

2.4 多字母代换密码

- 2.4.1 几种多字母函数
- 1. 普莱费尔密码
- 这是一种著名的双码代换密码，它的密钥由 5×5 阶矩阵给定，将英文字母随机填入阵中，将I和J算作一个字母。
- 可选定一个密钥字，除去重复字母后依次按行填入阵中，而后将字母表中还没用上的各字母继续按行填入阵中，就得到密钥阵K。

- 将明文划分成长为 $L=2$ 的组或字母对，用 (m_1, m_2) 表示，它们在密钥阵 K 中的位置用 (k_{ij}, k_{ln}) ，假设 $(m_1 \neq m_2)$ ，那么 $(m_1, m_2) = (k_{ij}, k_{ln})$ 的密文字母为：

$$(c_1, c_2) = \begin{cases} (k_{in}, k_{lj}) & \text{若 } i \neq l, \text{ 且 } j \neq n \\ (k_{i, j+1}, k_{i, n+1}) & \text{若 } i = l, \text{ 且 } j \neq n \\ (k_{i+1, j}, k_{l+1, j}) & \text{若 } i \neq l, \text{ 且 } j = n \end{cases}$$

式中，下标指数按模5运算。

如果 $m_1 = m_2$ ，那么可在 m_1 和 m_2 之间插入哑字母如 x ，那么明文变为 $\dots m_1 x m_2 \dots$ 。

- 例2.5: 明文 $m = \text{cryptographic system}$, 取 cryptology 为密钥字, 那么其密钥阵就是:

$$K = (k_{ij}) = \begin{pmatrix} C & R & Y & P & T \\ O & G & A & H & B \\ D & E & F & I & K \\ L & M & N & Q & S \\ U & V & W & X & Z \end{pmatrix}$$

相应加密结果是:

$m = \text{cr yp to gr ap hi cs ys te mx}$

$c = \text{RY PT CB EG HY IQ TL TN RK QV}$

• 2.矩阵变换密码

令明码表 Z_q ，采用 L 个字母进行
代换加密映射 $f: Z_q^L \rightarrow Z_q^L$ 。

假设映射是线性变换，可用 Z_q 上的 $L \times L$ 矩阵 T 表示
假设 T 是满秩的，那么变换为一一对应映射，存在
逆变换 T^{-1} ，使 $TT^{-1} = T^{-1}T = I$ 。

将 L 个字母的数字表示为 Z_q 上的 L 维向量

$m = (m_1, m_2, \dots, m_L)$,

那么相应的密文向量 $c = (c_1, c_2, \dots, c_L)$ 为 $mT = c$ 。

把 T^{-1} 作为解密矩阵，可由 c 恢复出相应明文 $cT^{-1} = m$

- 例2.7: 设 $q=26$, $L=4$, 选满秩阵

$$T = \begin{pmatrix} 8 & 6 & 5 & 10 \\ 6 & 9 & 8 & 6 \\ 9 & 5 & 4 & 11 \\ 5 & 10 & 5 & 4 \end{pmatrix}$$

加密时, 先将字母按下述乱序表变换成 Z_{26} 上的整数:

Abcdefghijklmnopqrstuvwxyz
3 15 4 10 1 13 7 24 2 16 9 14 5 12 20 6 18 25 8 19 22 21 0 17 23 11

对明文 $m=\text{cryptographic system}$ 的前 4 个字母组变换成量 $x=(4,25,23,6)$

由 $xT(\text{mod } 26)$ 得密文 $y=(3,8,2,25)$, 相应密文字母为 ASIR
类似可依次对后面明文组加密。

假设最后一组明文缺乏4个字母, 就加上哑字母 (如 x) 凑足4个。

最后可求得密文为 ASIR QGLT WCFW BMSK IPWG。

- 加密中，4个字母为一个整体，变换其中任一个明文字母都会使相应的4个密文字母受到影响。例如，将cryp变为crmp所得密文就由ASIR变为YUSK。
- 该例的逆阵

$$T^{-1} = \begin{pmatrix} 23 & 2 & 2 & 25 \\ 20 & 11 & 20 & 2 \\ 5 & 18 & 6 & 22 \\ 1 & 1 & 25 & 25 \end{pmatrix}$$

由 $yT^{-1}(\text{mod}26)$ 可得到 x ，由 x 及乱序表就可恢复出明文。

- 3.扩表法
- 扩表法就是将字母表 Z_q 扩展为 Z_q^L ，然后再采用单表代换。
- 将 Z_q 上的 L 个字母 $m_0, m_1, \dots, m_{L-1}$ 表示成 Z_q^L 中的整数
- $$x = m_0 + m_1q + m_2q^2 + \dots + m_{L-1}q^{L-1}$$
- 任一 L 长字母组都变成 $Z_q^L = \{0, 1, \dots, q^{L-1}\}$ 上的某个元素，然后再对该元素加密。

- 例2.8: 英文字母表 $Z_{26}=\{0,1,\dots,25\}$, 采用双码扩表加密, 那么 $Z_{26^2}=\{0,1,\dots,675\}$ 。
- 明文字母对is可表示成 Z_{26^2} 中的数字 $x=8+18\times 26=476$ 。
- 对 Z_{26^2} 采用仿射变换, 取 $k_0=576, k_1=129$
- $y\equiv 129\times 476+576\equiv 464$
- $\equiv 17\times 26+22(\text{mod } 675),$
- 相应密文字母为WR。
- 解密时先将密文字母WR变换成中的元素, 即 $y=17\times 26+22=464$, 而后按加密的反变换求解出 $x=18\times 26+8$ 。

- 2.4.2 密码分析
- 同样可以有分析方法。

2.5 Shannon理论

- 在密码系统中，对信息 m 的加密变换作用类似于向信息注入噪声。
- 密文 c 就相当于经过有扰信道得到的接收信息，密码分析就相当于在有扰信道下去除噪声，恢复原文。
- 所不同的是，这种干扰不是信道中的自然干扰，而是发送者有意加进的，目的是使窃听者难以恢复出原来的信息。

- **Shannon在1949年发表了“Communication theory of secrecy system”一文，用信息论的观点对信息加密问题作了全面阐述，深化了人们对密码学的理解，使信息论成为研究密码学的一个重要理论根底。**
- **Shannon从概率统计观点出发研究信息的传输和保密问题，将通信系统归为图2.1，将密码系统归为图2.2。**

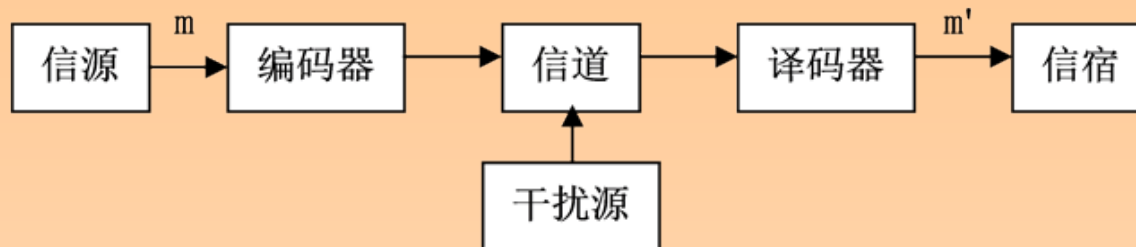


图 2.1 通信系统

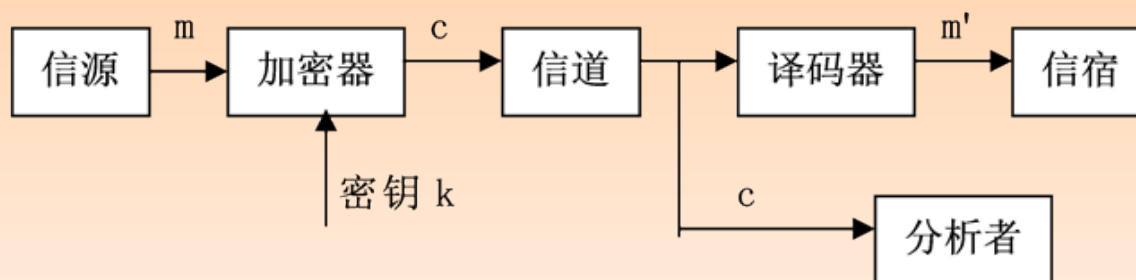


图 2.2 密码系统

通信系统设计目的是在信道有扰条件下，使接收的信息无错或过失尽可能地小。

密码系统设计的目的在于使窃听者即使在完全准确地收到了接收信号也无法恢复出原始信息。

在密码系统研究中，假定信道是没有自然干扰的。

• 2.4.5信息量和熵

定义 2.1：对于集合 $X=\{x_1, x_1, \dots, x_n\}$ ，有 $\sum_{i=1}^n p(x_i) = 1$ 。这

里 $p(x_i)$ 为事件 x_i 出现的概率。 x_i 出现给出的信息量定义为： $I(x_i) = -\log_a p(x_i)$ 。当 $a=2$ 时，相应的信息单位称为比特(bit)。

信息量反映了事件 x_i 出现的可能性大小，也是为确定事件 x_i 出现所必须付出的信息量。

定义 2.2: 将集合 X 中事件出现给出的信息量的统计平均值

$H(X) = -\sum_{i=1}^n p(x_i) \log_2 p(x_i) \geq 0$ 称为集合 X 的熵。当 $p(x_i)=0$ 时,

定义 $p(x_i) \log_a p(x_i) = 0$ 。

- 熵表示集合 X 中出现一个事件平均给出的信息量, 或者是集合 X 中事件的平均不确定性, 或者是确定集合 X 出现一个元素必须提供的信息量。
- 定理2.2: 对任意有 n 个事件的集合 X 有:
 $0 \leq H(X) \leq \log_2 n$ 。

设两事集

$X=\{x_1, x_2, \dots, x_n\}$ 和 $Y=\{y_1, y_2, \dots, y_m\}$, 联

合事集

$XY=\{x_i y_j, i=1, \dots, n, j=1, \dots, m\}$, $x_i y_j$ 的概为

$p(x_i y_j)$, 且

$$\sum_{i=1}^n p(x_i) \sum_{j=1}^m p(y_j | x_i) = \sum_{j=1}^m p(y_j) \sum_{i=1}^n p(x_i | y_j) = 1。$$

定义 2.3: 对于集合 X 和 Y 的联合事件集 XY 中事件出现给出的信息量的统计平均值

$H(XY) = -\sum_{i=1}^n \sum_{j=1}^m p(x_i y_j) \log_2 p(x_i y_j)$ 称为 X 和 Y 的联合熵。称

$H(X|Y) = -\sum_{j=1}^m \sum_{i=1}^n p(x_i y_j) \log_2 p(x_i | y_j)$ 和 $H(Y|X) = -\sum_{i=1}^n \sum_{j=1}^m p(x_i y_j) \log_2 p(y_j | x_i)$ 为

条件熵, 又称为含糊度。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/986144212211010234>