现代密码学

第六讲 古典密码算法

电子科技大学
信息与软件工程学院

第六讲 古典密码算法

- 置换密码
- 单表代替密码算法
- 多表代替密码算法

置换（Permutation）密码

- 对明文字符或字符组进行位置移动的密码
- 明文的字母保持相同，但顺序被打乱了。

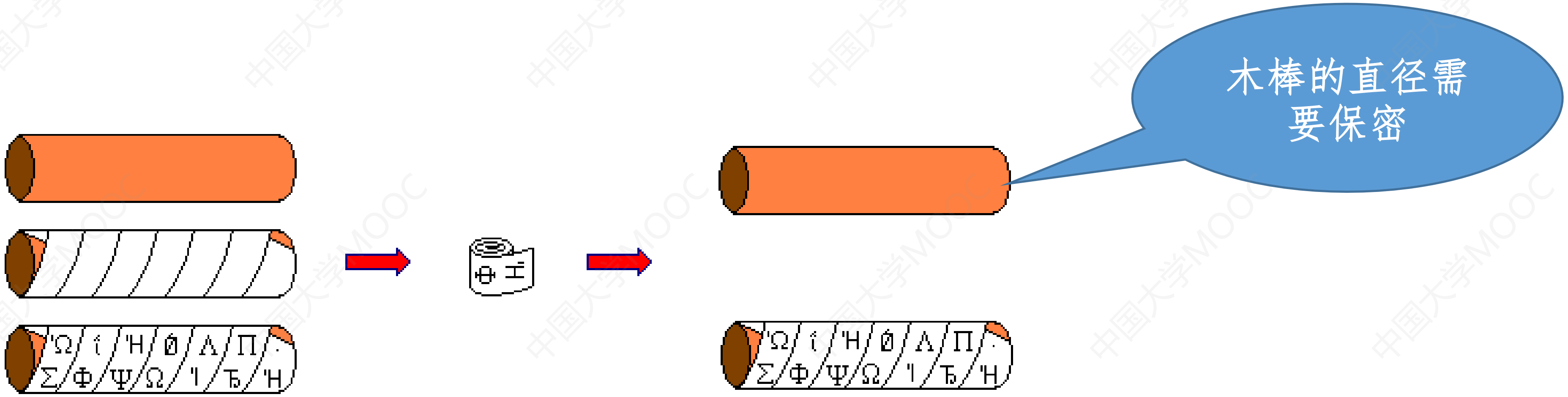
置换密码

- 对明文字符或字符组进行位置移动的密码
- 明文的字母顺序被打乱了，但明文字母本身不变

ATCADWTAKTAN

天书（Scytale）

- **500 B.C.，斯巴达人在军事上用于加解密**
  - 发送者把一条羊皮纸螺旋形地缠在一个圆柱形木棒上，核心思想是置换



第六讲 古典密码算法

- 置换密码
- 单表代替密码算法
- 多表代替密码算法

代替密码

- 代替(Substitution)密码构造一个或多个密文字母表，然后用密文字母表中的字母或者字母组来代替明文字母或字母组，各字母或字母组的相对位置不变，但其本身的值改变了。

- 代替密码分为单表代替密码和多表代替密码

字母与数字的转换

代替密码算法针对英文字母进行处理。首先将26个字母与十进制数字中的0~25一一对应，如下表所示。而这里的数的加法和乘法都定义为模26的加法和乘法。

字母	a	b	c	d	e	f	g	h	i	j	k	l	m
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
数字	13	14	15	16	17	18	19	20	21	22	23	24	25

单表代替密码

单表代替密码可分为

- 加法密码
- 乘法密码
- 仿射密码

单表代替密码——加法密码

$$y = x + k(\mathrm{mod}26)$$

明文：x

密文：y

密钥：k

解密：$x = y - k(\mathrm{mod}26)$

Caesar密码就是一种加法密码（k=3）

明文字母	ABCDEFGHIJKLMNOPQRSTUVWXYZ
密文字母	DEFGHIJKLMNOPQRSTUVWXYZABC

- 设明文为：LOVE
- 则密文为：ORYH

单表代替密码——乘法密码

$y = kx(\bmod 26)$

明文：x

密文：y

密钥：k

解密：$x = k^{-1}y(\bmod 26)$

条件：$(k, 26) = 1$

关键在于计算 k^{-1}：

方法：扩展的欧几里得算法

若 $(m, n) = 1$，则存在整数 k_1, k_2 使得 $k_1 m + k_2 n = 1$

这里 k_1 就是 $m^{-1} \bmod n$，

注意要将 k_1 变为正数

$$-k_1 \bmod n = (n - k_1) \bmod n$$

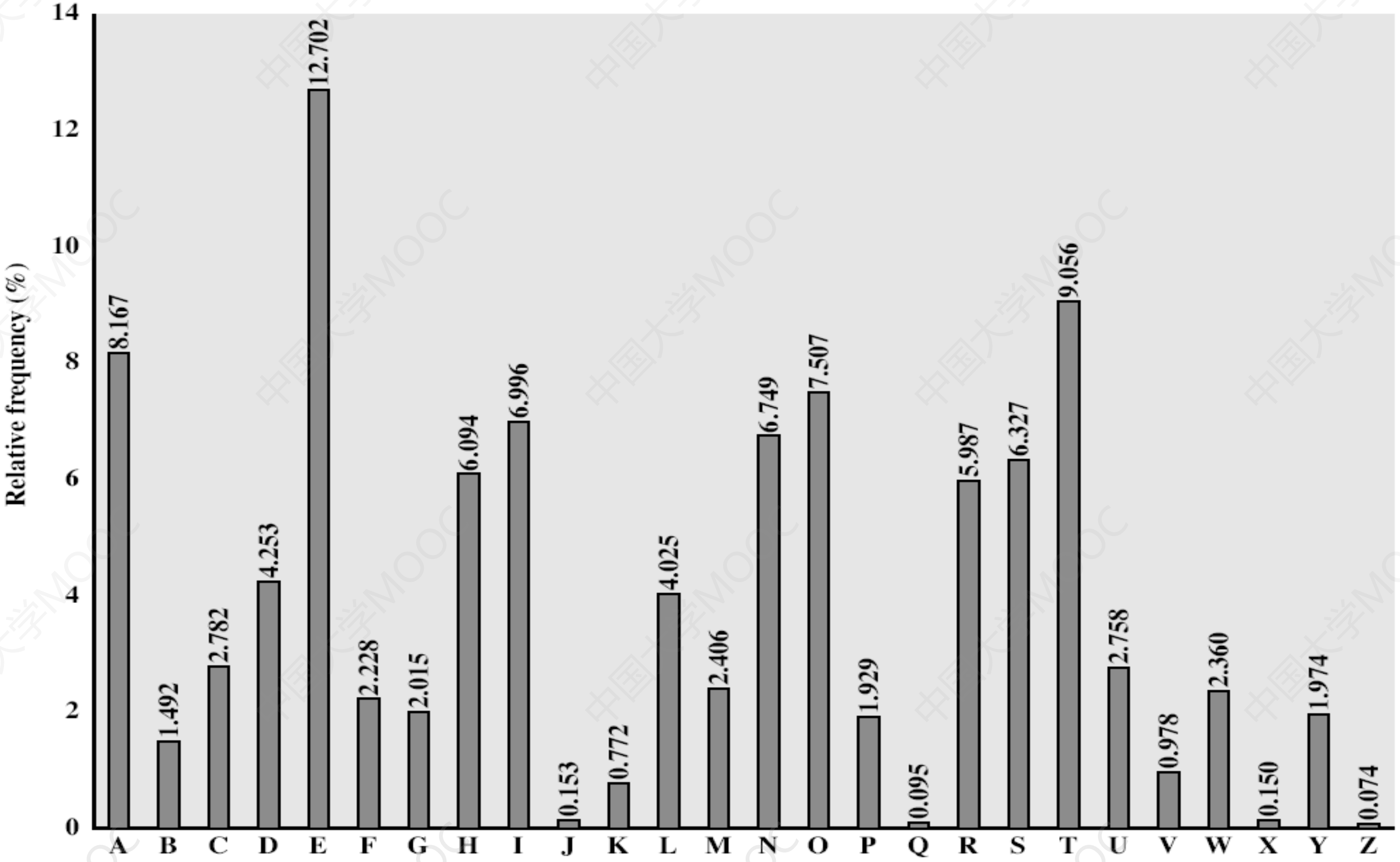
单表代替密码——仿射密码

- 加密函数： $y = ax + b \pmod{26}$
- 密钥：a, b
- 解密函数:$x = a^{-1}(y - b) \pmod{26}$
- 条件：$(a, 26) = 1$

仿射密码是乘法密码和加法密码的结合。

单表替代的统计分析

单表替代的特点是相同的明文被加密成相同的密文，这使得统计分析成为可能。



英文中字母出现频率是有规律的，只要能够收集到足够多的密文，通过统计就能够很容易地进行密码的破译：

e：出现频率约为0.127；

t，a，o，i，n，s，h，r：出现频率约在0.06到0.09之间

d，l：的出现频率约为0.04

c，u，m，w，f，g，y，p，b ：出现频率约在0.015到0.028之间

第六讲 古典密码算法

- 置换密码
- 单表代替密码算法
- 多表代替密码算法

Vigenere（维吉尼亚）密码

布莱斯·德·维吉尼亚（法语：Blaise De Vigenère，1523年8月5日－1596年），法国外交官、密码学家。

明文字母 →

替代方式 ↓

	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

Vigenere（维吉尼亚）密码。

我们先回忆前面讲过的凯撒密码，每个字母往后移动3位，相当于只有一种替换方式，而维吉尼亚怎么做的呢？也需要先选择一个词组或单词比如：hold。

P	t	h	i	s	i	s	t	h	e	p	l	a	i	n	t	e	x	t	明文
K																			
C																			密文

表 2.4 Vigenere 方阵

	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
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
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
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
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

多表代换密码

多表代换密码首先将明文M分为由n个字母构成的分组$M_1, M_2, \cdots, M_j$，对每个分组M_i的加密为：

$$C_i \equiv AM_i + B(\bmod N), i = 1, 2, \cdots, j$$

其中(A, B)是密钥，A 是$n \times n$的可逆矩阵，满足 $gcd(|A|, N) = 1$（$|A|$是行列式），$B = (B_1, B_2, \cdots, B_n)^T$，$C = (C_1, C_2, \cdots, C_n)^T$，$M_i = (m_1, m_2, \cdots, m_n)^T$

对密文分组C_i的解密为：

$$M_i \equiv A^{-1}(C_i - B)(\bmod N), i = 1, 2, \cdots, j$$

例题

设 $n=3, N=26$，

$$A=\begin{pmatrix}11 & 2 & 19\\ 5 & 23 & 25\\ 20 & 7 & 17\end{pmatrix}, \qquad B=\begin{pmatrix}0\\0\\0\end{pmatrix}$$

明文为“**YOUR PIN NO IS FOUR ONE TWO SIX**”。

将明文分成3个字母组成的分组“**YOU RPI NNO ISF OUR ONE TWO SIX**”，由表1-2得

$$M_1=\begin{pmatrix}24\\14\\20\end{pmatrix}, M_2=\begin{pmatrix}17\\15\\8\end{pmatrix}, M_3=\begin{pmatrix}13\\13\\14\end{pmatrix}, M_4=\begin{pmatrix}8\\18\\5\end{pmatrix},$$

$$M_5=\begin{pmatrix}14\\20\\17\end{pmatrix}, M_6=\begin{pmatrix}14\\13\\4\end{pmatrix}, M_7=\begin{pmatrix}19\\22\\14\end{pmatrix}, M_8=\begin{pmatrix}18\\8\\23\end{pmatrix}.$$

例题（续）

所以

$$C_1=A\begin{pmatrix}24\\14\\20\end{pmatrix}\pmod{26}=\begin{pmatrix}22\\6\\8\end{pmatrix},C_2=A\begin{pmatrix}17\\15\\8\end{pmatrix}\pmod{26}=\begin{pmatrix}5\\6\\9\end{pmatrix},C_3=A\begin{pmatrix}13\\13\\14\end{pmatrix}\pmod{26}=\begin{pmatrix}19\\12\\17\end{pmatrix},$$

$$C_4=A\begin{pmatrix}8\\18\\5\end{pmatrix}\pmod{26}=\begin{pmatrix}11\\7\\7\end{pmatrix},C_5=A\begin{pmatrix}14\\20\\17\end{pmatrix}\pmod{26}=\begin{pmatrix}23\\19\\7\end{pmatrix},C_6=A\begin{pmatrix}14\\13\\4\end{pmatrix}\pmod{26}=\begin{pmatrix}22\\1\\23\end{pmatrix},$$

$$C_7=A\begin{pmatrix}19\\22\\14\end{pmatrix}\pmod{26}=\begin{pmatrix}25\\15\\18\end{pmatrix},C_8=A\begin{pmatrix}18\\8\\23\end{pmatrix}\pmod{26}=\begin{pmatrix}1\\17\\1\end{pmatrix}.$$

密文为“**WGI FGJ TMR LHH XTH WBX ZPS BRB**”。

例题（续）

解密时，先求出

$$A^{-1}=\begin{pmatrix}11 & 2 & 19\\ 5 & 23 & 25\\ 20 & 7 & 17\end{pmatrix}^{-1}(\mathrm{mod}26)=\begin{pmatrix}10 & 23 & 7\\ 15 & 9 & 22\\ 5 & 9 & 21\end{pmatrix}$$

再求

$$M_1=A^{-1}\begin{pmatrix}22\\ 6\\ 8\end{pmatrix}=\begin{pmatrix}24\\ 14\\ 20\end{pmatrix},M_2=A^{-1}\begin{pmatrix}5\\ 6\\ 9\end{pmatrix}=\begin{pmatrix}17\\ 15\\ 8\end{pmatrix},$$

$$M_3=A^{-1}\begin{pmatrix}19\\ 12\\ 17\end{pmatrix}=\begin{pmatrix}13\\ 13\\ 14\end{pmatrix},M_4=A^{-1}\begin{pmatrix}11\\ 7\\ 7\end{pmatrix}=\begin{pmatrix}8\\ 18\\ 5\end{pmatrix},$$

$$M_5=A^{-1}\begin{pmatrix}23\\ 19\\ 7\end{pmatrix}=\begin{pmatrix}14\\ 20\\ 17\end{pmatrix},M_6=A^{-1}\begin{pmatrix}22\\ 1\\ 23\end{pmatrix}=\begin{pmatrix}14\\ 13\\ 4\end{pmatrix},$$

例题（续）

$$M_7 = A^{-1}\begin{pmatrix}25\\15\\18\end{pmatrix} = \begin{pmatrix}19\\22\\14\end{pmatrix}, M_8 = A^{-1}\begin{pmatrix}1\\17\\1\end{pmatrix} = \begin{pmatrix}18\\8\\23\end{pmatrix}.$$

得明文为“**YOU RPI NNO ISF OUR ONE TWO SIX**”。

求mod26下的逆矩阵

$$A = \begin{pmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 17 \end{pmatrix}$$

$$|A|(mod26) = -4869(mod26) \equiv 19$$

因为19和26互素，所以矩阵A可逆

$$|A|^{-1}(mod26) \equiv 19^{-1}(mod26) \equiv 11$$

伴随矩阵

$$A^* = \begin{pmatrix} A_{11} & A_{21} & A_{31} \\ A_{12} & A_{22} & A_{32} \\ A_{13} & A_{23} & A_{33} \end{pmatrix}(mod26) = \begin{pmatrix} 216 & 99 & -387 \\ 415 & -193 & -180 \\ -425 & -37 & 243 \end{pmatrix}(mod26) = \begin{pmatrix} 8 & 21 & 3 \\ 25 & 15 & 2 \\ 17 & 15 & 9 \end{pmatrix}$$

逆矩阵

$$A^{-1} = |A|^{-1}A^* = 11 \times \begin{pmatrix} 8 & 21 & 3 \\ 25 & 15 & 2 \\ 17 & 15 & 9 \end{pmatrix}(mod26) = \begin{pmatrix} 10 & 23 & 7 \\ 15 & 9 & 22 \\ 5 & 9 & 21 \end{pmatrix}$$

感 谢 聆 听！

xynie@uestc.edu.cn