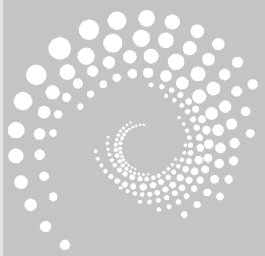
第3章

古 典 密 码

CHAPTER 3



本章将对古典密码[①]进行详细介绍。

3.1 简单替换密码

在简单替换密码（simple substitution cipher）中，消息中的每个字母都被一个固定的替代字母代替。假设有如下消息。

$$M = m_1 m_2 m_3 m_4 \cdots$$

如果 m_1，m_2，$\cdots$ 是连续的字母，则

$$\begin{aligned} E &= e_1 e_2 e_3 e_4 \cdots \\ &= f(m_1) f(m_2) f(m_3) f(m_4) \cdots \end{aligned}$$

通常 $f(m)$ 函数有逆函数，密钥是字母表的排列（当替代物是字母时），例如：

XGUACDTBFHRSLMQVYZWIEJOKNP

此时，第一个字母 X 是 A 的替代物，第二个字母 G 是 B 的替代物，其他字母可以此类推。

3.2 换位（固定周期 d）密码

在换位（transposition）密码中，消息被分为长度为 d 的组，有一个置换作用于第一组，相同置换作用于第二组，以此类推。置换是密钥，可以由前 d 个整数的置换表示。因此，对于 $d = 5$，可能有 2 3 1 5 4 作为置换。例如：

$$\begin{array}{cccccccccc} m_1 & m_2 & m_3 & m_4 & m_5 & m_6 & m_7 & m_8 & m_9 & m_{10} \cdots \\ \downarrow & & & & & & & & & \\ m_2 & m_3 & m_1 & m_5 & m_4 & m_7 & m_8 & m_6 & m_{10} & m_9 \cdots \end{array}$$

两个或多个转置的顺序应用称为复合转置（compound transposition）。如果加密周期为 d_1，d_2，$\cdots$，d_s，则结果是周期 d 的转置，其中 d 是 d_1，d_2，$\cdots$，d_s 的最小公倍数。

换位密码的加密过程如下。

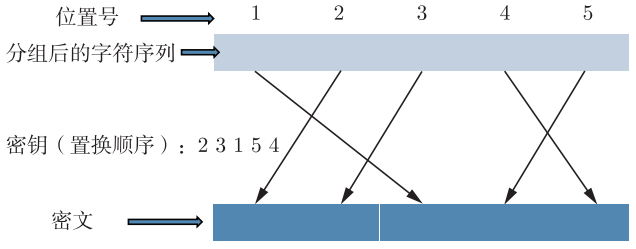


图 3.1 换位密码的加密过程

① “古典”本身就是一个模糊的定义，通常认为香农经典论文发表之前的为“古典”，而利用香农的基本思想设计的密码系统不是“古典密码”。

3.3　凯撒密码

凯撒（Caesar）密码的加密表达式如下。

$$\begin{cases} c = m + 3(\text{mod } 26), & 0 \leqslant m \leqslant 25 \\ m = c - 3(\text{mod } 26), & 0 \leqslant c \leqslant 25 \end{cases} \tag{3.1}$$

下面通过示例说明凯撒密码的具体实现过程。

例　利用凯撒密码对“LI XIAO FENG SHI LAO SHI”进行加密。

分析：需要加密消息的都是大写，使用 ASCII 对其编码并去掉空格，将其变为“LIXIAOFENGSHILAOSHI”。因为 A~Z 的 ASCII 为 65~90，所以编码运算要减去 65，而解码运算要加上 65。

消息：LI　XIAO　FENG　SHI　LAO　SHI
密码：OL　ZLDR　IHQJ　VKL　ODR　VKL

3.4　移位变换（加法）密码

移位变换（shift transformation）密码的加密表达式如下。

$$\begin{cases} c = m + k(\text{mod } 26), & m \geqslant 0,\ k \leqslant 25 \\ m = c - k(\text{mod } 26), & c \geqslant 0,\ k \leqslant 25 \end{cases} \tag{3.2}$$

3.5　维吉尼亚密码

在维吉尼亚（Vigenère）密码中，密钥由 d 个字母序列组成。这些字母在消息下方重复书写，消息和密文模 26 加（考虑字母表编号从 $A = 0$ 到 $Z = 25$），即

$$e_i = m_i + k_i(\text{mod } 26)$$

其中，k_i 在索引 i 中为周期 d。如果密钥为 G A H，则

消息：　N O W I S T H E
重复密钥：　G A H G A H G A H G A
密码：　T O D O S A N E

对该计算过程说明如下。

获得示例加密过程中字母对应的数字：

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

则该过程可以写为

消息：	13	14	22	8	18	19	7	4
重复密钥：	6	0	7	6	0	7	6	0
密文：	19	14	3	14	18	0	13	4

周期为 1、密钥为 D 的维吉尼亚称为凯撒密码。它是一种简单的替换，其中 M 的每个字母在字母表中前进一个固定的量。这个量是密钥，可以是 0～25 的任何数字。所谓的博福特（Beaufort）密码和变异博福特（variant Beaufort）密码类似于维吉尼亚密码，这两种方式分别通过以下表达式加密。

$$e_i = k_i - m_i (\mathrm{mod}\ 26) \tag{3.3}$$

$$e_i = m_i - k_i (\mathrm{mod}\ 26) \tag{3.4}$$

周期为 1 的博福特密码称为反向凯撒密码。

两个或多个维吉尼亚密码按顺序的应用称为复合维吉尼亚密码，其公式为

$$e_i = m_i + k_i + l_i + \cdots + s_i (\mathrm{mod}\ 26)$$

其中，k_i，l_i，$\cdots$，s_i 有不同的周期。通常以它们的和（$k_i + l_i + \cdots + s_i$）的周期作为一个复合变换，该周期是各周期的最小公倍数。

当维吉尼亚密码使用一个没有限制的密钥且永不重复时，可以形成如下维吉尼亚系统。

$$e_i = m_i + k_i (\mathrm{mod}\ 26) \tag{3.5}$$

其中，k_i 是在 0，1，$\cdots$，25 中随机且独立选择的。如果密钥是有意义的文本，则称其为“运行密钥”（running key）密码。[①]

3.6 乘法密码

乘法密码的加密表达式如下。

$$\begin{cases} c = am (\mathrm{mod}\ 26) \\ m = bc (\mathrm{mod}\ 26)，\ b = a^{-1} (\mathrm{mod}\ 26) \end{cases} \tag{3.6}$$

3.7 仿射变换密码

仿射变换（affine transformation）密码的加密表达式如下。

$$\begin{cases} c = am + b (\mathrm{mod}\ 26) \\ m = a^{-1}(c-b) (\mathrm{mod}\ 26)， \quad a \geqslant 0，\ b \leqslant 25，\ \gcd(a，26) = 1，\ a^{-1}a = 1 (\mathrm{mod}\ 26) \end{cases} \tag{3.7}$$

其中，a，b 是密钥。

① “有意义的文本”通常是指一个单词或一个短语，如密钥是“little boy”等。

3.8　多表代换密码

多表代换密码将明文 M 进行分组，每组长度为 n 个字母[①]，分组后的明文序列 $\boldsymbol{M}_1$，$\boldsymbol{M}_2$，$\cdots$，$\boldsymbol{M}_f$，$\boldsymbol{M}_i$ $(i=1,\ 2,\ \cdots,\ f)$ 表示分组消息，其加密表达式如下。

$$\boldsymbol{C}_i = \boldsymbol{A}\boldsymbol{M}_i + \boldsymbol{B} \pmod{N},\ i=1,\ 2,\ \cdots,\ f$$

其中，$\boldsymbol{A}$ 是 $n \times n$ 可逆矩阵，满足 $\gcd(|\boldsymbol{A}|,\ N)=1$；$|\boldsymbol{A}|$ 表示矩阵 $\boldsymbol{A}$ 的行列式；$\boldsymbol{B}$ 为 $n \times 1$ 矩阵；$\boldsymbol{M}_i$ 为一分组的 $n \times 1$ 矩阵表示；$\boldsymbol{C}_i$ 是加密后所得密文分组的 $n \times 1$ 矩阵表示。对密文分组的解密表达式如下。

$$\boldsymbol{M}_i = \boldsymbol{A}^{-1}(\boldsymbol{C}_i - \boldsymbol{B}) \pmod{N}$$

对字母进行加密时，通常取 $N=26$。

3.8.1　游乐场密码

游乐场密码（playfair cipher）是一种特殊类型的二元图替换，它将乱序的 25 个字母写在 5×5 的正方形中（字母 J 在字母方阵中经常被丢弃，因为 J 很少见，当它出现时，可以用 I 代替）。假设密钥正方形如下。

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

图 3.2　密钥正方形

其中，数字符号 AC 的替代物是由 A 和 C 定义的矩形的其他两个角上的一对字母，即 LO（首先取 L，因为它在 A 的上面）。如果数字符号与 RI 在一条水平线上，则使用它们右边 DF 的字母即 RF 变为 DR。如果字母在垂直线上，则使用它们下面的字母，即 PS 变为 UW。如果字母相同，则可以使用空值进行分隔或省略一个字母等。

3.8.2　自动密钥密码

自动密钥密码（autokey cipher）是一种维吉尼亚类型的系统，消息本身或生成的密文被用作“密钥”，称为自动密钥密码。加密从“启动密钥”（整个密钥）开始，并继续使用消息或密文，其长度即启动密钥的长度所取代。

---

① 注意分组密码时的填充问题，即当最后一组密码的长度小于 n 时需要补齐，补齐时需要考虑解密方如何判断解密后的信息是补齐的信息还是原信息。

假设启动密钥是 COMET。如果用消息作为“密钥”，则

消息： SENDSUPPLIES···

密钥： COMETSENDSUP···

密文： USZHLMTCOAYH···

如果用密文作为“密钥”[①]，则

消息： SENDSUPPLIES···

密钥： COMETUSZHLOH···

密文： USZHLOHOSTS···

习题

1. 利用凯撒密码对“nice”进行加密，产生的密文是什么？
2. 简述加法密码和凯撒密码之间的关系。
3. 假设乘法密码的加密函数为 $c = 11m \pmod{26}$，则其解密密钥是多少？
4. 仿射密码通用加密函数为 $c = am + b \pmod{26}$，其中 m 为明文，c 为密文。通常将仿射密码体制中的什么视为此体制的密钥？如果采用了仿射加密，那么在相互传输消息时需要先将密钥告诉对方。假设密钥的交换采用文件方式且文件是通过安全信道传输，试想有几种具体实现的方案，并实现验证。

   提示：

   （1）可以直接将两个变量以二进制的方式写入文件，在使用时依次读出。

   （2）可以定义一个结构体，然后将此结构体直接写入文件，在使用时读出此结构体。

   （3）如果是 Windows 系统，则可以使用 Windows 的 API WritePrivateProfileString 和 GetPrivateProfileString，具体可参考微软官网上的示例代码。当然，也可以自定义函数来实现 WritePrivateProfileString 和 GetPrivateProfileString 功能，以此提高程序的可移植性。Linux 系统中有 ini 文件操作库，则可以定义一个接口库（函数壳），根据不同的编译参数决定链接 Windows 库还是 Linux 库，同样也可以提高程序的可移植性。
5. 仿射密码加密函数为 $c = 17m + 2 \pmod{26}$，求其解密函数。
6. 假设敌手用模 26 的仿射密码加密，获取的密文为 gzyyf。已知明文是 “he” 开头，请破解此消息。
7. 假设仿射变换的加密是 $\boldsymbol{E}_{11,\ 23}(m) = 11m + 23 \pmod{26}$，对明文 “the national security agency” 加密，并用解密变换 $\boldsymbol{D}_{11,\ 23}(c) = 11^{-1}(c - 23) \pmod{26}$ 进行解密验证。

① 从保密的角度来看，这个系统是微不足道的，因为除了开头的 d 个字母外，敌人会拥有整个“密钥”。

8. 假设由仿射变换对一个明文加密得到的密文为 “edsgickxhuklzveqzvkxwkzzukvcuh”。已知明文的前两个字符为 “if”，对该明文解密。
9. 已知一个多表替代的加密函数如下，计算该加密函数对应的解密函数。

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 11 & 2 \\ 5 & 23 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \pmod{26} \tag{3.8}$$

其中，(y_1, y_2) 为密文，(x_1, x_2) 为明文。

10. 假设在多表代换密码中，$\boldsymbol{A} = \begin{pmatrix} 3 & 13 & 21 & 9 \\ 15 & 10 & 6 & 25 \\ 10 & 17 & 4 & 8 \\ 1 & 23 & 7 & 2 \end{pmatrix}$，$\boldsymbol{B} = \begin{pmatrix} 1 \\ 21 \\ 8 \\ 17 \end{pmatrix}$ 加密为 $\boldsymbol{C}_i = \boldsymbol{A}\boldsymbol{M}_i + \boldsymbol{B} \pmod{26}$，对明文 “PLEASE SEND ME THE BOOK，MY CREDIT CARD NO IS SIX ONE TWO ONE THREE EIGHT SIX ZERO ONE SIX EIGHT FOUR NINE SEVEN ZERO TWO” 用解密变换 $\boldsymbol{M}_i = \boldsymbol{A}^{-1}\boldsymbol{C}_i - \boldsymbol{B} \pmod{26}$ 验证结果，其中 $\boldsymbol{A}^{-1} = \begin{pmatrix} 23 & 13 & 20 & 5 \\ 0 & 10 & 11 & 0 \\ 9 & 11 & 15 & 22 \\ 9 & 22 & 6 & 25 \end{pmatrix}$。
11. 假设在多表代换密码 $\boldsymbol{C}_i = \boldsymbol{A}\boldsymbol{M}_i + \boldsymbol{B} \pmod{26}$ 中，$\boldsymbol{A}$ 是二阶矩阵，$\boldsymbol{B}$ 是零矩阵。已知明文 “dont” 被加密为 “elni”，求矩阵 $\boldsymbol{A}$。