



## 《现代密码学》第二讲

# 古典密码学





## 《现代密码学》第二讲

# 古典密码体制

# 上讲内容回顾



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

● 密码学分类

● 密码学与信息安全的关系



信息安全中心



# 本章主要内容

- 代换密码
- 置换密码
- Hill 密码
- 转轮密码
- 古典密码的惟密文攻击方法



# 密码分类

● **代换密码 ( substitution )** : 代换是古典密码中用到的最基本的处理技巧。所谓代换,就是将明文中的一个字母由其它字母、数字或符号替代的一种方法。

- 凯撒密码
- 仿射密码
- 单表代换
- 多表代换

● **置换密码 ( permutation )** : 将明文字符按照某种规律重新排列而形成密文的过程。

● **Hill 密码**

● **转轮密码**





# 注意事项

本讲中，被加密的文本均假设为 26 个英文字符，在算法描述中，也常常用数字表示每个字母，对照表如下：

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25



# 本章主要内容

- 代换密码
- 置换密码
- Hill 密码
- 转轮密码
- 古典密码的惟密文攻击方法



# 凯撒密码

已知最早的代换密码，又称移位密码

- 代换表（密钥）：

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
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

- 数学描述：

$$c = E(p) = (p + k) \bmod (26)$$

$$p = D(c) = (c - k) \bmod (26)$$

明文  $p \in \mathbb{Z}_{26}$ ，密文  $c \in \mathbb{Z}_{26}$ ，密钥  $k$  取  $[1, 25]$   
，只  
有 25 个





# 凯撒密码



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

例：使用其后的第三个字母代换该字母

明文：meet me after the toga  
party

密文：PHHW PH DIWHU WKH WRJD  
SDUWB



信息安全中心



# 仿射密码

## ● 移位密码的扩展

明文  $p \in Z_{26}$  , 密文  $c \in Z_{26}$  ,

密钥  $k=(a, b) \in Z'_{26} \times Z_{26}$  且  $\gcd(a, 26)=1$ .

加密:

$$c = E(p) = (a \times p + b) \bmod 26$$

解密:

$$p = D(c) = (c - b) \times a^{-1} \bmod 26$$



# 仿射密码

例：令密钥  $k=(7, 3)$ ，且  $\gcd(7, 26)=1$ 。

明文  $hot=(7, 14, 19)$

加密：

$$(7 \times 7 + 3) \bmod 26 = 0$$

$$(7 \times 14 + 3) \bmod 26 = 23$$

$$(7 \times 19 + 3) \bmod 26 = 6$$

密文为  $(0, 23, 6) = (a, x, g)$

解密：  $7^{-1}=15=-11 \bmod 26$

$$(0 - 3) \times 15 \bmod 26 = 7$$

$$(23 - 3) \times 15 \bmod 26 = 14$$

$$(6 - 3) \times 15 \bmod 26 = 19$$

明文为  $(7, 14, 19) = (h, o, t)$





# 仿射密码

练习：令密钥  $k=(9, 3)$ ，且  $\gcd(9, 26)=1$ 。

明文  $hot=(7, 14, 19)$ ，求加解密过程。

加密：

$$7 * 9 + 3 = 14 \text{ mod } 26$$

$$14 * 9 + 3 = 25 \text{ mod } 26$$

$$19 * 9 + 3 = 18 \text{ mod } 26$$

$$9 * 3 - 26 = 1 \text{ 所以 } 9^{-1} = 3 \text{ mod } 26$$

解密：

$$(14 - 3) * 3 = 7 \text{ mod } 26$$

$$(25 - 3) * 3 = 14 \text{ mod } 26$$

$$(18 - 3) * 3 = 19 \text{ mod } 26$$



# 单表代换密码

代换表是 26 个字母的任意置换

例：

加密函数：

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

解密函数：

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
s	g	m	a	k	e	x	o	f	h	b	v	q	z	u	j	d	w	l	p	t	c	i	n	r	y

明文：if we wish to replace letters

密文：WI RF RWAJ UH YFTSDVF SFUUFYA





# 单表代换密码

## 练习：

•明文：nice work，使用上例中的单表代换表，求密文。

•密文： X W V F          R H Y E



# 多表代换密码

加密明文消息时采用不同的单表代换，由密钥具体决定采用哪个表代换消息，密钥通常是一个词的重复。

- 简化多表代换密码 - 维吉尼亚密码  
( **Vigenère Cipher** ) : 由 26 个类似 caesar 密码的代换表组成



# 多表代换密码

● **维吉尼亚密码**：在长为  $m$  的密码中，任何一个字母可被影射为 26 个字母中的一个

明文  $p \in (Z_{26})^m$ ，密文  $c \in (Z_{26})^m$ ，密钥  $k \in (Z_{26})^m$

**加密**

$$c = (p_1 + k_1, p_2 + k_2, \dots, p_m + k_m) \bmod 26;$$

**解密**

$$p = (c_1 - k_1, c_2 - k_2, \dots, c_m - k_m) \bmod 26.$$





# 多表代换密码

例：

	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

Key:

GOOGLE

Plaintext:

BUY YOUTUBE

Ciphertext:

HIMEZYZIPK





# 多表代换密码

练习：

•明文：nice work，密钥：hot，求密文。

•密文：U W V L K H Y Y



# 本章主要内容

- 代换密码
- 置换密码
- Hill 密码
- 转轮密码
- 古典密码的惟密文攻击方法



# 置换密码

加密变换使得信息元素只有位置变化而形态不变，如此可以打破消息中的某些固定模式（结构）

明文  $p \in (Z_{26})^m$ ，密文  $c \in (Z_{26})^m$ ，

密钥  $k \in \{\pi \mid \text{定义在 } 1, 2, \dots, m \text{ 上的置换}\}$

**加密**

$$c = (p_{\pi(1)}, p_{\pi(2)}, \dots, p_{\pi(m)}) \bmod 26;$$

**解密**

$$p = (c_{\pi^{-1}(1)}, c_{\pi^{-1}(2)}, \dots, c_{\pi^{-1}(m)}) \bmod 26.$$



# 置换密码



例：密钥

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

明文： she sells sea shells by the sea shore

分组： shesel lsseas hellsb ythese ashore

置换： EESLSH SALSES LSHBLE HSYEET HRAEOS





# 置换密码

练习：

明文：nice work

X	1	2	3	4
Pi(x)	2	4	1	3

求密文和逆置换。

密文： ienc okwr

X	1	2	3	4
Pi <sup>-1</sup> (x)	3	1	4	2



# 本章主要内容

- 代换密码
- 置换密码
- **Hill 密码**
- 转轮密码
- 古典密码的惟密文攻击方法

# 希尔密码 (Hill cipher)



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

1929 年, Lester S. Hill 提出

明文  $p \in (\mathbb{Z}_{26})^m$ , 密文  $c \in (\mathbb{Z}_{26})^m$ ,

密钥  $K \in \{ \text{定义在 } \mathbb{Z}_{26} \text{ 上 } m \times m \text{ 的可逆矩阵} \}$

加密

$$c = p * K \bmod 26$$

解密

$$p = c * K^{-1} \bmod 26$$



信息安全中心





# 希尔密码

例：

密钥：

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

加密：

$$(9 \ 20) \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (99 + 60, 72 + 140) = (3, 4)$$

解密：

$$(3, 4) \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} = (9, 20)$$





# 希尔密码

置换密码可以看做是希尔密码的特例。

练习：

设 hill 密码的密钥如下，求对应置换密码

的置换表。


$$K_{\pi} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

X	1	2	3	4
Pi(x)	3	4	1	2





# 本章主要内容

- 代换密码
- 置换密码
- Hill 密码
-  转轮密码
- 古典密码的惟密文攻击方法

# 转轮密码 (Rotor Machine)



北京邮电大学  
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 19 世纪 20 年代，开始出现机械加解密设备，最典型的是转轮密码机
- 1918 年 Arthur Scherbius 发明的 EIGMA，瑞典 Haglin 发明的 Haglin，和日军发明的“紫密”和“兰密”都属于转轮密码机。



信息安全中心

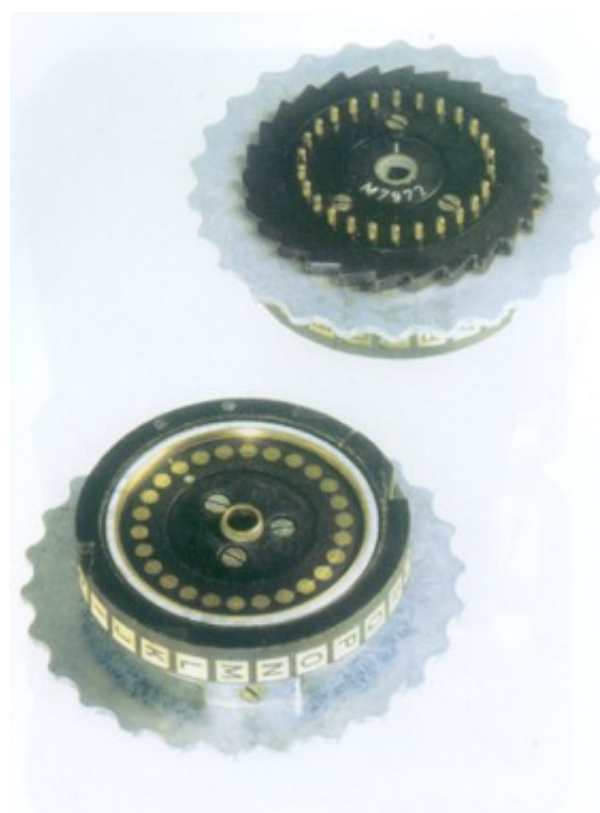
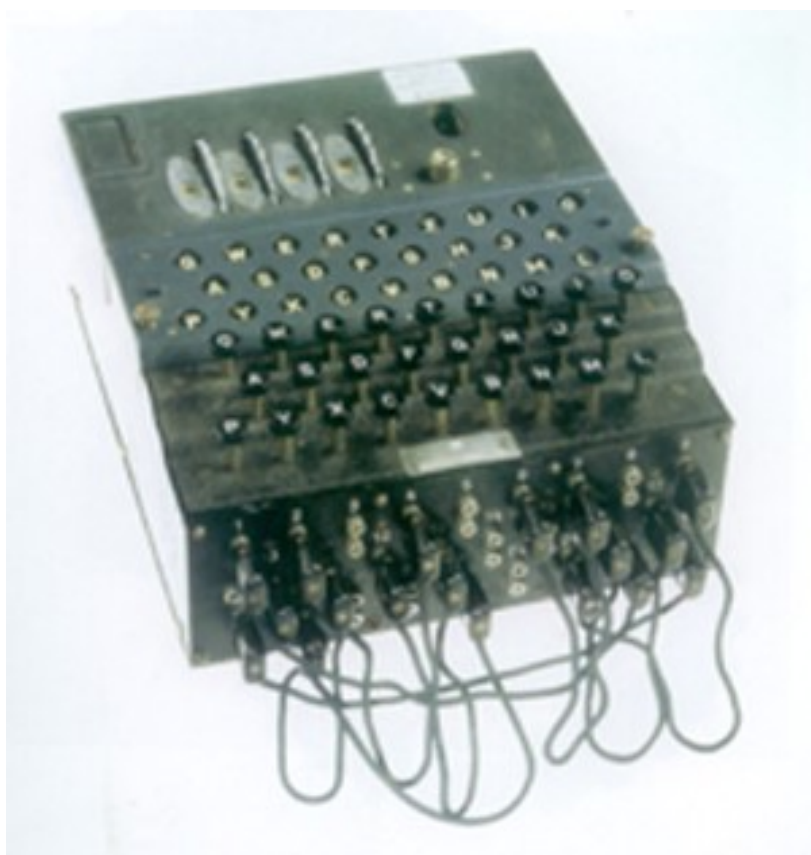
# 转轮密码



北京邮电大学

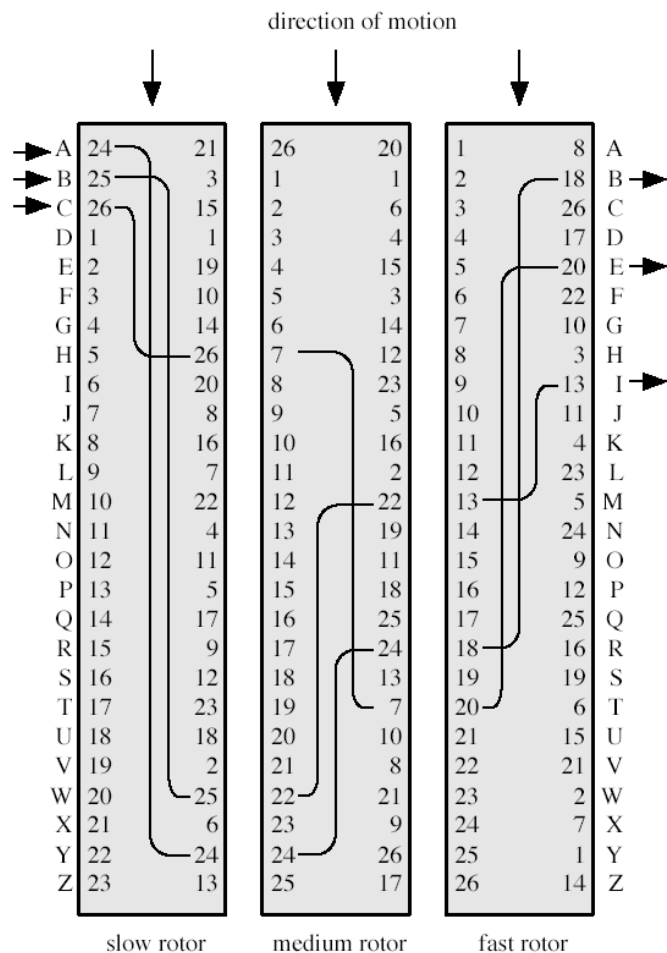
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

## Enigma 密码机

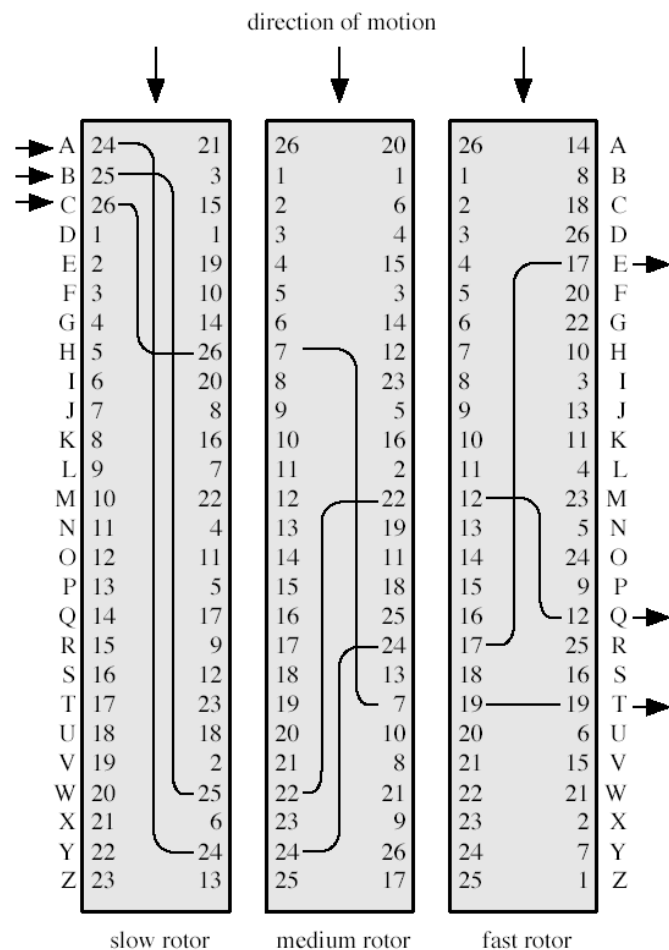


信息安全中心

# 转轮密码



(a) Initial setting



(b) Setting after one keystroke



# 转轮密码

- 转轮密码机的工作原理是：当按下某一键时，电信号从慢轮子的输入引脚进入，经过内部连线流经每个转轮，最后从快轮子的输出引脚输出密文。如果按下字母键 A，则一个电信号被加到慢轮子的输入引脚 24 并通过内部连线连接到慢轮子的输出引脚 24，经过中轮子的输入引脚 24 和输出引脚 24，连接到快轮子的输入引脚 18，最后从快轮子的输出引脚 18 输出密文字母 B。
- 快轮子转动一个位置，即快轮子的所有引脚向下移动一个位置，原最下边的引脚移至顶端，显然，此时若再按个 A 键，则一个电信号被加到慢轮子的输入引脚 24 并通过内部连线连接到慢轮子的输出引脚 24，经过中轮子的输入引脚 24 和输出引脚 24，连接到快轮子的输出引脚 17，最后从快轮子的输出引脚 17 输出密文字母 E，显然，两次的输出结果是完全不同的，从而实现了多表代换密码。





# 转轮密码

- 图中共有三个转轮：慢轮子、中轮子和快轮子。其中快轮子转动一圈（26 个位置），中轮子转动一个位置；中轮子转动一圈（26 个位置），慢轮子转动一个位置。因此，在加密或解密个字母以后，所有转轮都恢复到初始状态。由此可知，一个有 3 个转轮的转轮密码机是一个密钥周期为  $26^3$  的多表代换密码机械装置。





# THE END !

