CHAPTER 3

# 第3章 古典密码

**知识单元与知识点**

- 隐写术、代替、换位、频率分析攻击的相关概念；
- 代替密码体制及其实现方法分类。

**能力点**

- 深入理解隐写术、代替、换位、频率分析攻击的基本含义；
- 认识代替密码体制及其实现方法；
- 认识换位的实现方法。

**重难点**

- 重点：代替、换位的概念与实现方法。
- 难点：频率分析攻击；Hill 密码。

**学习要求**

- 了解隐写术与加密的区别与联系；
- 掌握代替、换位、频率分析攻击等概念；
- 了解代替与换位的实现方法。

古典密码是密码学发展的一个阶段，也是近代密码学产生的渊源，尽管古典密码大都较简单，一般可用手工或机械方式实现其加密和解密，目前已很少采用，但研究这些密码的原理，有助于理解、构造和分析近代密码。

## 3.1 隐写术

信息隐藏是一门体现人类高度智慧的信息安全斗争技术和艺术。从古至今，几乎所有新的信息隐藏手段和技术一旦出现，就立即会被用于情报作战中，不仅演绎出许多惊心动魄、惊险绝伦的故事，而且在一定程度上决定着战争的胜负乃至国家的命运。

根据密码学的发展历史，我们知道有两种隐藏明文信息的方法：隐写术(steganography 或 covered writing)和密码编码学(secret writing)。密码编

码学是通过各种文本转换的方法使得消息内容不可理解，即隐藏消息的含义。隐写术则是隐藏消息本身的存在，这种方法通常在一段看来无伤大雅的文字、图片或其他实物中嵌入、排列一些词汇或字母隐含地表达真正的意思。

下面来看几个有关信息隐藏的生动例子。

**1. 诗情画意传“密语”**

古老的中华文化博大精深、源远流长。我国古代早有以藏头诗、藏尾诗、漏格诗以及绘画等形式，将要表达的意思和“密语”隐藏在诗文或画卷中的特定位置，一般人只注意诗或画的表面意境，而不会去注意或破解隐藏其中的密语。

一个例子是庐剧《无双缘》中“早迎无双”的故事。写的是合肥知县刘震有一女名叫无双，自小与表兄王仙客青梅竹马，两小无猜，相亲相爱。两人长大以后，刘震便为他们订下了婚约。一年后，王仙客赴京赶考，科场得意，万岁钦点头名状元，封授翰林学士，并赐宫花金印回庐州完婚。王仙客一路吹吹打打，好不威风。不想，人马行至双峰山下，被绿林好汉古氏兄妹夺去行囊，失落文书金印，变成一名乞丐来到刘家。刘震问明前后情况，即刻变脸赖婚，把女儿无双另许豪门公子曹进。王仙客与舅舅刘震论理，刘震也觉得理亏，便把责任推给女儿无双。无双知道爹爹势利无赖，非常气愤，但苦于见不到表兄王仙客，只得写诗一首，速派丫鬟把诗送给王仙客：

早妆未罢暗凝眉，
迎户愁看紫燕飞，
无力回天春已老，
双栖画栋不如归。

诗中每句的首字即组成“早迎无双”，表达了她此时期待的心情。

另一个例子是著名大诗人白居易写的回文七言诗《游紫霄宫》。全诗书写如图 3.1 所示，通过藏头拆字，作者实际要表达的意思是：

水洗尘埃道未甞，甘于名利两相忘。
心怀六洞丹霞客，口诵三清紫府章。
十里采莲歌达旦，一轮明月桂飘香。
日高公子还相觅，见得山中好酒浆。

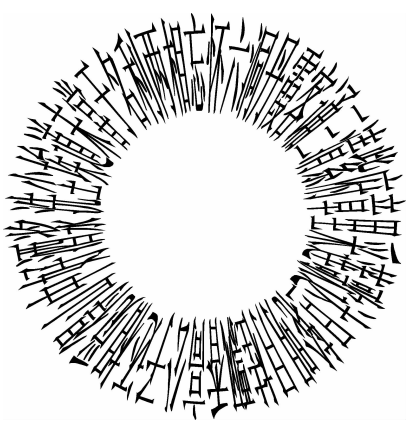


图 3.1　《游紫霄宫》

我国古代还有一种很有趣的信息隐藏方法，即消息的发送者和接收者各有一张完全相同的带有许多小孔的掩蔽纸张，而这些小孔的位置是随机选择并被戳穿的。发送者在纸张的小孔位置写上秘密消息，然后在剩下的位置补上一段掩饰性的文字。接收者只要将掩蔽纸覆盖在其上就可立即读出秘密的消息来。直到 16 世纪，意大利的数学家卡丹(Cardan)又发展了这种方法，现在被称为卡丹网格式密码。例如：

王先生：

来信收悉，你的盛情真是难以报答。我已在昨天抵达广州。秋雨连绵，每天需备伞一把方能上街，苦矣。大约本月中旬我才能返回，届时再见。

但是,当收信人用网格纸覆盖以后读出来的消息却是:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | 情 | | 报 | | 在 | 雨 |
| 伞 | 把 | | | | 中 | | |

**2. 悠扬琴声奏响“进军号角”**

历史上许多信息隐藏和传输的方法都是为了满足情报作战的需要而发展和成熟起来的,有些信息隐藏的设计非常巧妙。如第二次世界大战期间,一位热情的女钢琴家常为联军作慰问演出,并通过电台播放自己谱写的钢琴曲。由于联军在战场上接连遭到失败,反间谍机关开始怀疑这位女钢琴家,可因找不到钢琴家传递情报的手段和途径而迟迟不能决断。原来,这是一位忠实的德国女间谍,每当她从联军军官那里获得军事情报后,就按照事先规定的密码巧妙地将其编成乐谱,并在电台演奏时一次次公开将重要情报通过悠扬的琴声传递出去。

恐怖大亨拉登借用他的讲话录音或录像带在新闻媒体中播放的途径,借由特定的音调、音速、俚语等公开发布恐怖袭击命令也是一个例子。

**3. 显微镜里传递情报**

第二次世界大战期间,德国情报机关还曾利用微缩原理和照相方法,将秘密文件、资料情报缩小至数十或数百乃至数千分之一,制成很薄的显微点膜片,然后把它们“埋藏”在书报杂志中某个字或标点符号上,或是将超微膜片藏在邮票、信封内进入邮政系统传递。对方收到后,按照双方约定好的位置和标记,通过技术手段再重新将显微点还原成像。

今天,密写技术有了很大发展,特别是将激光技术和水印技术用于“密写”,使信息隐藏更为隐蔽。以微缩技术制作显微点,可以在厚度仅 $1.0\mu m$、面积仅 $1mm^2$ 的显微点上,隐藏几百甚至上千字的信息量,倘若把经过技术处理的显微点隐藏在一本厚厚的书、一株植物的根、叶或一只动物的皮毛里,要想发现它,真如同大海捞针一样难。

**4. 魔术般的密写术**

密写术用于情报和通信联络也有着悠久历史。它的原理是利用某些化合物对纸张、布料、塑料等有“潜隐”功能的载体进行书写的一种技术。用这些化学物质书写的信息肉眼看不见,只有用其他适宜的化合物或通过某种光、电、热、汽等物理方法才能显示出来。早期间谍普遍使用的密写剂是有机物质溶液,如尿液、牛奶、醋、果汁等,这些有机物质经文火加热后立即碳化,从而使字迹显影。

**5. 网络与数字幽灵**

现代信息隐藏技术的研究建立在信息理论、统计理论、认识心理学和现代信息技术手段的基础上。而现代电子加密技术和数字技术的发展,又为信息隐藏提供了更为先进、高效的技术和手段。数字信息隐藏的最大特征,就是由公开信息作掩护,第三方很难感觉到秘密信息的存在。计算机网络的出现和广泛使用,是信息技术发展的一个突破性成就,而一些情报机构、恐怖组织或犯罪集团正是利用这一渠道,将秘密信息经过加密技术处理后,通过电子邮件、电子文档或图表在网上公开传输,犹如若隐若现的“幽灵”,很难跟踪、截获和破解。

一种利用图像来隐藏消息的方法,例如现在数码相片的最大分辨率典型地可以达到几

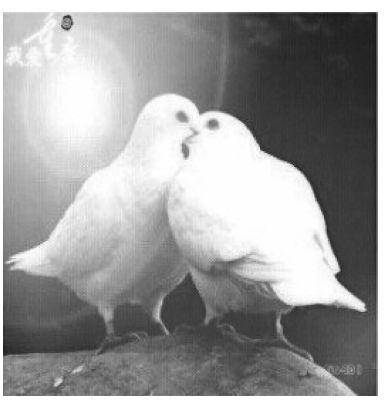
百万或更高的像素个数，通常每个像素用24位（即3个字节）来描述，每个字节表示一个基本的色彩（红、绿或蓝），每个字节的最低有效位能被改变而不会明显影响该图像的质量。这就意味着能够在一张数字快照中轻松地隐藏一条达到K甚至M位数量级大小的消息。目前，已经出现了一些采用这种方法进行消息隐藏的软件包可供使用。

**6. “量子”技术隐形传递信息**

在科幻电影或神话小说中，常常有这样的场面：某人突然在某地消失掉，而后却在别的地方莫名其妙地显现出来。这种来无影去无踪的过程，从物理学角度可以想象或解释为隐形传递的过程。量子隐形信息传递是发送者利用量子特性的独特功能，对所提取的信息通过运用量子技术突破经典信息系统的极限超水平进行信息传递，这便是量子力学和信息科学相结合的重要产物。具体内容请参考第11章的介绍。

交流与微思考

**【问题】** 2013年春天，有位小伙子向一个心仪已久的重庆妹子浪漫表白，这个姑娘既没答应也没说不，只发给小伙子一张图片（如右）。



小伙子激动地研究了一晚上还是没看懂，不得不惊叹重庆妹子含蓄的“神回复”。第二天怀着忐忑的心情咨询了身边博学多才的朋友才推敲出其隐藏的真正含义。你知道是什么吗？

**【提示】** 鸽吻，汉语拼音拼读为ge＋wen，其音喻义为gun（滚）。结合自己的所见所闻，再补充一些关于隐写术的实际例子。

信息隐藏是保证信息安全的支撑技术，可能事关国家的根本利益。信息隐藏技术又是一把“双刃剑”，它在越来越多地融合到未来信息战场军事谋略中的同时，也在被敌方或恐怖犯罪组织所利用。目前的信息隐藏和传递手段已将传统和现代高技术手法融为一体，隐藏手段越来越高明，侦破难度愈来愈大。这些技术看来很古老，但它们仍有现实意义，而且在古代信息隐藏技术基础上发展起来的现代信息隐藏技术（如数字水印）正在焕发出新的光彩。据报道，近期世界上一系列恐怖事件的发生，安全部门在事件发生前未成功侦破，其中一个重要原因就是安全部门过分依赖高科技，而忽略了恐怖组织利用其他传统的信息传递方法和渠道，从而出现了信息安全侦察的“盲区”。

信息隐藏技术将是未来信息对抗的焦点，是敌对双方借以获取和破解信息的制高点，因此备受各国关注。国际上诸多情报机关和相关机构为此而绞尽脑汁，秘密斗争。作为未来情报战的重要组成部分，信息隐藏技术必将对战争的进程和胜败产生重大影响。

当前，世界上一些军事强国已开发成功了秘密信息隐藏和恢复处理系统，并根据军事通信系统发展和机要通信的应用需求及特点，研究提出了实用性强、安全性高、功能完善和不易破解的信息隐藏新技术和新算法。一些著名的情报部门和机构更是加紧了信息隐藏技术的应用，以“确保国家政治、军事、经济信息安全、可靠、迅速地传递和共享”。

信息技术的飞速发展，已使当今的信息隐藏技术远远脱离了传统意义上的“锦囊妙计”的概念，并以其破解难度大、覆盖范围广、安全系数高等特点被称为信息战场上的“大谋略”、

“大智慧”。尤其以量子技术等为代表的高新技术在信息隐藏领域的应用,使信息隐藏的“深度”和“广度”呈几何级数增长。可以预见,未来的信息隐藏技术和手段,已不是单纯的信息获取与反获取,破解与反破解的过程,而是人类贯穿于未来战争乃至和平建设时期始终的白热化智慧大较量。

与加密技术相比,隐写术的优缺点分析如表3.1所示。

**表3.1 隐写术的特点**

| 隐写术的优点 | 隐写术的缺点 |
| --- | --- |
| 能够被某些人使用而不容易发现他们之间在进行秘密通信。而加密则很容易被发现谁与谁在进行秘密通信,这表明通信本身可能是重要的或秘密的,或表明通信双方对其他人有需要隐瞒的事情,这种发现本身可能具有某种意义或作用 | (1) 它形式简单但构造费时,要用大量的开销来隐藏相对较少的信息。<br>(2) 一旦该系统的构造方法被发现,就会变得完全没有价值(当然如果在隐写术的构造方法中加入了某种形式的密钥,则这个问题可以克服。另一种可选方案是:一条消息先被加密,然后使用隐写术隐藏)。<br>(3) 隐写术一般无稳健性,如数据改动后隐藏的信息不能被恢复 |

## 3.2 代替

代替和换位是古典密码中用到的两种基本处理技巧,它们在现代密码学中依然得到广泛使用。我们先来看称为“暗号”的有关代替的例子。简单地说,暗号就是通过事物的状态或人的行为来传达事先约定的信息。暗号包含了密码算法的基本特征——变换,即把一些简单的信息变换成一些常见的事物或现象。暗号的使用从古到今非常普遍,在电影里屡见不鲜,如窗台上的花瓶、手中拿着的报纸、口中哼唱的小曲,可分别代表“平安无事”、“我是你要找的人”、“我在找自己人”。据我国北宋时编撰的《武经总要》记载,周武王时期(约公元前11世纪)姜太公用称为“阴符”的符契进行军事上的保密通信,它是用物件的不同长度形成暗号来表示(暗示)不同的信息,如表3.2所示。

**表3.2 姜太公用于保密通信的“阴符”及其含义**

| 符契的长度 | 对应的明文信息 | 符契的长度 | 对应的明文信息 |
| --- | --- | --- | --- |
| 长一寸 | 大胜克敌 | 长六寸 | 警众坚守 |
| 长三寸 | 失利亡士 | 长七寸 | 却敌报远 |
| 长四寸 | 败军亡将 | 长八寸 | 降城得邑 |
| 长五寸 | 请粮益民 | 长九寸 | 破军擒将 |

基于暗号的保密通信实际上是将要传递的保密信息通过平时司空见惯的事物或人的行为来实现,即通过代替这种变换或转化起到隐蔽的作用。山贼的“黑话”道理也一样。

代替就是将明文中的一个字符用另外一个字符取代;具体的代替方案称为密钥(如图3.2所示,这里不区分大小写)。如26个英文字母仍然用26个英文字母来代替,可能的密钥(代替方案)就有$26!-1\approx4\times10^{26}$种(减1是因为有一种排列代替的密文和原文完全一致,即被其本身代替,等于没有被代替,起不到保密的作用)。

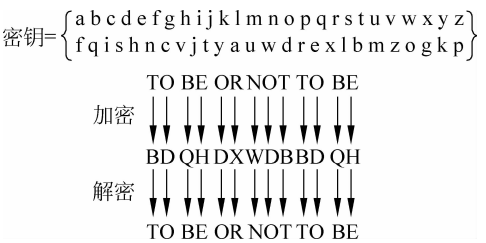



图 3.2 代替

## 3.2.1 代替密码体制

代替密码体制的一般定义是：设 $P=C=K=Z_{26}$，这里 $P$、$C$、$K$、$Z_{26}$ 分别表示明文空间、密文空间、密钥空间和 26 个整数(对应 26 个英文字母)组成的空间。很明显，明文、密文和密钥的取值范围是一样的，它们的空间大小也是相同的。

对于任意的 $k\in K$，定义：

$$\text{加密：}e_k(x)=x+k(\text{mod }26)=y\in C \tag{3.1}$$

即明文为 $x$，密钥为 $k$(实现上就是将 26 个英文字母向后循环移 $k$ 位)，密文为 $y$。

$$\text{解密：}x=d_k(y)=y-k(\text{mod }26) \tag{3.2}$$

在使用该方法时，要求 26 个英文字母与模 26 的剩余类集合{0,1,2,…,25}建立一一对应关系，如 A 对应 0，B 对应 1，……，Z 对应 25(如表 3.3 所示)①。不区分大小写。

**表 3.3 字母与数字对应表**

| 字 母 | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 对应的数字 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 字母 | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 对应的数字 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

当 $k=3$ 时，即为著名的恺撒(Caesar)密码：加密时 26 个英文字母循环后移 3 位，解密时则循环前移 3 位。这一方法据史书记载，最早约在公元前 50 年，被罗马大帝 Julius Caesar 用于和他的军队指挥官之间进行保密通信。

**【例 3-1】** 设明文为：China，对应的数字为：2 7 8 13 0。

下面分析加密过程。

C：$e_3(2)=2+3(\text{mod }26)=5$，对应着字母 F；

h：$e_3(7)=7+3(\text{mod }26)=10$，对应着字母 K；

① 有趣的代替计算：如果运用这样的代替方案，即令 A、B、C、…、Z 这 26 个英文字母分别等于百分之 1、2、3、…、26，那么我们就能得出如下有趣的结论：HARD WORK(努力工作)：H+A+R+D+W+O+R+K=8+1+18+4+23+15+18+11=98。类似地，KNOWLEDGE(知识)=96、LOVE(爱情)=54、LUCK(幸运)=47，这些我们通常很看重的东西都不是最完满的，虽然它们非常重要。那么，究竟什么能使得生活变得圆满？是 MONEY(金钱)吗？不！MONEY=72；是 LEADERSHIP(领导能力)吗？不！LEARDERSHIP=97；是 SEX(性)吗？更不是！SEX=48。那么，什么能使生活变得圆满呢？是 ATTITUDE(心态)=100！正是我们对待工作、生活的态度能够使我们的生活达到 100%的圆满。

i：$e_3(8)=8+3 \pmod{26}=11$，对应着字母 L；

n：$e_3(13)=13+3 \pmod{26}=16$，对应着字母 Q；

a：$e_3(0)=0+3 \pmod{26}=3$，对应着字母 D。

所以明文“China”基于恺撒密码被加密为“FKLQD”。

解密过程是加密过程的逆过程，下面具体分析。

F：$d_3(5)=5-3 \pmod{26}=2$，对应着 C；

K：$d_3(10)=10-3 \pmod{26}=7$，对应着 H；

L：$d_3(11)=11-3 \pmod{26}=8$，对应着 I；

Q：$d_3(16)=16-3 \pmod{26}=13$，对应着 N；

D：$d_3(3)=3-3 \pmod{26}=0$，对应着 A。

即“FKLQD”经恺撒密码解密恢复为“CHINA”(不区分大小写)。

恺撒密码的特点：

- 属于单字母简单替换密码。
- 已知加密与解密算法($k=3$)。

$$c = e_k(p) = (p+3) \bmod 26$$

$$p = d_k(c) = (c-3) \bmod 26$$

- 明文语言集已知(用于英文字母)且易于识别。
- 结构过于简单，密码分析员只使用很少的信息就可预言加密的整个结构。

正是由于后三个特征使得恺撒密码很容易被蛮力攻击方法分析。

## 3.2.2 代替密码的实现方法分类

### 1. 单表代替密码

单表代替密码(Monoalphabetic Cipher)对明文中的所有字母都使用同一个映射，即 $\forall p \in P, f: P \to C, f(p)=c$。为了保证加密的可逆性，要求映射 $f$ 是一一映射。单表代替包括最早的恺撒加密(加密时向后移3位，由于3是固定的，故没有密钥)、一般意义上的单字母代替(即移位密码，也称通用恺撒密码。向后移 $k$ 位，$k$ 是任意的，故认为 $k$ 是密钥，共有26个密钥)、使用密钥的单表代替和仿射加密。前两个已在上面的内容中介绍，下面分析使用密钥的单表代替和仿射加密。

1) 使用密钥的单表代替加密

这种密码选用一个英文短语或单词串作为密钥，去掉其中重复的字母得到一个无重复字母的字母串，然后将字母表中的其他字母依次写于此字母串之后，就可构造出一个字母代替表。这种单表代替泄露给破译者的信息更少，而且密钥可以随时更改，增加了灵活性。

**【例 3-2】** 设密钥为 key。

| 明文 | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 对应的密文 | **k** | **e** | **y** | a | b | c | d | f | g | h | i | j | l |
| 明文 | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 对应的密文 | m | n | o | p | q | r | s | t | u | v | w | x | z |

因此，如果明文为 China，则对应的密文为 yfgmk。

**【例 3-3】** 设密钥为 spectacular。

| 明文 | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 对应的密文 | **s** | **p** | **e** | **c** | **t** | **a** | **u** | **l** | **r** | b | d | f | g |
| 明文 | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 对应的密文 | h | i | j | k | m | n | o | q | v | w | x | y | z |

因此，如果明文为 China，则对应的密文为 elrhs。

2) 仿射加密

仿射密码的加密是一个线性变换。

$$\text{加密：} y = f(x) = k_1 x + k_2 (\bmod 26) \tag{3.3}$$

$$\text{解密：} x = f^{-1}(y) = k_1^{-1}(y - k_2)(\bmod 26) \tag{3.4}$$

式(3.4)中的“−1”表示“逆”(逆的计算参考第 4 章关于欧几里德算法的介绍)。很明显，$k_1=1$ 时为通用恺撒变换；如果同时 $k_2=3$，则为恺撒密码。

仿射加密要求 $\gcd(k_1,26)=1$，即 $k_1$ 与 26 互素，否则就退化为 $y=f(x)=k_2 (\bmod 26)$。故密钥空间大小为 $(k_1,k_2)=12\times 26=312$，因为与 26 互素的 $k_1$ 有 12 个取值：1,3,5,7,9,11,15,17,19, 21,23,25；$k_2$ 有 26 个取值。

**【例 3-4】** 设 $k=(7,3)$，注意到 $7^{-1}(\bmod 26)=15$，加密函数是 $y=f(x)=7x+3(\bmod 26)$，相应的解密函数是 $x=f^{-1}(y)=15(y-3)(\bmod 26)=15y-19(\bmod 26)$。

若要加密明文：China，首先将字母 C,h,i,n,a 转换为数字 2,7,8,13,0；然后加密：

$$7\times\begin{bmatrix}2\\7\\8\\13\\0\end{bmatrix}+\begin{bmatrix}3\\3\\3\\3\\3\end{bmatrix}=\begin{bmatrix}17\\52\\59\\94\\3\end{bmatrix}\bmod 26=\begin{bmatrix}17\\0\\7\\16\\3\end{bmatrix}=\begin{bmatrix}R\\A\\H\\Q\\D\end{bmatrix}$$

即在当前密钥下，“China”经仿射加密变换成“RAHQD”。

解密：

$$15\times\begin{bmatrix}17\\0\\7\\16\\3\end{bmatrix}-\begin{bmatrix}19\\19\\19\\19\\19\end{bmatrix}=\begin{bmatrix}236\\-19\\86\\221\\26\end{bmatrix}\bmod 26=\begin{bmatrix}2\\7\\8\\13\\0\end{bmatrix}=\begin{bmatrix}C\\H\\I\\N\\A\end{bmatrix}$$

可见，原始消息“China”已得到恢复。

单表代替密码的密钥量很小，不能抵抗穷尽密钥搜索攻击，另外，它没有将明文字母出现的概率掩藏起来，很容易受到频率分析攻击。如果密码分析者知道明文的性质(如非压缩的英语文本)，则分析者就能够利用该语言的规律性进行分析。从这一点意义上讲，汉语在加密方面的特性要优于英语，因为汉语常用字有 3000 多个，而英语只有 26 个字母。

所谓频率分析攻击，就是基于某种语言中各个字符出现的频率不一样，表现出一定的统

计规律,这种统计规律可能在密文中得以保存,从而通过一些推测和验证过程来实现密码分析的方法。如英语的单字母频率分布如图 3.3 所示,由图可见,字母 E 出现的频率最高,接近 13%,其次是 T、N、R、I、O、A、S,出现的频率在 6%～9%之间,B、X、K、Q、J、Z 出现的频率较低,一般低于 1%;就双字母而言,常见的字母组合有 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;常见的三字母组合有 THE、ING、AND、HER、ERE、ENT、THA、NTH、WAS、ETH、FOR、DTH 等。

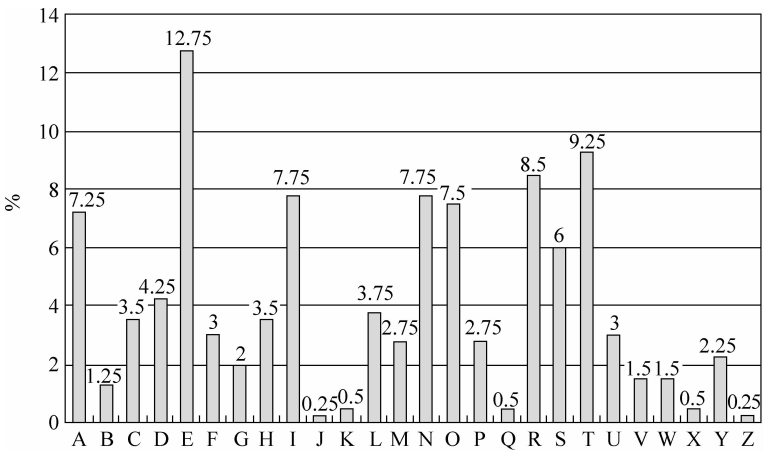



图 3.3　一个长的英文文本中各字母出现的相对频率

频率分析攻击的一般方法:

第一步,对密文中出现的各个字母进行统计,找出它们各自出现的频率。

第二步,根据密文中出现的各个字母的频率,和英语字母标准频率进行对比分析,做出假设,推论加密所用的公式。

第三步,证实上述假设(如果不正确,继续作其他假设)。

**【例 3-5】** 密文为 FMXVE DKAPH FERBN DKRXR SREFM ORUDS DKDVS HVUFE DKAPR KDLYE VLRHH RH。得到的密文字母频次统计表为(单位:次):

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 1 | 0 | 7 | 5 | 4 | 0 | 5 | 0 | 0 | 5 | 2 | 2 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 1 | 1 | 2 | 0 | 8 | 3 | 0 | 2 | 4 | 0 | 2 | 1 | 0 |

其中出现频次较高的是:R-8;D-7;E、H、K-5;F、V-4。

(1) 参照表 3.3 中字母与数字的代替方案,假设:E→R,$f(E)=R$,即 $f(4)=17$;T→D,$f(T)=D$,即 $f(19)=3$。于是有:

$$4k_1+k_2=17(\mathrm{mod}\ 26)$$

$$19k_1+k_2=3(\mathrm{mod}\ 26)$$

以上两式相减可得:

$$15k_1 = -14 \pmod{26} = 12 \pmod{26}$$

于是有：

$$k_1 = 6 \pmod{26}$$

但 6 不与 26 互素，说明不是真正解。猜测应终止，可再做其他假设继续测试。

(2) 再假设：E→R，$f(E)=R$，即 $f(4)=17$；T→H，$f(T)=H$，即 $f(19)=7$。于是有：

$$4k_1 + k_2 = 17 \pmod{26}$$

$$19k_1 + k_2 = 7 \pmod{26}$$

以上两式相减可得：

$$15k_1 = -10 \pmod{26} = 16 \pmod{26}$$

于是有：

$$k_1 = 8 \pmod{26}$$

但 8 不与 26 互素，说明也不是真正解。猜测应终止，可再做其他假设继续测试。

(3) 再假设：E→R，$f(E)=R$，即 $f(4)=17$；T→K，$f(T)=K$，即 $f(19)=10$。于是有：

$$4k_1 + k_2 = 17 \pmod{26}$$

$$19k_1 + k_2 = 10 \pmod{26}$$

以上两式相减可得：

$$15k_1 = -7 \pmod{26} = 19 \pmod{26}$$

于是有：

$$k_1 = 3 \pmod{26}$$

此时 3 与 26 互素，是合法解。再计算出：$k_2=5 \pmod{26}$。

下面验证密钥$(k_1,k_2)=(3,5)$的正确性。

由于 $k_1^{-1}=9 \pmod{26}$，因此，解密函数为：

$x=f^{-1}(y)=k_1^{-1}(y-k_2)=9\cdot(y-5) \pmod{26}$。

将密文分别代入后可解得：ALGORITHMAS ARE QUITE GENERAL DEFINITIONS OF ARITHMETIC PROCESSES。这是一段有意义的字符串，说明所得出的密钥是正确的。

**【例 3-6】**

```
密文：        wklv  phvvdjh    lv qrw  wrr  kdug   wr  euhdn
假设性分析：T---  --------    -- -OT  TOO  -----  TO  ------
            T---  --------    -- NOT TOO  -----  TO  ------
            T-IS  --------    IS NOT TOO  -----  TO  ------
            THIS MESSAGE IS NOT TOO HARD TO BREAK
```

由于该消息长度太短，很难完全用频率分析法分析，还需要结合其他知识。分析如下：

(1) 空格给出了分词的重要信息(实际使用时通常将空格删除，甚至通常将字符分 5 个一组书写)。

(2) 先考虑英语中的短词，如 AM IS TO BE HE WE 等(双字母组合)；AND ARE YOU SHE 等(三字母组合)。

(3) 重要线索：wrr，英文中常用 xyy 结构的常用单词只有 SEE 和 TOO，次常用的单词

还有 ADD、ODD、OFF,特别生疏的单词有 WOO 和 GEE;假设“wrr”为“TOO”。

(4) 单词 lv 是 wklv 的结尾,有可能是双字母单词 SO、IS、IN 等;不存在 T-SO 这种组合的英文单词;由于已假设 q=N,因此不可能为 IN;lv 可能是 IS。

(5) 假设第一个单词是 THIS,即密文的 k 是明文的 H。考察已译出的字母,它们均是明文字母后移 3 位(即恺撒密码),从而可推导出其他字母。

**2. 多表代替密码(Polyalphabetic Cipher)**

单表代替密码表现出明文中单字母出现频率分布与密文中相同,多表代替密码使用从明文字母到密文字母的多个映射来隐藏单字母出现的频率分布,每个映射是简单代替密码中的一对一映射(即处理明文消息时使用不同的单字母代替)。多表代替密码将明文字符划分为长度相同的消息单元,称为明文组,对字符成组进行代替,即使用了多张字符代替表,这样一来同一个字符具有不同的密文,改变了单表代替中密文的唯一性,使密码分析更加困难。多字母代替的优点是容易将字母的自然频度隐蔽或均匀化,从而有利于对抗统计分析。

在多字母代替中,每一组有 $d$ 个字母,每个字母有 26 种可能,故密文取决于 $d, f_1, \cdots, f_d$。对于每一个变换 $f$,有 26!种可能,共有 $d$ 个变换。故密钥总数为 $26! \times 26! \times \cdots \times 26! = (26!)^d$。

Playfair 密码、Hill 密码、Vigenere 密码都是这一类型的密码。

1) Playfair 密码

Playfair 密码出现于 1854 年,英国军队在第一次世界大战期间使用的就是该密码。它将明文中的双字母组合作为一个单元对待,并将这些单元转换为密文双字母组合。Playfair 密码基于一个 5×5 字母矩阵,该矩阵使用一个关键词(密钥)来构造,其构造方法是:从左至右、从上至下依次填入关键词的字母(去除重复的字母),然后以字母表顺序依次填入其他的字母。加密时字母 I 和 J 被当作同一个字母。

对每一对明文字母 $p_1$、$p_2$ 的加密方法如下:

(1) 若 $p_1$、$p_2$ 在同一行时,则对应的密文 $c_1$、$c_2$ 分别是紧靠 $p_1$、$p_2$ 右端的字母。其中第一列被看作是最后一列的右方。(解密时反向)

(2) 若 $p_1$、$p_2$ 在同一列时,则对应的密文 $c_1$、$c_2$ 分别是紧靠 $p_1$、$p_2$ 下方的字母。其中第一行看作是最后一行的下方。(解密时反向)

(3) 若 $p_1$、$p_2$ 不在同一行、也不在同一列时,则 $c_1$、$c_2$ 是由 $p_1$ 和 $p_2$ 确定的矩形的其他两角的字母,并且 $c_1$ 和 $p_1$、$c_2$ 和 $p_2$ 分别同行。(解密时处理方法相同)

(4) 若 $p_1 = p_2$,则插入一个字母(例如 Q,需要事先约定)于重复字母之间,并用前述方法处理。

(5) 若明文字母数为奇数时,则在明文的末端添加某个事先约定的字母作为填充。

**【例 3-7】** 密钥是“PLAYFAIR IS A DIGRAM CIPHER”,则构造的字母矩阵如图 3.4 所示。

如果明文是:

$$p = \text{playfair cipher}$$

先将明文分成两个一组:

pl ay fa ir ci ph er

基于图 3.4 的对应密文为：

LA YF PY RS MR AM CD

再如 $p$=poland，则 $c$=AKAYQR。

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

图 3.4 字母矩阵表

Playfair 密码与简单的单一字母代替法密码相比有了很大的进步。第一，虽然仅有 26 个字母，但有 676(即 26×26)种双字母组合，因此识别各种双字母组合要困难得多；第二，各个字母组的频率要比单字母呈现出大得多的范围，使得频率分析困难得多。由于这些原因，Playfair 密码过去长期被认为是不可破的，它被英国陆军在第一次世界大战中作为一流的密码系统使用，在第二次世界大战中仍被美国陆军和其他同盟国大量使用。但 Playfair 密码还是相对容易攻破(几百字的密文通常就够了)，因为它仍然使许多明文语言的结构保存完好，使得密码分析者能够利用。

2) Vigenere 密码

Vigenere 密码是 16 世纪法国数学家 Blaise de Vigenere 于 1568 年发明的，它是最著名的多表代替密码的例子。Vigenere 密码使用一个词组作为密钥，密钥中每一个字母用来确定一个代替表，每一个密钥字母被用来加密一个明文字母，第一个密钥字母加密明文的第一个字母，第二个密钥字母加密明文的第二个字母，等所有密钥字母使用完后，密钥又再循环使用。Vigenere 密码算法如下：

设密钥 $k=(k_1,k_2,\cdots,k_d)$，明文 $p=(p_1,p_2,\cdots,p_n)$，密文 $c=(c_1,c_2,\cdots,c_n)$。

加密变换：

$$c_i = f_{k_i}(p_i) = e_{k_i}(p_i) = p_i + k_i (\mathrm{mod}\ 26) \tag{3.5}$$

解密变换：

$$p_i = f_{k_i}^{-1}(c_i) = d_{k_i}(c_i) = c_i - k_i (\mathrm{mod}\ 26) \tag{3.6}$$

为了帮助理解该方案，需要构造一个表(如图 3.5 所示)，26 个密文的每个字母都是水平排列的，最左边一列为密钥字母，最上面一行为明文字母。

加密过程：给定一个密钥字母 k 和一个明文字母 p，密文字母就是位于 k 所在的行与 p 所在的列的交叉点上的那个字母。

解密过程：由密钥字母决定行，在该行中找到密文字母，密文字母所在列的列首对应的明文字母就是相应的明文。

**【例 3-8】** $p$=data security，$k$=best。

根据密钥的长度，首先将明文分解成长度为 4 的序列：data secu rity。每一序列利用密钥 $k$=best 进行加密得密文：$c$=EELT TIUN SMLR。

解密方法如前所述。

| 密钥字母 \ 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 3.5　Vigenere 表

3) Hill 密码

Hill 密码是另一种多字母代替密码,它是由数学家 Lester Hill 于 1929 年研制的。与前面介绍的多表代表密码不同的是,Hill 密码要求首先将明文分成同等规模的若干个分组(最后一个分组可能涉及填充),每一个分组被整体加密变换,即 Hill 密码属于分组加密,其余已介绍的密码属于流加密。Hill 密码算法的基本思想:将一个分组中的 $d$ 个连续的明文字母通过线性变换转换为 $d$ 个密文字母。这种变换由 $d$ 个线性方程决定,其中每个字母被分配一个数值(0,1,…,25)。解密只需要做一次逆变换就可以了。密钥就是变换矩阵本身。即:

$$(\text{明文})m = m_1 m_2 \cdots m_d \tag{3.7}$$

$$(\text{密文})c = e_k(m) = c_1 c_2 \cdots c_d \tag{3.8}$$

其中,

$$\begin{aligned} c_1 &= k_{11} m_1 + k_{21} m_2 + \cdots + k_{d1} m_d \pmod{26} \\ c_2 &= k_{12} m_1 + k_{22} m_2 + \cdots + k_{d2} m_d \pmod{26} \\ &\vdots \\ c_d &= k_{1d} m_1 + k_{2d} m_2 + \cdots + k_{dd} m_d \pmod{26} \end{aligned}$$

写成矩阵形式:

$$c_{[1\times d]} = m_{[1\times d]} \cdot k_{[d\times d]} \pmod{26} \tag{3.9}$$

或

$$(c_1,c_2,\cdots,c_d)=(m_1,m_2,\cdots m_d)\cdot\begin{bmatrix}k_{11} & k_{12} & \cdots & k_{1d}\\ \vdots & \vdots & & \vdots\\ k_{d1} & k_{d2} & \cdots & k_{dd}\end{bmatrix}\pmod{26} \tag{3.10}$$

即密文分组＝明文分组×密钥矩阵。

**【例 3-9】** $p$＝hill，使用的密钥为：

$$\boldsymbol{k}=\begin{bmatrix}8 & 6 & 9 & 5\\ 6 & 9 & 5 & 10\\ 5 & 8 & 4 & 9\\ 10 & 6 & 11 & 4\end{bmatrix}$$

hill 被数字化后的 4 个数字是：7,8,11,11。

所以，

$$\boldsymbol{c}=(7\quad 8\quad 11\quad 11)\cdot\begin{bmatrix}8 & 6 & 9 & 5\\ 6 & 9 & 5 & 10\\ 5 & 8 & 4 & 9\\ 10 & 6 & 11 & 4\end{bmatrix}\bmod 26=(9,8,8,24)$$

$$=(\mathrm{JIIY})$$

$\boldsymbol{k}$ 的逆矩阵 $\boldsymbol{k}^{-1}$ 可根据线性代数的矩阵行列式 mod 26 计算得出。由矩阵及其逆矩阵的定义可知 $\boldsymbol{k}\cdot\boldsymbol{k}^{-1}=\boldsymbol{k}^{-1}\cdot\boldsymbol{k}=\boldsymbol{I}$（单位矩阵），$\boldsymbol{k}$ 的逆矩阵 $\boldsymbol{k}^{-1}$ 可表示为：

$$\boldsymbol{k}^{-1}=\boldsymbol{k}^{*}/\det(\boldsymbol{k}) \tag{3.11}$$

式中，$\boldsymbol{k}^{*}$ 为 $\boldsymbol{k}$ 的伴随矩阵；$\det(\boldsymbol{k})$ 为 $\boldsymbol{k}$ 的行列式。

伴随矩阵 $\boldsymbol{k}^{*}$ 的元素可表示为：

$$k_{ji}^{*}=(-1)^{i+j}M_{ij} \tag{3.12}$$

式中，$M_{ij}$ 为矩阵 $\boldsymbol{k}$ 去掉第 $i$ 行、第 $j$ 列后剩余的元素所组成的矩阵的行列式，即元素 $k_{ij}$ 的余子式。

在本例中，$\boldsymbol{k}$ 的行列式：

$$\det(\boldsymbol{k})=\begin{vmatrix}8 & 6 & 9 & 5\\ 6 & 9 & 5 & 10\\ 5 & 8 & 4 & 9\\ 10 & 6 & 11 & 4\end{vmatrix}=-1$$

$$k_{11}^{*}=(-1)^{1+1}M_{11}=\begin{vmatrix}9 & 5 & 10\\ 8 & 4 & 9\\ 6 & 11 & 4\end{vmatrix}=3$$

$$k_{12}^{*}=(-1)^{2+1}M_{21}=\begin{vmatrix}6 & 9 & 5\\ 8 & 4 & 9\\ 6 & 11 & 4\end{vmatrix}=-20$$

$$k_{13}^{*}=(-1)^{3+1}M_{31}=\begin{vmatrix}6 & 9 & 5\\ 9 & 5 & 10\\ 6 & 11 & 4\end{vmatrix}=21$$

$$k_{14}^{*}=(-1)^{4+1}M_{41}=\begin{vmatrix}6&9&5\\9&5&10\\8&4&9\end{vmatrix}=-1$$

类似可得其余元素,于是得到 $\boldsymbol{k}$ 的伴随矩阵为:

$$\boldsymbol{k}^{*}=\begin{bmatrix}3&-20&21&-1\\-2&41&-44&-1\\-2&6&-6&1\\1&-28&30&1\end{bmatrix}$$

所以 $\boldsymbol{k}$ 的逆矩阵为:

$$\boldsymbol{k}^{-1}=\boldsymbol{k}^{*}/\det(\boldsymbol{k})=\begin{bmatrix}3&-20&21&-1\\-2&41&-44&-1\\-2&6&-6&1\\1&-28&30&1\end{bmatrix}\Big/(-1)(\bmod 26)$$

$$=\begin{bmatrix}-3&20&-21&1\\2&-41&44&1\\2&-6&6&-1\\-1&28&-30&-1\end{bmatrix}(\bmod 26)=\begin{bmatrix}23&20&5&1\\2&11&18&1\\2&20&6&25\\25&2&22&25\end{bmatrix}$$


**【问题】** 在计算逆矩阵时可能碰到分数取模的情形,如$\frac{2}{3}\bmod 26$,该如何计算?

**【提示】** 分数取模的运算方法参考第6章例6-11中介绍。

因此解密有:

$$p=\boldsymbol{c}\cdot\boldsymbol{k}^{-1}=(9\quad 8\quad 8\quad 24)\cdot\begin{bmatrix}23&20&5&1\\2&11&18&1\\2&20&6&25\\25&2&22&25\end{bmatrix}\bmod 26$$

$$=(7,8,11,11)$$

$$=(\text{hill})$$

很明显,基于Hill密码加解密的长消息将被分组,分组的长度由密钥矩阵的维数决定。与Playfair算法相比,Hill密码的强度在于完全隐藏了单字母的频率。字母和数字的对应也可以改成其他方案,使得更不容易攻击成功。一般来说,Hill密码能比较好地抵抗频率法的分析,对抗仅有密文的攻击强度较高,但易受已知明文攻击。

总之,代替是密码学中有效的加密方法,20世纪上半叶用于外交通信。对代替加密的破译威胁主要来源如图3.6所示。

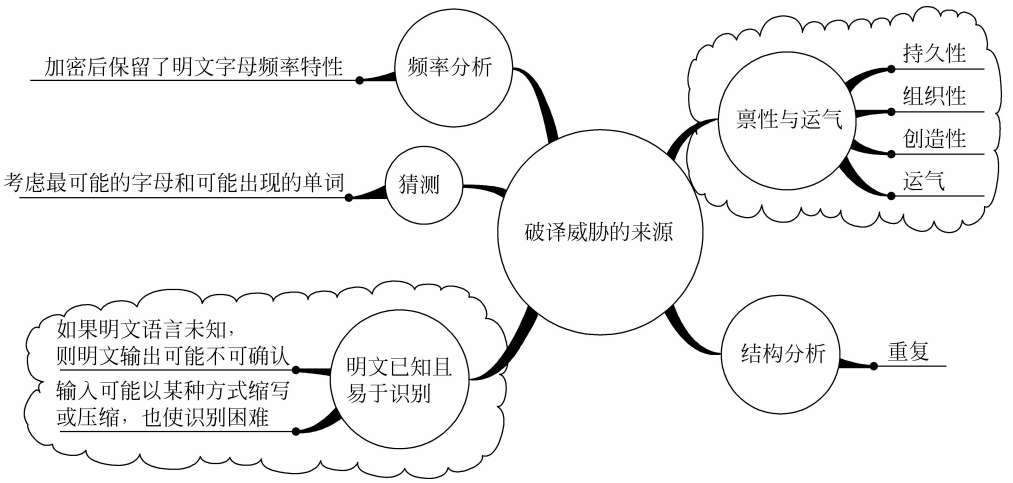



图 3.6 破译威胁的主要来源

## 3.3 换位

上一节所介绍的代替密码操作的目的是制造混乱，使得确定消息和密钥是怎样转换成密文的尝试变得困难。本节将介绍另一类重要的密码变换基本操作——换位。

换位就是重新排列消息中的字母，以便打破密文的结构特性。即它交换的不再是字符本身，而是字符被书写的位置。实际上，古希腊的 scytale 的例子，以及我国古代的藏头诗、回文诗等采用的都是换位的密码处理方法。

一种换位的处理方法是：将明文按行（或列）写在一张格纸上，然后按列（或行）的方式读出结果，即为密文（称为无密钥换位密码）；为了增加变换的复杂性，可以设定读出列（或行）的不同次序（该次序即为算法的密钥），也可以设定不同列（或行）的长度不同（称为有密钥换位密码）。

**【例 3-10】** Alice 要向 Bob 以密文发送的明文是 cryptography is an applied science，假设密钥是 encry。根据密钥中字母在英文字母表中的出现次序可确定为：23145。加密和解密处理的过程如图 3.7 所示。由于密钥长度为 5 个字符，故将每行的宽度确定为 5；发送方 Alice 首先将明文按行写入，然后根据密钥所确定的次序进行列交换；最后，按列从左到右、从上到下读出密文为：YRIPDN COHNII RGYAEE PASPSC TPALCE。该密文传输给接收方后，接收方按照与发送方相反的处理程序经过 3 个步骤，最终恢复出正确的明文。

在换位密码中，密文与明文的字母保持相同但出现的顺序被打乱了，经过多重换位操作有助于混乱的进一步加强。但由于密文字母与明文字母相同，密文中字母的出现频率与明文中字母的出现频率相同，密码分析者可以容易地由此进行判别。

简单的代替和换位操作单独使用时，都不能提供高等级的安全性，但如果将换位与代替密码技术相结合，却可以得到十分有效的强密码编码方案。

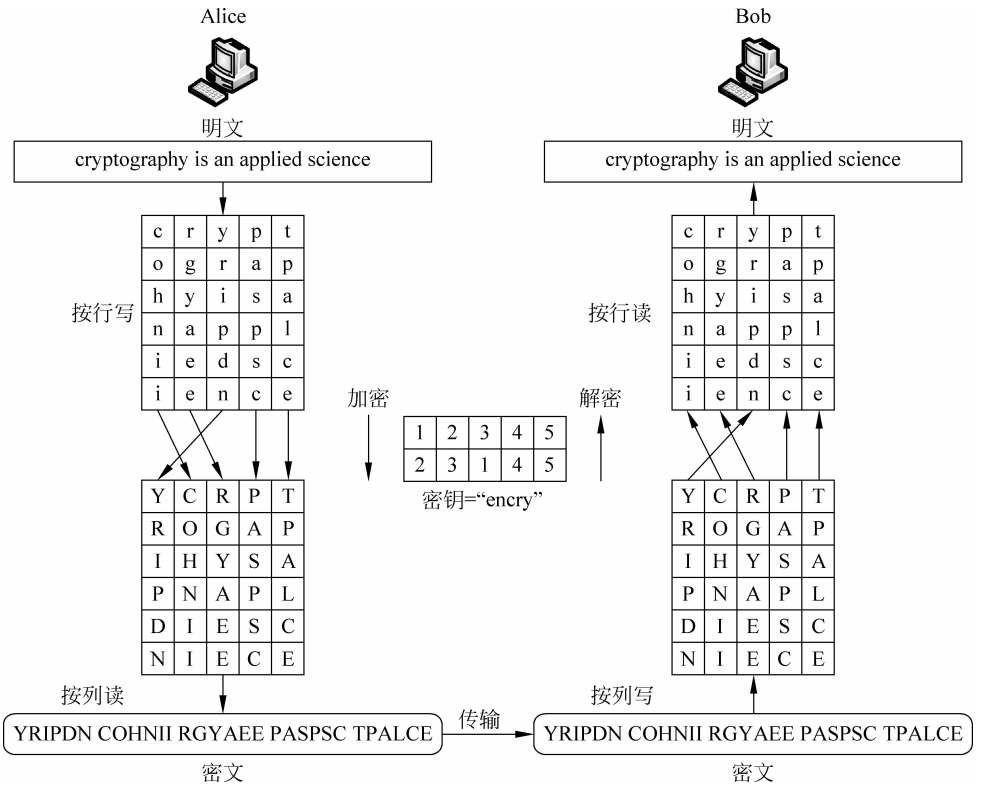



图 3.7　有密钥换位密码示例


3.1　举例说明什么是隐写术。

3.2　区别隐写术与密码编码学。

3.3　下表是用卡丹网格式密码书写的密信,请试着将隐藏的秘密信息提取出来。

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 大 | 风 | 渐 | 起 | ， | 寒 | 流 | 攻 | 击 | 着 | 我 | 们 | 的 | 肌 | 体 | ， | 雪 | 花 | 从 | 天 |
| 空 | 中 | 落 | 下 | ， | 预 | 示 | 明 | 天 | 五 | 点 | 的 | 活 | 动 | ， | 开 | 始 | 时 | 会 | 有 |
| 困 | 难 | 。 | | | | | | | | | | | | | | | | | |

3.4　试写出下图北宋婉约派词人秦观所写的一首回文诗。

3.5 试述代替与换位的区别。

3.6 频率分析的基本处理方法是什么？

3.7 使用穷尽密钥搜索法，破译如下利用代替密码加密的密文：BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD。

3.8 用 Playfair 算法加密明文“Playfair cipher was actually invented by wheatstone”，密钥是 fivestars。

3.9 用 Hill 密码加密明文“pay more money”，密钥是：

$$\boldsymbol{k}=\begin{bmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{bmatrix}$$

3.10 用 Vigenere 算法加密明文“We are discovered save yourself”，密钥是 deceptive。