# 矩阵换位

## Rectangular Transposition 刘卓

## 1 普费尔密码

普费尔密码 (Playfair Cipher) 由查尔斯·惠斯通 (Charles Wheatstone) 发明,里昂·普费尔 (Lyon Playfair) 推广,由此得名普莱费尔密码。在第二次布尔战争和第一次世界大战中被英军广泛使用,之后的第二次世界大战中澳大利亚人也使用它。

#### 加密步骤

### 1.1 确定密钥

#### 例 1

假设普费尔密码矩阵使用密钥(Keyword): DIVERGENT

将密钥放置在一个  $5\times 5$  矩阵中,如果遇到相同字母,则跳过。比如 DIVERGENT,填充时第二个字母E跳过忽略。通常字母I和字母J放在一个框框内。剩下的空则按拉丁字母表挨个填充,遇到已有字母则跳过。

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

## 1.2 将要加密的讯息分成两个一组

- 使用字母 X 插入进重复的字母
- 如果字符串长度是奇数,则在字符串末尾加一个字母 Q

#### 例 2

明文 PLAN, 则划分为 PL||AN 明文 CHEEG, 则划分为 CH||EX||EG 明文 ACT, 则划分为 AC||TQ

#### 1.3 加密

- 若两个字母在同一列, 取这两个字母右方的字母(若字母在最右方则取最左方的字母)。
- 若两个字母在同一行,取这两个字母下方的字母(若字母在最下方则取最上方的字母)。
- 若两个字母不在同一直行或同一横列,在矩阵中找出另外两个字母,使这四个字母成为一个长方形的四个角,取对应行的字母。

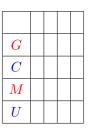
#### 例 3

根据例 1 表格:

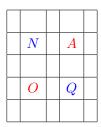
规则 1 中,如字符 GT 则加密为 NA;如字符 TG 则加密为 AN;如字符 NB 则加密为 TG(因为 B 在最右,则取最左边的字母 G);

	G	N	T	A	
ĺ					

规则 2 中,如字符 MG 则加密为 UC;如字符 DC 则加密为 GM;如字符 GU 则加密为 CD(因为 U 在最下,则取最上边的字母 D);



规则 3 中,如字符 AO 则加密为 NQ;如字符 OA 则加密为 QN;如字符 NZ 则加密为 BW;



一共拥有 25! 的密钥可能性。

## 2 ADFGVX 密码

ADFGVX 密码是由德国上校弗里茨·内贝尔 (Fritz Nebel) 发明。ADFGVX 密码和 Playfair 密码相似,也是矩阵换位密码一种。

### 2.1 加密步骤

- 1. 确定一个密钥,构建一个 6×6 ADFGVX 矩阵,输入 26 个拉丁字母和 10 个数字;
- 2. 将明文中的每个字母转换为其在 ADFGVX 中的坐标表。坐标的顺序为(行索引、列索引);
- 3. 将转换后的文本(从左到右逐行)重新排列为一种含有 n 列的表,并使用长度为 n 的选定排列对这些列进行排列;
- 4. 从上到下逐列读取已排列的表以获得密文;

密钥空间 = 36!

**例 4** 如密钥是 SUMMER, 则 ADFGVX 矩阵是:

	A	D	F	G	V	X
A	S	U	M	E	R	A
D	В	С	D	F	G	Н
F	I	J	K	L	N	О
G	Р	Q	Т	V	W	X
V	Y	Z	0	1	2	3
X	4	5	6	7	8	9

例 5

使用列表 8 4 3 2 7 6 1 5 和如下表格加密"from one day to another in battle"

	A	D	F	G	V	X
A	i	w	О	u	1	d
D	e	f	r	у	0	a
F	9	b	c	1	g	h
G	j	k	2	m	n	7
V	p	3	q	s	6	t
X	4	v	X	5	z	8

#### 解:

将明文中的每个字母转换为其在 ADFGVX 中的坐标表

f	r	О	m	О	n	e	d	a	у
DD	DF	AF	GG	AF	GV	DA	AX	DX	DG
t	О	a	n	О	t	h	e	r	
VX	AF	DX	GV	AF	VX	FX	DA	DF	
i	n	b	a	t	t	1	е		
AA	GV	FD	DX	VX	VX	AV	DA		

然后逐行填入列表84327615所形成的矩阵中。

8	4	3	2	7	6	1	5
D	D	D	F	A	F	G	G
A	F	G	V	D	A	A	X
D	X	D	E	V	X	A	F
D	X	G	V	A	F	V	X
F	X	D	A	D	F	A	A
G	V	F	D	D	X	V	X
B	X	A	V	D	A	X	F

填充过程中,最后两个没有足够的明文让其填上。可以规定字母 X 作为填充物,X 在 ADFGVX 矩阵中的坐标是 XF,因此最后填充物为 XF

然后按照列表顺序从上到下以此读取密文。

8	4	3	2	7	6	1	5
D	D	D	F	A	F	G	G
A	F	G	V	D	A	A	X
D	X	D	E	V	X	A	F
D	X	G	V	A	F	V	X
F	X	D	A	D	F	A	A
G	V	F	F	D	X	V	X
B	X	A	V	D	A	X	F

## 2.2 解密步骤

与加密步骤反之。

- 1. 将密文的字母填入一个由 n 个长度组成的列表中, 一列一列填写条目, 从上到下, 从左到右。
- 2. 按照规定列表重新排列。
- 3. 从左到右,从上到下,逐行读取。然后将结果文本分成每两个字母一组。
- 4. 使用 ADFGVX 表格中的坐标将每对转换为明文, 坐标的顺序为(行索引、列索引)。