现代密码学

Modern Cryptography

张方国

中山大学计算机学院

Office: Room 305, IM School Building

E-mail: isszhfg@mail.sysu.edu.cn

HomePage: https://cse.sysu.edu.cn/content/2460

第三讲 古典密码学2

- 代换密码：
  希尔密码
- 置换密码及其密码分析
- 流密码及其密码分析
- 古典密码学的意义

希尔（Hill）密码

Hill密码算法的基本思想是将*n*个明文字母通过线性变换，将它们转换为*n*个密文字母。解密只需做一次逆变换即可。

算法的密钥***K*** **=｛** Z_{26}上的 $n\times n$可逆矩阵｝，明文***M***与密文***C***均为***n***维向量，记为

$$M=\begin{pmatrix} m_1\\ m_2\\ \vdots\\ m_n\end{pmatrix},\quad C=\begin{pmatrix} c_1\\ c_2\\ \vdots\\ c_n\end{pmatrix},\quad K=(k_{ij})_{n\times n}=\begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1n}\\ k_{21} & \ddots & & \\ \vdots & & \ddots & \\ k_{n1} & k_{n2} & \cdots & k_{nn}\end{bmatrix}$$

其中，

$$\begin{cases} c_1 = k_{11}m_1 + k_{12}m_2 + \ldots + k_{1n}m_n \bmod 26\\ c_2 = k_{21}m_1 + k_{22}m_2 + \ldots + k_{2n}m_n \bmod 26\\ \qquad\qquad\ldots\ldots\\ c_n = k_{n1}m_1 + k_{n2}m_2 + \ldots + k_{nn}m_n \bmod 26\end{cases}$$

或写成

$$C = K\cdot M\ (\mathrm{mod}\ 26)$$

解密变换则为：

$$M = K^{-1}\cdot C(\mathrm{mod}\ 26).$$

其中，K^{-1}为K在模26上的逆矩阵，满足：$K\ K^{-1} = K^{-1}\ K = I \pmod{26}$

这里 I 为单位矩阵。

定理：假设A = ($a_{i,j}$) 为一个定义在Z_{26}上的$n \times n$矩阵，若A 在模26上可逆，则有： $A^{-1} = (\det A)^{-1} A^* \pmod{26}$；这里$A^*$为矩阵A的伴随矩阵

在$n = 2$的情况下，有下列推论：

假设 $A=\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$，是一个$Z_{26}$上的2×2矩阵，它的行列式：

$\det A = a_{1,1}a_{2,2} - a_{1,2}a_{2,1}$ 是可逆的，那么：$A^{-1} = (\det A)^{-1}\begin{pmatrix} a_{2,2} & -a_{1,2} \\ -a_{2,1} & a_{1,1} \end{pmatrix} \bmod 26$

例如， $K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$

$$\det\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = 11\times 7 - 3\times 8 \pmod{26} = 77 - 24 \pmod{26} = 53 \pmod{26} = 1$$

这时 $1^{-1} \bmod 26 = 1$ ，所以*K*的逆矩阵为：

$$K^{-1} = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}^{-1} = 1^{-1} \times \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \bmod 26$$

【例2.5】设明文消息为**good**，试用***n*=2**，密钥 $K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$ 的**Hill**密码对其进 行加密，然后再进行解密。

解：将明文划分为两组：**(g，o)** 和 **(o，d)**，即（**6，14**）和（**14，3**）。

加密过程如下：

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = K\begin{pmatrix} m_1 \\ m_2 \end{pmatrix} = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}\begin{pmatrix} 6 \\ 14 \end{pmatrix} = \begin{pmatrix} 178 \\ 116 \end{pmatrix} \equiv \begin{pmatrix} 22 \\ 12 \end{pmatrix} \pmod{26} \Rightarrow \begin{pmatrix} w \\ m \end{pmatrix}$$

$$\begin{pmatrix} c_3 \\ c_4 \end{pmatrix} = K\begin{pmatrix} m_3 \\ m_4 \end{pmatrix} = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}\begin{pmatrix} 14 \\ 3 \end{pmatrix} = \begin{pmatrix} 178 \\ 63 \end{pmatrix} \equiv \begin{pmatrix} 22 \\ 11 \end{pmatrix} \pmod{26} \Rightarrow \begin{pmatrix} w \\ l \end{pmatrix}$$

因此，**good**的加密结果是***wmwl***。显然，明文不同位置的字母“**o**”加密成

的密文字母不同。为了解密，由前面计算有 $K^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$ ，可由密文解密计算出明文：

$$\begin{pmatrix} m_1 \\ m_2 \end{pmatrix} = K^{-1}\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}\begin{pmatrix} 22 \\ 12 \end{pmatrix} = \begin{pmatrix} 370 \\ 638 \end{pmatrix} \equiv \begin{pmatrix} 6 \\ 14 \end{pmatrix} \pmod{26} \Rightarrow \begin{pmatrix} g \\ o \end{pmatrix}$$

$$\begin{pmatrix} m_3 \\ m_4 \end{pmatrix} = K^{-1}\begin{pmatrix} c_3 \\ c_4 \end{pmatrix} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}\begin{pmatrix} 22 \\ 11 \end{pmatrix} = \begin{pmatrix} 352 \\ 627 \end{pmatrix} \equiv \begin{pmatrix} 14 \\ 3 \end{pmatrix} \bmod 26 \Rightarrow \begin{pmatrix} o \\ d \end{pmatrix}$$

因此，解密得到正确的明文“good”。

Hill密码分析

- 完全隐藏了字符(对)的频率信息
- 密钥空间较大，在忽略密钥矩阵K可逆限制条件下，$|K|=26^{n\times n}$
- 惟密文攻击相对较难
- 线性变换的安全性很脆弱，易被已知明文攻击击破。
- 对于一个mxm的hill密码，假定有m个明文-密文对，明文和密文的长度都是m.可以把明文和密文对记为：$P_j=(p_{1j}, p_{2j}, .. p_{mj})$和$C_j=(C_{1j}, C_{2j}, \ldots, C_{mj})$，$C_j=P_jK, 1\le j \le m$
  定义mxm的方阵$X=(P_{ij})$ $Y=(C_{ij})$，得到$Y=XK$，$K=X^{-1}Y$

置换密码(Permutation Cipher)

- 置换密码又称为换位密码，通过改变明文消息各元素的相对位置，但明文消息元素本身的取值或内容形式不变。它是对明文L长字母组中的字母位置进行重新排列，而每个字母本身并不改变。

明文：$\boldsymbol{m}=m_1 m_2,\ldots,m_L$。，

加密变换：$\boldsymbol{c}=(c_1,c_2,\ldots,c_L)=E_\pi(\boldsymbol{m})=m_{\pi(1)}\, m_{\pi(2)} \ldots m_{\pi(L)}$。

解密变换：

$$d_\pi(c)=(c_{\pi^{-1}(1)},\ldots,c_{\pi^{-1}(L)})=(m_1 \ldots m_L)$$

密码体制 1.6　置换密码

令 m 为一正整数。$\mathcal{P}=\mathcal{C}=(\mathbb{Z}_{26})^m$，$\mathcal{K}$ 由所有定义在集合 $\{1,2,\cdots,m\}$ 上的置换组成。对任意的密钥(置换) π，定义加密变换：

$$e_\pi(x_1,\cdots,x_m)=(x_{\pi(1)},\cdots,x_{\pi(m)})$$

相应的解密变换为：

$$d_\pi(y_1,\cdots,y_m)=(y_{\pi^{-1}(1)},\cdots,y_{\pi^{-1}(m)})$$

上式中 π^{-1} 为置换 π 的逆置换。

置换密码的例子

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

x	1	2	3	4	5	6
$\pi^{-1}(x)$	3	6	1	5	2	4

假设我们要加密的明文为：

sheselllsseashellsbytheseashore

首先，将明文字母分为每六个一组：

shesel | lsseas | hellsb | ythese | ashore

对每组的六个字母使用加密变换 π，则可得：

EESLSH | SALSES | LSHBLE | HSYEET | HRAEOS

因此，最后的密文如下：

EESLSHSALSESLSHBLEHSYEETHRAEOS

置换密码在实质上是Hill密码的特例

给定一个集合{1，2， . . .，n}的置换π，写出置换矩阵为

$$K_\pi = (k_{ij})_{n\times n} \qquad k_{ij} = \begin{cases} 1 & \text{若} j = \pi(i) \\ 0 & \text{否则} \end{cases}$$

；表示仅第i行中第π(i)个元素为1，其余为零。

这时，置换矩阵是每一行和每一列都刚好有一个“1”，而其余元素为“0”的稀疏矩阵。

如加解密置换π=(3 5 1 6 4 2)，π^{-1}=（3 6 1 5 2 4），对应的置换矩阵为：

$$K_\pi = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \qquad K_{\pi^{-1}} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

加密变换： $E_{\pi}(M)=E_{\pi}(m_1,m_2,\cdots m_n)=(m_{\pi(1),\ldots,}m_{\pi(n)})=K_{\pi}\cdot M=(c_1,c_2,\cdots c_n)$

解密变换： $D_{\pi}(C)=D_{\pi}(c_1,c_2,\ldots,c_n)=(c_{\pi^{-1}(1)}c_{\pi^{-1}(2)}\ldots\ldots c_{\pi^{-1}(n)})$

$$= K_{\pi}^{-1}\cdot C = M$$

所以，置换密码实质上是输入分组的一个线性变换。

置换密码安全性

- 不能抗击已知明密文攻击

密码体制的分类

依据对信息元素的处理方式分类 $\begin{cases} \text{序列(流)密码} \\ \text{分组(块)密码} \end{cases}$

一个密码体制的明文必要分组长度n若为1，则称该密码为序列（流）密码，否则（即n>1）称该密码为分组（块）密码。

流密码

- 在前面研究的密码体制中，密文串是通过如下方式得到：

  $y=y_1y_2\ldots=e_k(x_1)e_k(x_2)\ldots$

这种类型的密码体制称为分组密码

- 另一种广泛使用的密码体制为流密码，其基本思想是产生一个密钥流$z=z_1z_2\ldots$,然后使用如下规则来加密$x=x_1x_2\ldots$

  $y=y_1y_2\ldots=e_{z1}(x_1)e_{z2}(x_2)\ldots$

流密码

根据密钥流是否依赖明文流，可将流密码分为两种：

(1)同步流密码，就是生成的密钥流独立于明文流；

(2)异步流密码，密钥流不仅与密钥有关，还与明文或密文相关。

同步流密码

同步流密码是一个六元组(*P*，*C*，*K*，*L*，*E*，*D*)和函数*g*，且满足下面条件：

（1）*P*是一个非空有限集合，表示所有的明文空间。

（2）*C*是一个非空有限集合，表示所有的密文空间。

（3）*K*是一个非空有限集合，表示所有的密钥空间。

同步流密码

（4）**L是一个非空有限集合，表示密钥流字母表。**

（5）**g是一个密钥流生成器。g将密钥k作为输入产生一个无限的密钥流** $z = z_1 z_2 \ldots, z_i \in L,\ i=1,2,\ldots$。

对每一个$z \in L$**，都有一加密函数**$E_z \in E$**和相应的解密函数**$D_z \in D$**使得对任意明文**$x \in P$**，都有** $D_z(E_z(x))=x$。

维吉尼亚密码是流密码

我们利用前面提到的维吉尼亚密码给同步流密码定义一个解释。假设 m 为维吉尼密码的密钥长度，定义 $\mathcal{K}=(\mathbb{Z}_{26})^m$，$\mathcal{P}=\mathcal{C}=\mathcal{L}=\mathbb{Z}_{26}$；定义 $e_z(x)=(x+z)\bmod 26$，$d_z(y)=(y-z)\bmod 26$。再定义密钥流 $z_1z_2\cdots$，如下所示：

$$z_i=\begin{cases}k_i & 若\ 1\leqslant i\leqslant m\\ z_{i-m} & 若\ i\geqslant m+1\end{cases}$$

上式中 $K=(k_1,k_2,\cdots,k_m)$，这样利用 K 可产生的密钥流如下：

$$k_1k_2\cdots k_mk_1k_2\cdots k_mk_1k_2\cdots$$

如果对所有 $i\geqslant 1$ 的整数有 $z_{i+d}=z_i$，则称该流密码为具有周期 d 的周期流密码。如上面分析的密钥字长为 m 的维吉尼亚密码可看做是周期为 m 的流密码。

同步流密码的产生方法

- 线性移位寄存器LFSR

下面给出另一个产生(同步)密钥流的方法。假设以$(k_1, k_2, \cdots, k_m)$开始,并且$z_i = k_i, 1 \leqslant i \leqslant m$。利用次数为$m$的线性递归关系来产生密钥流:

$$z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j} \bmod 2$$

这里$c_0, c_1, \cdots, c_{m-1} \in \mathbb{Z}_2$是确定的常数。

- 例1.8 设m=4,密钥流按照如下线性递归关系产生：$z_{i+4}=(z_i+z_{i+1})\bmod 2$ $i>0$.
- 若初始向量为(1,0,0,0)

  则密钥流为：100010011010111…
- 若初始向量为(1,0,0,1)

  则密钥流为：

基于LFSR的同步流密码分析

密文是明文和密钥流的模2加，即 $y_i = (x_i + z_i) \bmod 2$。

线性递归关系从初态 $(z_1, z_2, \cdots, z_m) = (k_1, k_2, \cdots, k_m)$ 产生密钥流：

$$z_{m+i} = \sum_{j=0}^{m-1} c_j z_{i+j} \bmod 2, \quad i \geq 1$$

这里 $c_0, c_1, \cdots, c_{m-1} \in \mathbb{Z}_2$。

因为这个密码体制中所有运算都是线性的，同前面的希尔密码一样，它容易受到已知明文攻击。假定 Oscar 有了明文串 $x_1 x_2 \cdots x_n$ 和相应的密文串 $y_1 y_2 \cdots y_n$，那么他能计算密钥流比特 $z_i = (x_i + y_i) \bmod 2, 1 \leq i \leq n$。若 Oscar 再知道 m 的值，那么 Oscar 仅需要计算 $c_0, c_1, \cdots, c_{m-1}$ 的值就能重构整个密钥流。换句话说，他只需要确定 m 个未知的值就够了。

同步流密码分析

现在已知，对任何 $i \geq 1$，我们有

$$z_{m+i} = \sum_{j=0}^{m-1} c_j z_{i+j} \bmod 2$$

它是 m 个未知数的线性方程。如果 $n \geq 2m$，就有 m 个未知数的 m 个线性方程，利用它就可以解出这 m 个未知数。

m 个线性方程能以矩阵形式表示为：

$$(z_{m+1}, z_{m+2}, \cdots, z_{2m}) = (c_0, c_1, \cdots, c_{m-1})\begin{bmatrix} z_1 & z_2 & \cdots & z_m \\ z_2 & z_3 & \cdots & z_{m+1} \\ \vdots & \vdots & \ddots & \vdots \\ z_m & z_{m+1} & \cdots & z_{2m-1} \end{bmatrix}$$

如果系数矩阵有逆(模 2)，则可解得：

$$(c_0, c_1, \cdots, c_{m-1}) = (z_{m+1}, z_{m+2}, \cdots, z_{2m})\begin{bmatrix} z_1 & z_2 & \cdots & z_m \\ z_2 & z_3 & \cdots & z_{m+1} \\ \vdots & \vdots & \ddots & \vdots \\ z_m & z_{m+1} & \cdots & z_{2m-1} \end{bmatrix}^{-1}$$

异步流密码

在流密码中，还有这样一种情况，密钥流 z_i 的产生不但与密钥 K 有关，而且还与明文元素 $(x_1,\cdots,x_{i-1})$ 或密文元素 $(y_1,\cdots y_{i-1})$ 有关，这类流密钥我们称为异步流密码。下面给出一个来源于维吉尼亚密码的异步流密码，称做自动密钥密码。称为“自动密钥”的原因是因为它使用明文来构造密钥流(除了最初的“原始密钥”外)。当然，由于仅有26个可能的密钥，自动密钥密码是不安全的。

密码体制 1.7 自动密钥密码

设 $\mathcal{P}=\mathcal{C}=\mathcal{K}=\mathcal{L}=\mathbb{Z}_{26}$，$x_1=K$，定义 $z_i=x_{i-1}$，$i\geq 2$。对任意的 $0\leq z\leq 25$，$x,y\in\mathbb{Z}_{26}$，定义

$$e_z(x)=(x+z)\bmod 26$$

和

$$d_z(y)=(y-z)\bmod 26$$

- 例1.9:

- 对称密码体制主要分为分组密码和流密码
- **对称密码的两个基本运算**
  - **代换和置换(Substitution & permutation)**
- **对称密码的两个基本设计原则:**
  扩散（Diffusion):明文的统计结构被扩散消失到密文的长程统计特性,使得明文和密文之间的统计关系尽量复杂
  混乱(confusion)：使得密文的统计特性与密钥的取值之间的关系尽量复杂

经典密码算法特点

- 要求的计算强度小
- DES之前
- 以字母表为主要加密对象
- 替换和置换技术
- 数据安全基于算法的保密
- 密码分析方法基于明文的可读性以及字母和字母组合的频率特性