。

2. 统计分析

统计分析攻击方法是密码分析者利用明文、密文和密钥的统计规律破译密码的方法。利用统计分析方法进行攻击时，密码分析者对截获的密文进行统计分析，获取它的统计规律，并与明文的统计规律进行对照比较，从中得到明文和密文的对应关系或变换信息，最终得到明文或者密钥。例如，在经典的换位密码、置换密码体制中，可通过分析单字母、双字母、三字母等的频率和其他统计特性破译密文。对抗统计分析攻击的主要方法是尽可能使明文的统计特性不带密文信息，以此达到破坏密文统计规律的目的，即把明文和密文的统计特性扩散到整个密文，进而使密文呈现出极大的随机性，达到破坏统计分析攻击的目的。目前，能够抵抗统计分析攻击已经被认为是现代密码方法设计要达到的一项基本要求。

3. 线性密码分析

日本学者 M.Matsui 首次在分析 DES 时对线性密码分析的方法进行了详细描述，即利用明文、密文和密钥之间的线性关系恢复部分密钥比特。线性密码分析是一种已知明文攻击，即密码分析者能获得当前密钥下的一些明文-密文对，通过建立明文、密文和密钥的某些比特之间的线性关系作为区分器，统计轮函数中各个组件的线性关系以及它们之间成立的概率，然后使用轮函数的线性逼近计算成立概率，进而得到明文、密文和密钥之间的不平衡线性逼近，恢复部分密钥比特。它也是一种统计分析方法，不能保证适用于所有情况，但在大多数情况下都是可行的。结合其他分析方法或者辅助技术，攻击者经常可以扩展这种攻击，进而获得更多的密钥比特信息。线性密码分析的数学表达式为

$$P_{i1} \oplus P_{i2} \oplus \cdots \oplus C_{j1} \oplus C_{j2} \oplus \cdots = K_{k1} \oplus K_{k2} \oplus \cdots$$

其中，$i_1, i_2, \cdots, j_1, j_2, \cdots, k_1, k_2, \cdots$，表示固定位置。

4. 差分密码分析

差分密码分析是一种选择明文攻击，与线性密码分析相比，它在实际应用中更可行，它是由 Biham 和 Shamir 于 1990 年提出的，最初也是用来分析 DES 的。现在它是针对迭代密码算法较有效的攻击方法之一。与线性密码分析一样，差分密码分析也是概率攻击，其基本思想是：通过分析明文对的差分值对密文对的差分值的影响恢复某些密钥比特，然后对剩余的密钥比特使用穷举搜索获得。它主要研究的是加密过程中，明文对或中间状态对差分逐轮的扩散情况，而不是一次加密。这里的差分是明(密)文对的异或值。在差分密码分析的基础上，又发展出截断差分、高阶差分、不可能差分和矩形攻击等多种分析方法。

5. 侧信道攻击

当密码算法在硬件设备及软件系统应用时，攻击者一旦可以访问加密设备，就可以通过对设备实际操作的执行时间、能量消耗或电磁辐射等特征进行测量，如果这些特征的变化在一定程度上依赖于密钥，那么攻击者可能将此密码破解。目前，侧信道攻击方法给密码设备的安全问题带来非常严重的威胁。

5.2.2　古典密码分析

古典密码是密码学的早期发展阶段，其思想比较简单而且其容易破译。由于古典密码便于理解密码分析的思想，故把它单独列出来，并进行较为详细的分析。

在一定的条件下，古典密码体制中的任何一种方法都是可以破译的。面对已知明文攻击，移位密码、仿射密码、置换密码、维吉尼亚密码等都是十分脆弱的。即使使用唯密文攻击，大多数古典密码体制依然很容易被攻破。鉴于古典密码大都是用来保护基于英文语言表达的信息，所以英文语言的统计分析是攻击古典密码的有力工具，使得大多数古典密码体制都不能很好地隐藏明文消息的统计特征。

这里将针对单表替代密码，利用英文语言的统计特性和密码特征，运用唯密文攻击或

已知明文攻击等方式介绍古典密码的基本分析方法。

单表替代密码通过一个固定的替换表进行加解密，任何一个明文字母在替换表中都对应一个固定的替代字母(密文)。对于这种古典密码，加法密码和乘法密码的密钥量比较小，可利用穷举密钥的方法进行破译。面对数百上千级别的密钥，对于古代分析者企图用穷举全部密钥的方法破译密码可能会有一定困难，但是随着计算机的出现，这一问题很容易解决。

事实上，密文字母表也只是明文字母表的众多排列中的一种。设明文字母表包含 n 个字母，则共有 $n!$种排列。对于明文字母表为英文字母表的情况，密文字母表共有 26!种。由于密钥词组代替密码的密钥词组的选择具有任意性，因此，这 26!种字母排列表的大部分都有可能被用作密文字母表，即使借助计算机以穷举攻击方式进行破解，也是很困难的。

穷举破解不是攻击密码的唯一方法。一旦密文的消息足够长，密码分析者便可利用语言的统计特性进行分析，任何自然语言都有许多固有的统计特性，如果语言的这种统计特性在明文中有所反映，密码分析者便可通过分析明文和密文的统计规律而破译密码。许多著名的古典密码都可利用统计分析的方法进行破译。通过对大量英文语言的研究可以发现，每个字母出现的频率不一样，e 出现的频率最高。如果所统计的文献足够长，便可发现各字母出现的频率比较稳定，而且只要不是太特殊的文献，不同文献统计出的频率大体一致，如表 5-1 所示。应该指出的是，由于用于统计的明文长度不同以及明文的内容类型不同，如诗歌、小说、科技文献等，不同文献中 26 个英文字母出现的频率可能略有差别。

表 5-1　26 个英文字母出现的频率统计表

字　母	出现频率	字　母	出现频率
a	0.0856	n	0.0707
b	0.0139	o	0.0797
c	0.0279	p	0.0199
d	0.0378	q	0.0012
e	0.1304	r	0.0677
f	0.0289	s	0.0607
g	0.0199	t	0.1045
h	0.0528	u	0.0249
i	0.0627	v	0.0092
j	0.0013	w	0.0149
k	0.0042	x	0.0017
l	0.0339	y	0.0199
m	0.0249	z	0.0008

通过对 26 个英文字母出现频率的分析，可得以下结果。

(1) 字母 e 出现的频率最大,约为 0.13。

(2) 出现频率为 0.05～0.1 的字母集合为{t,a,o,i,n,s,h,r}。

(3) 出现频率为 0.04 附近的字母集合为{d,l}。

(4) 出现频率为 0.013～0.029 的字母集合为{c,u,m,w,f,g,y,p,b}。

(5) 出现频率小于 0.01 的字母集合为{v,k,j,x,q,z}。

在密码分析中,除了考虑单字统计特性外,掌握双字母、三字母的统计特性以及字母间的连缀关系等信息也是很有用的。

出现频率最高的 30 个双字母组合依次是 th he in er an re ed on es st en at to nt ha nd ou ea ng as or ti is et it ar te se hi of。

出现频率最高的 20 个三字母组合依次是 the ing and her ere ent tha nth was eth for dth hat she ion int his sth ers ver。

特别地,the 出现的频率几乎是 ing 的 3 倍,这在密码分析中很有用。此外,统计资料还表明:以 t,a,s,w 为起始字母的英文单词约占一半;以 e,s,d,t 字母结尾的英文单词超过一半。

以上这些统计数据是通过非专业性文献中的字母进行统计得到的,对于密码分析者来说,这些都是十分有用的信息。除此之外,密码分析者对明文相关知识的掌握对破译密码也是十分重要的。

字母和字母组的统计数据对于密码分析者是十分重要的,因为它们可以提供有关密钥的许多信息。例如,对于字母 e 的出现频率较其他字母的出现频率高得多,如果是单表替代密码,可以预计大多数密文都将包含一个频率比其他字母都高的字母。当出现这种情况时,猜测这个字母所对应的明文字母为 e,进一步比较密文和明文的各种统计数据及其分布,便可确定密钥,从而破译单表替代密码。

下面通过一个具体实例说明如何借助英文语言的统计规律破译单表替代密码。

【例 5-1】 设某段明文经单表替代密码加密后的密文如下

YIFQ FMZR WQFY VECF MDZP CVM R ZWNM DZVE JBTX CDDUMJ
NDIF EFMD ZCDM QZKC EYFC JMYR NCWJ CSZR EXCH ZUNMXZ
NZUC DRJX YYSM RTMEYIFZ WDYV ZVYF ZUMR ZCRW NZDZJJ
XZWG CHSM RNMD HNCM FQCH ZJMX JZWI EJYU CFWD JNZDIR

试分析出对应的明文。为了表述更加清楚,本例的密文用大写字母表示,明文用小写字母表示。

解:这里将加密变换记为 E_k,解密变换记为 D_k,本段密文共有 168 个字母。要破解上述密文,需要以下三步。

第一步:统计出密文中各个字母的出现次数和频率,如表 5-2 所示。

第二步:从出现频率最高的几个字母、双字母组合及三字母组合开始,并假定它们是英文语言中出现频率较高的字母及字母组合对应的密文,逐步推测出各密文字母对应的明文字母。

表 5-2　例 5-1 密文中各英文字母的出现次数和出现频率

字　母	出现次数	出现频率	字　母	出现次数	出现频率
A	0	0.000	N	9	0.054
B	1	0.0006	O	0	0.000
C	15	0.089	P	1	0.006
D	13	0.077	Q	4	0.024
E	7	0.042	R	10	0.060
F	11	0.065	S	3	0.018
G	1	0.006	T	2	0.012
H	4	0.024	U	5	0.030
I	5	0.030	V	5	0.030
J	11	0.065	W	8	0.048
K	1	0.006	X	6	0.036
L	0	0.000	Y	10	0.060
M	16	0.095	Z	20	0.119

(1) 由表 5-2 可知，密文字母 Z 出现的次数多于任何其他密文字母，出现频率约为 0.12。结合统计表 5-1，猜测出 $D_k(Z)=e$；除 Z 外，出现频率至少 10 次的字母有 C，D，F，J，M，R，Y，它们出现的频率基本为 0.06～0.095，则可以猜测这些密文字母可能对应的明文字母集合为{t，a，i，n，o，r，h，s}中的某一个。

(2) 假设 $D_k(Z)=e$ 是正确的，则需要密文中带 Z 的双字母出现的情况，包括 Z 在前和在后两种情况，如表 5-3 所示。

表 5-3　例 5-1 密文中包含 Z 的双字母出现次数

Z-	出现次数	-Z	出现次数
ZW	4	DZ	4
ZU	3	NZ	3
ZR	2	RZ	2
ZV	2	HZ	2
ZC	2	XZ	2
ZD	2	FZ	2
ZJ	2		

由表 5-3 可知，出现 4 次的有 DZ 和 ZW，出现 3 次的有 NZ 和 ZU，而 RZ、HZ、XZ、FZ、ZR、ZV、ZC、ZD、ZJ 都出现 2 次。

由于 ZW 出现了 4 次，而 WZ 一次也未出现，同时结合表 5-2 中 W 出现的概率为 0.048，因此可以猜测 $D_k(W)=d$。

由于 DZ 出现 4 次，ZD 出现 2 次，可以猜测密文 D 的明文可能的集合为{r，s，t}，但还无法确定。

(3) 假设 $D_k(Z)=e$ 和 $D_k(W)=d$ 成立，继续分析 ZRW 和 RZW，并且还出现了 RW，这里还发现 R 在密文中频繁出现，而 nd 是一个明文中常见的双字母组合，所以可以猜测 $D_k(R)=n$。

(4) 至此，推测出 3 个密文字母可能对应的明文字母，其对应关系如下。

YIFQFM***ZRW***QFYVECFMD***Z***PCVM***RZW***NMD***Z***VEJBTX
end e ned e
CDDUMJNDIFEFMD***Z***CDMQ***Z***KCEYFCJMY***R***NC***W***JCS***Z***
e e n d e
REXCH***Z***UNMX***Z***N***Z***UCD***R***JXYYSM***R***TMEYIF***ZW***DYV***Z***
n e e e n n ed e
VYF***Z***UM***RZ***C***RW***N***Z***DZJJX***ZW***GCHSM***R***NMDHNCMFQ
e ne nd e e ed n
CH***Z***JMXJ***ZW***IEJYUCF***W***DJN***Z***DI***R***
e ed d e n

注：第一行大写表示密文，斜体表示可能破译出来的密文；第二行是密文字母可能破译出来的内容，下同。

由于 NZ 是密文中出现次数较多的双字母组合，而 ZN 又未出现，因为 N 的出现频率为 0.054，所以可以猜测 $D_k(N)=h$。假设 $D_k(N)=h$ 正确，依据一个明文片段 ne-ndhe (neCnde)，且密文 C 出现的频率为 0.089，结合表 5-1 及组合字母出现频率分析结果，可以猜测 $D_k(C)=a$。

(5) 假设 $D_k(N)=h$ 和 $D_k(C)=a$ 成立，至此我们已经猜测出 5 个密文字母的明文，则明文和密文对应情况如下。

YIFQFM***ZRW***QFYVE***C***FMD***Z***P***C***VM***RZWN***MD***Z***VEJBTX
end a e a nedh e
CDDUMJ***N***DIFEFMD***ZC***DMQ***Z***K***C***EYF***C***JMY***RNCW***J***C***S***Z***
a h ea e a a nh ad a e
REX***C***H***Z***U***N***MX***ZNZ***U***C***D***R***JXYYSM***R***TMEYIF***ZW***DYV***Z***
n a e h ehe a n n ed e