《密码学》

期末速成课


置换密码
列置换
周期置换
代换密码
单表代换密码
字母频率分析法
移位密码
基于密钥的单表代换密码
仿射密码
多表代换密码
重合指数法
playfair密码
维吉尼亚密码
希尔密码

考点	重要程度	占分	题型
1. 置换密码/代换密码概念	★★★	1 - 3	选择/填空
2. 列置换	★★★	0 - 3	大题
3. 移位密码	★★★★★	0 - 3	选择 填空
4. 仿射密码	★★★★	3 - 5	选择/大题
5. 维吉尼亚密码	★★★★	3 - 5	大题/选择

2.1 传统密码体制

一、置换密码

➢ 明文中的字母重新排列，只是位置改变

置换密码包括列置换和周期置换

- 列置换：
- (1,4,3)(5,6)
- 1->4 4->3 3->1 5->6 6->5
- 第一列放到第4列，第4列放到第3列，第3列放到第1列，第5列放到第6列，第6列放到第5列

扫码观看
视频讲解更清晰

一、置换密码

设明文P为“Beijing 2008 Olympic Games”

密匙σ=（1 4 3）（5 6）.则加密过程为：

$$[M]_{4\times6}=\begin{bmatrix} B & e & i & J & i & n \\ g & 2 & 0 & 0 & 8 & O \\ l & y & m & p & i & c \\ G & a & m & e & s & \end{bmatrix} \overset{\sigma}{\Rightarrow} [M_P]_{4\times6}=\begin{bmatrix} i & e & J & B & n & i \\ 0 & 2 & 0 & g & O & 8 \\ m & y & p & l & c & i \\ m & a & e & G & & s \end{bmatrix}$$

由矩阵$[M_p]_{4\times6}$得到密文G为“iomme2yaJ0peBglGnOc i8is”

根据加密密匙逆置换σ^{-1}=（1 3 4）（5 6），则解密过程如下

$$[M_P]_{4\times6}=\begin{bmatrix} i & e & J & B & n & i \\ 0 & 2 & 0 & g & O & 8 \\ m & y & p & l & c & i \\ m & a & e & G & & s \end{bmatrix} \overset{\sigma^{-1}}{\Rightarrow} [M]_{4\times6}=\begin{bmatrix} B & e & i & J & i & n \\ g & 2 & 0 & 0 & 8 & O \\ l & y & m & p & i & c \\ G & a & m & e & s & \end{bmatrix}$$

二、代换密码

1、单表代换密码

（1）移位密码

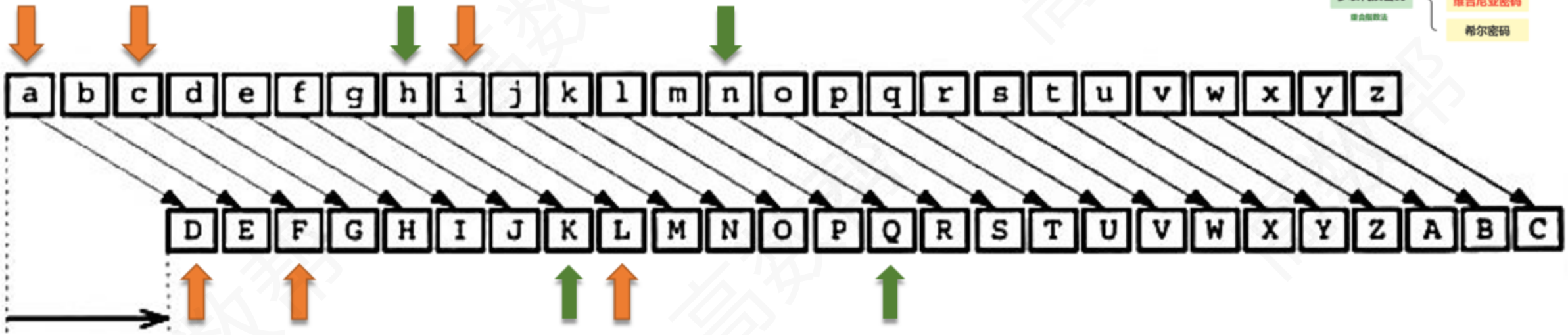
加密变换： $y = (x+a) \bmod 26 , x,y \in Z26$

解密变换： $x = (y-a) \bmod 26 , x,y \in Z26$

- 将明文中所使用的字母按照一定的字数进行“平移”移3位就是凯撒密码
- 凯撒密码是特殊的移位密码

扫码观看
视频讲解更清晰

二、代换密码



平移3个字母

- 凯撒密码　P=c h i n a　　K=3

  C=f k l q d

二、代换密码

(2) 基于密钥的单表代换密码

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

明文：nice work，使用上例中的代换表，求密文。

密文：X W V F R H Y E

二、代换密码

(3) 仿射密码

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

加密：$E(X) = (ax + b)(mod\ m)$

$E(X) = (ax + b)(mod\ 26)$

解密：$D(X) = a^{-1}(x - b)(mod\ m)$

$D(X) = a^{-1}(x - b)(mod\ 26)$

二、代换密码

运用到：乘法逆元和模运算

举例:以 $E(X) = (5x+8)(mod\ 26)$ **为例**

$E(X) = (ax+b)(mod\ 26)$

明文	A	F	F	I	N	E	C	I	P	H	E	R
x	0	5	5	8	13	4	2	8	15	7	4	17
y = 5x + 8	8	33	33	48	73	28	18	48	83	43	28	93
y mod 26	8	7	7	22	21	2	18	22	5	17	2	15
密文	I	H	H	W	V	C	S	W	F	R	C	P

----加密

二、代换密码

$$D(X) = a^{-1}(x-b)(mod\ 26)$$

明文	I	H	H	W	V	C	S	W	F	R	C	P
x	8	7	7	22	21	2	18	22	5	17	2	15
y=21(x-8)	0	-21	-21	294	273	-126	210	294	-63	189	-126	147
y mod 26	0	5	5	8	13	4	2	8	15	7	4	17
密文	A	F	F	I	N	E	C	I	P	H	E	R

----解密

二、代换密码

2、多表代换密码

（1）playfair密码

A. 编制密码表（5×5）

①密钥去掉重复字母和空格

②按照字母顺序按行排列

③按字母序填入不在密钥串中的字母

密匙：shiyanb 可编成

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

二、代换密码

B. 整理明文/密文

- 将明文/密文两个字母组成一对
  - 若对每一个明文对P1/P2
    - P1=P2，添加一个事先约定的字母，插入重复字母中（P1，X，P2）
    - 最后缺一个，添加一个事先约定的字母，放到末尾

密文：KQSAMFPAOPMFPA

KQ SA MF PA OP MF PA

二、代换密码

C. 加密规则

①在同一行，密文在右

②在同一列，密文在下

③不在同行同列，矩形对角

D. 解密规则

①在同一行，明文在左

②在同一列，明文在上

③不在同行同列，明文在对角

扫码观看
视频讲解更清晰

二、代换密码

【Eg】 明文：mimaxue 密钥：chonga

1. 编制密码表（5×5）

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

2. 整理明文 （约定+x）

mi	ma	xu	ex

扫码观看
视频讲解更清晰

二、代换密码

【Eg】 明文：mimaxue 密钥：chonga

3. 加密

mi	ma	xu	ex

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

mi

ij

【加密规则】

①在同一行，密文在右

②在同一列，密文在下

③不在同行同列，矩形对角

二、代换密码

【Eg】 明文：mimaxue 密钥：chonga

3. 加密

mi	ma	xu	ex

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

ma

fi

【加密规则】

①在同一行，密文在右

②在同一列，密文在下

③不在同行同列，矩形对角

二、代换密码

【Eg】 明文：mimaxue 密钥：chonga

3. 加密

mi	ma	xu	ex

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

xu

yv

【加密规则】

①在同一行，密文在右

②在同一列，密文在下

③不在同行同列，矩形对角

二、代换密码

【Eg】 明文：mimaxue 密钥：chonga

3. 加密

mi	ma	xu	ex

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

ex

ln

【加密规则】

①在同一行，密文在右

②在同一列，密文在下

③不在同行同列，矩形对角

二、代换密码

【Eg】 明文：mimaxue 密钥：chonga

mi	ma	xu	ex

mi	ma	xu	ex
ij	fi	yv	ln

ij	fi	yv	ln

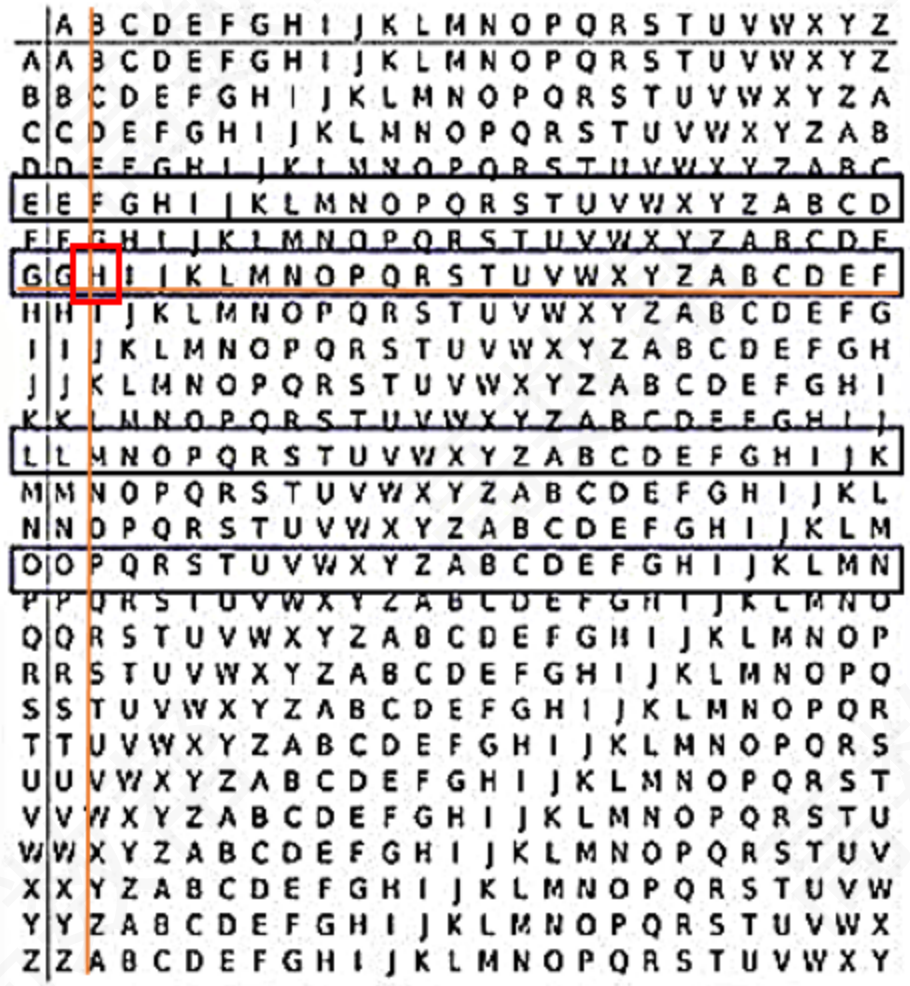
扫码观看
视频讲解更清晰

二、代换密码

（2）维吉尼亚密码

密钥中的字母为行

明文中的字母为列



Key:
GOOGLE
Plaintext:
BUYYOUTUBE
Ciphertext:
HIMEZYZIPK

二、代换密码

（3）希尔密码

希尔密码是利用矩阵进行加密的一种加密算法，其本质是一种多表代换密码

密钥：

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

加密：

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

解密：

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

单表代换——字母频率分析法

多表代换——重合指数法