PART 2

传统加密技术

2.2 代换技术

2.2 代换技术

◆**密码学的发展：**

- **1949年之前- 古典密码学**
- **49～75年- 现代常规密码**
- **76年之后- 公钥密码学**

◆**加密算法的两个基本原理：**

代换和置换

Substitution代换（代替）：将明文中的每个元素映射成另一个元素。

Permutation置换： 将明文中的元素重新排列，明文中的字母保持不变。

代替：换对应字符集； 置换：改变位置。

2.2 代换技术

2.2.1 Caesar密码

- 有记载表明，在古罗马就已经使用采用代换技术的对称密码。据说有一位名叫Julius Caesar的国王在作战时曾使用过一种密码技术（如今把这种密码技术称为“凯撒密码”技术）。

2.2 代换技术

2.2.1 Caesar密码

该密码技术的思路是这样的：将26个英文字母a，b，c，…依次排列，z后面再接排a，b，c，…**取移位间隔为3**，将每个字母（明字符）由与它间隔为3的字母来替代（密字符），由此构成了一张明字符和密字符的对照表，称为密码表,如下所示：

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

由密码表，取明文块**M= network**，相应的密文块**C=QHWZRUN**。

2.2 代换技术

2.2.1 Caesar密码

- 如果把字母表编码为0-25的数字(p_{27})，加密算法可以如下表达，对于每个明文字母p，代换成密文字母C：$C = E(3, p) = (p + 3) \bmod 26$
- 注意到k(移位间隔)的取值可以在1至25之间变化，所以总共可以得到25个不同的密码表。以上介绍的是k=3的一种情况。如果**取k=5**，那么明文**M=network**加密后就变为密文**C=SJYBTWP**。

2.2 代换技术

2.2.1 Caesar密码

- 一般化的恺撒加密算法为： **C = E(k, p) = (p + k) mod 26**
- 一般化的恺撒解密算法为： **p = D(k, C) = (C - k) mod 26**

2.2 代换技术

2.2.1 Caesar密码

可见，同样的明文，如果k的取值不同，那么就会得到不同的密文。

这个k就是这种密码技术的密钥。因为k的取值最多只有25种，所以这种密码技术在计算技术如此发达的今天已经不再安全。但从这种技术中我们可以了解它的加密思想，从而可以古为今用。

2.2 代换技术

2.2.1 Caesar密码

Caesar密码的三个重要特征使我们可以采用穷举攻击分析方法：

1. **已知加密和解密算法。**
2. **需测试的密钥只有25个。**
3. **明文所用的语言是已知的，且其意义易于识别。**

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

2.2 代换技术

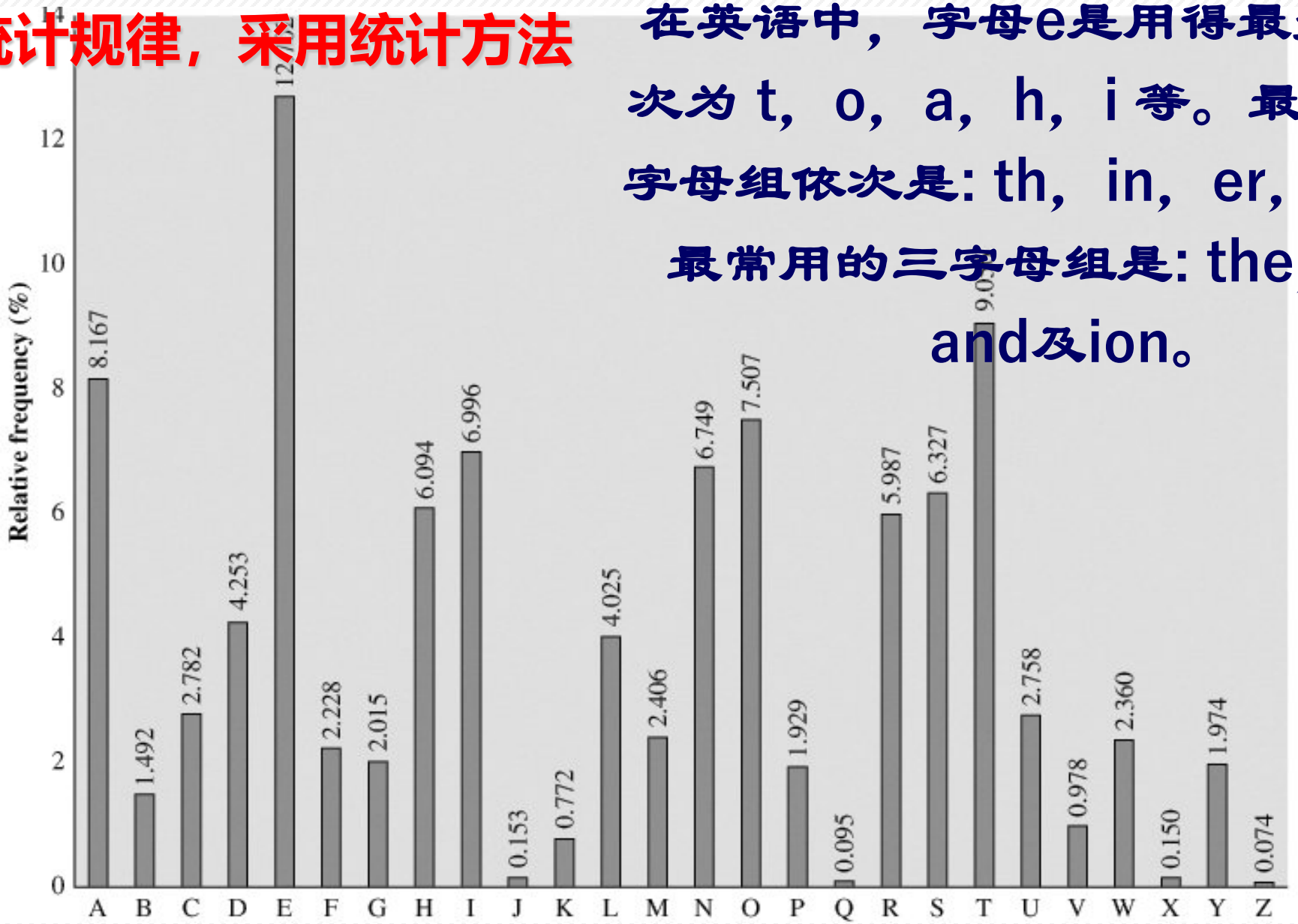
2.2.2 单表代换密码

- **Caesar密码仅有25种可能的密钥**，是远不够安全的。通过允许26个字母任意代换，密钥空间将会急剧增大。
- **如果密文行是26个字母的任意置换**，那么就有**26!**种可能的密钥，这比DES的密钥空间要大10个数量级，应该可以抵挡穷举攻击了。这种方法称为单表代换密码。
- 对于这种加密方法，如何进行攻击呢?

2.2 代换技术

根据语言的统计规律，采用统计方法

在英语中，字母e是用得最多的，其次为t，o，a，h，i等。最常用的两字母组依次是：th，in，er，re及an。最常用的三字母组是：the，ing，and及ion。



2.2 代换技术

2.2.2 单表代换密码

◆先得有足够多的密文

- 几十个字母以上
- 明文得有明确的意义(古典算法时通常是这样的)

◆统计密文中各个字母的出现概率

◆结合明文的统计

- 猜测出现得最多密文字母对应明文字母 e (或 t、a)，最少的是 z (或 j)
- 猜测出现得最多密文字母双组是th
- 观察所谓的明文，并重试

2.2 代换技术

2.2.2 单表代换密码

- **单表代换密码容易被攻击**，因为单字母替代不会改变字母的频率，所以**原始文字的统计特征几乎被完整保留下来**。
- 有两种主要方法可以减少代换密码里明文结构在密文中的残留度：一种是**对明文中的多个字母一起加密**；另外一种是采用**多表代换**。

2.2 代换技术

2.2.3 Playfair

- 采用多字母一起加密最著名的密码体制是Playfair密码，将明文中的双字母组合作为一个单元对待，并将这些单元转换为密文的双字母组合。例如使用的**密钥词是monarchy**，建立右边所示矩阵：

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

- 其矩阵的构造如下：首先，**从左到右、从上到下填入该密钥的字母，重复的字母只保留一个，其余去除;其次，按照字母表顺序将其余字母填入矩阵的剩余空间。**字母I和J被算作一个字母，可以根据使用者的意愿在形成密文时确定用I或J。

2.2 代换技术

2.2.3 Playfair密码

Playfair算法根据下列规则**每次对明文的两个字母进行加密**，这两个字母构成一对：ba lx lo on

(1) **一对明文字母如果是重复的则在这对明文字母之间插入一个填充字符**，如x。例如**balloon先把它变成ba lx lo on 这样四个字母对。**

(2)如果分割后的明文字母对在矩阵的**同一行中都出现(不需要相邻)**，那么**分别用矩阵中其右侧的字母代替**，行的最后一个字母由行的第一个字母代替。例如，**ar加密为RM，ek加密为FE。**

2.2 代换技术

2.2.3 Playfair密码

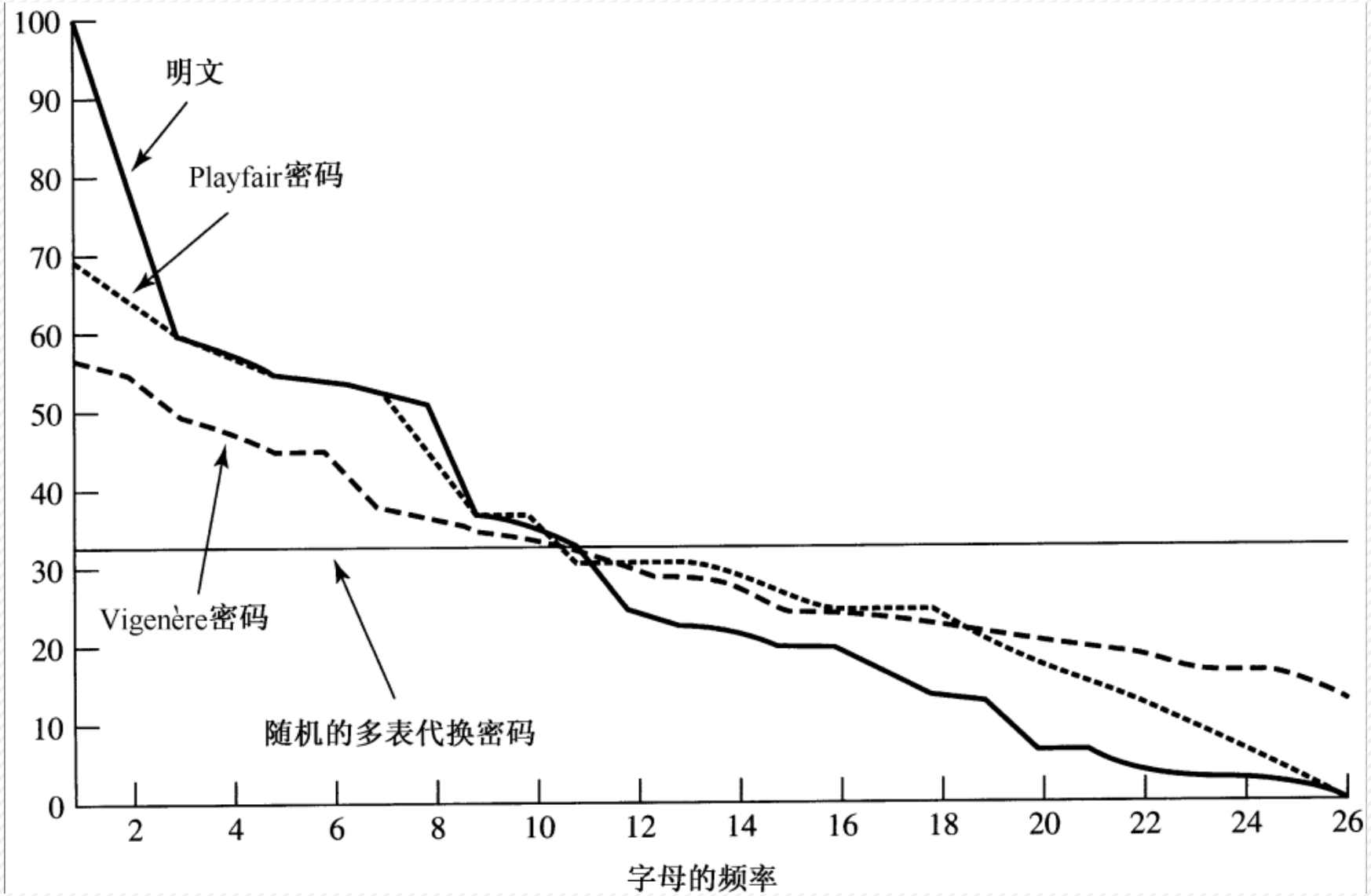
(3) 如果分割后的**明文字母对在矩阵的同一列中都出现**，则**分别用矩阵中其下方的字母代替，列的最后一个字母由列的第一个字母代替。** 如**mu加密为CM**

(4) 否则，**明文对中的每一个字母将由与其同行，且与另一个字母同列的字母代替。**例如**hs加密为BP，ea加密为IM（或JM）**

2.2 代换技术

2.2.3 Playfair密码

◆Playfair密码与单字母替代密码相比有明显的优势：其一，双字母有**26*26=676种组合方式，识别各种双字母组合比单字母困难得多**;其二，各种字母组的相对频率范围也更为广泛，使**频率分析更加困难**。因此，Playfair曾被认为是不可破译的，英国陆军在第一次世界大战中采用了它，二战中它仍被美国陆军和其他同盟国大量使用。


100
90
80
70
60
50
40
30
20
10
0
明文
Playfair密码
Vigenère密码
随机的多表代换密码
2
4
6
8
10
12
14
16
18
20
22
24
26
字母的频率

2.2 代换技术

2.2.4 多表代换加密(维吉尼亚密码)

- 改进简单的单表代换的另外一种方法是**在明文消息中采用不同的单表代换**。这种方法一般称之为多表代换密码，此类算法中最著名且最简单的是**Vigenère(维吉尼亚密)密码**。其相当于凯撒加密的进一步推广，明文的每个字母使用不同k的凯撒加密。
- 我们可以构造一个维吉尼亚密码表的矩阵，最左边为密钥字母，最上面为明文，加密过程很简单：给定密钥字母x和明文字母y，密文字母为位于x行和y列的字母。

Table 2.3 The Modern Vigenère Tableau

Key	Plaintext 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

2.2 代换技术

2.2.4 多表代换加密(维吉尼亚密码)

◆例如取密钥为: **deceptive**

密钥: deceptivedeceptivedeceptive

明文: **wearediscoveredsaveyourself**

密文: **ZICVTWQNGRZGVTWAVZHCQYGLMGJ**

(注：1917年的《科学美国人》杂志曾错误的判断维吉尼亚密码是不可破解的)

2.2 代换技术

2.2.5 一次一密

- 陆军情报军官Joseph Mauborgne建议使用与消息一样长且无重复的随机密钥来加密消息，另外，**密钥只对一个消息进行加解密，之后丢弃不用。每一条新消息都需要一个与其等长的新密钥。**
- 这就是著名的一次一密，**在理论上它是不可攻破的。**它**产生的随机输出与明文没有任何统计关系。**因为密文不包含明文的任何信息，所以无法可破。

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

◆假设我们将明文good和密钥zsej做模26的加法得到密文：

good 明文

zsej 密钥

fgsm 密文

也许会想到，穷举所有可能的密钥，如果试解的密钥是**useb**则得到**look**，如果试解的密钥是**quzh**则得到**part**，事实上所有四个字符的组合都可能出现，当然good也在其中，可是你没有办法确定哪一组解是正解，这样的破解和随意乱猜四个字母可能的单词组合没什么分别。

2.2 代换技术

2.2.5 一次一密

- 因为给出任何长度与密文一样的明文，都存在着一个密钥产生这个明文。因此，如果你用穷举法搜索所有可能的密钥，就会得到大量可读、清楚的明文，但是没有办法确定哪一个才是真正所需的，因而这种密码是不可破的。
- 在实际中，一次一密提供完全的安全性存在**两个基本难点**：

1. **产生大规模随机密钥有实际困难**。任何经常使用的系统都需要建立在某个规则基础上的数百万个随机字符，提供这样规模的真正随机字符是相当艰巨的任务。
2. **更令人担忧的是密钥的分配和保护**。对每一条发送的消息，需要提供给发送方和接收方等长度的密钥。因此，存在庞大的密钥分配问题。

因为上面这些困难，一次一密实际很难商用，主要用于安全性要求很高的低带宽信道。

2.3 置换技术

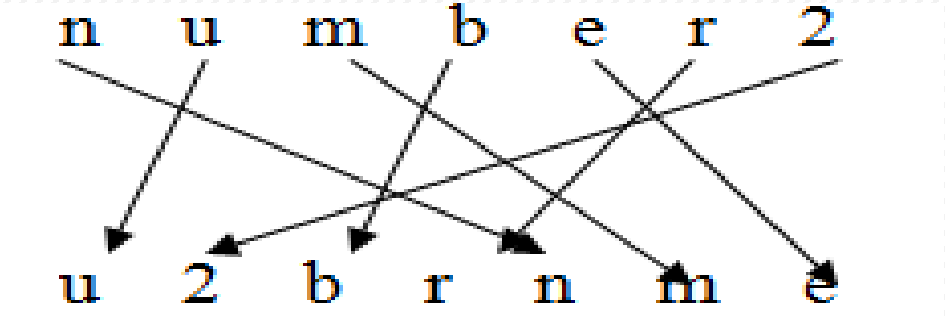
2.3 置换技术

置换是通过变动明文块内部的字符排列次序来达到加密信息的目的。

例如：明文number2，我们可以通过对它内部包含的字符、符号或数字重新排列次序使它变为密文，这个过程叫做置换。

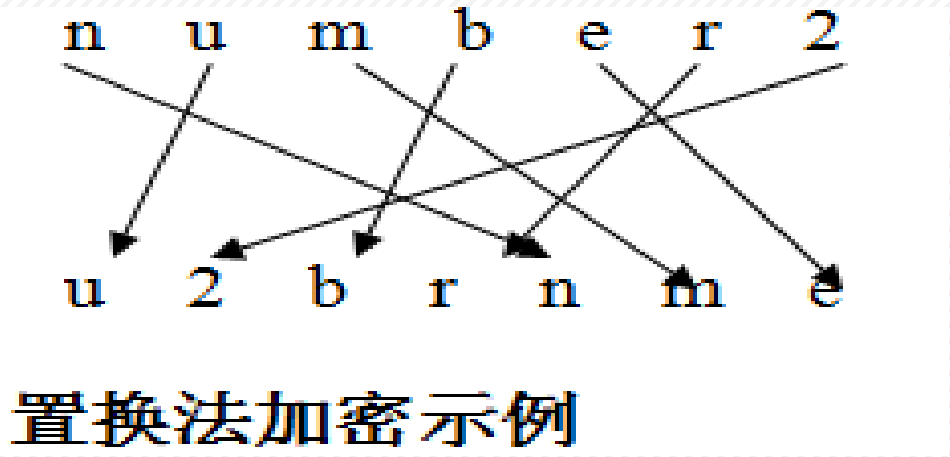
2.3 置换技术

如：把第2个字符“u”移到第1个位置，把第7个字符“2”移到第2个位置，把第3个字符“m”移到第6个位置…见下图所示，就可以把明文number2置换为密文u2brnme。



置换法加密示例

2.3 置换技术



置换法加密示例

密钥即为置换和逆置换。

置换为：[2，7，4，6，1，3，5]（2表示当前位置用第2个字母置换，其他类推）

逆置换为：[5，1，6，3，7，4，2]

2.3 置换技术

一种更复杂的方案是把消息一行一行地写成矩形块，然后按列读出，但是把列的次序打乱。列的次序就是算法的密钥。

如：明文为：Attack Postpone Duntilt Woamxyz

将明文按行的形式放置。密钥为：4 3 1 2 5 6 7

密钥为：4 3 1 2 5 6 7

明文为：A T T A C K P

O S T P O N E

D U N T I L T

W O A M X Y Z

表示把TTNA这一列置换到第1列的位置

密文为：TTNAAPTMTSUOAODWCOIXKNLYPETZ

2.3 置换技术

密文恢复为明文的过程如下：

密钥的逆置换为：　3 4 2 1 5 6 7

密文按矩阵展开为：T A T A C K P

T P S O O N E

N T U D I L T

A M O W X Y Z

明文为：

A T T A C K P

O S T P O N E

D U N T I L T

W O A M X Y Z

2.4 轮转机

2.4 轮转机

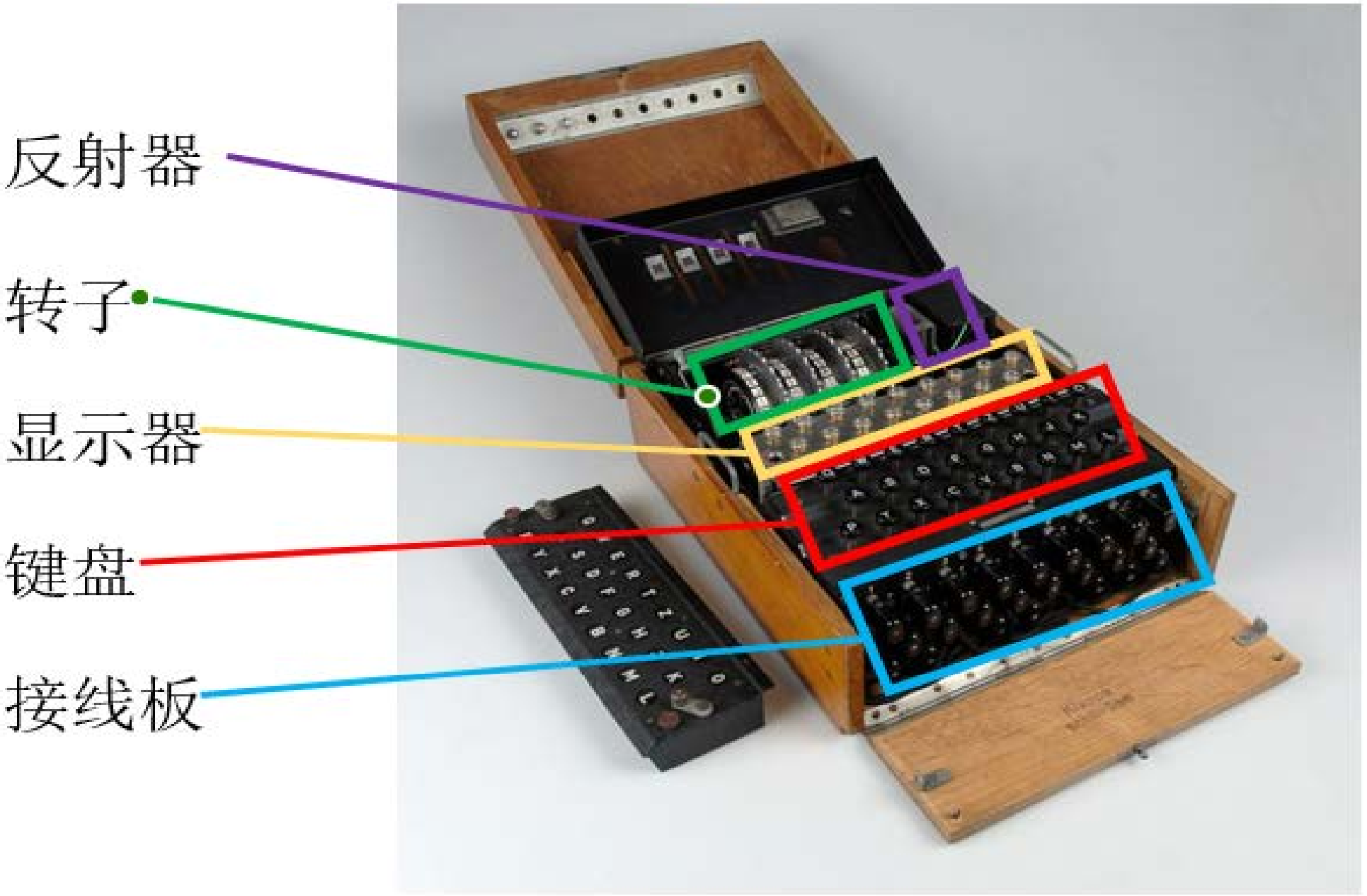
如何提高密码安全性？

- 多步置换密码
- 多步代换密码
- 一个代换，接着一个置换

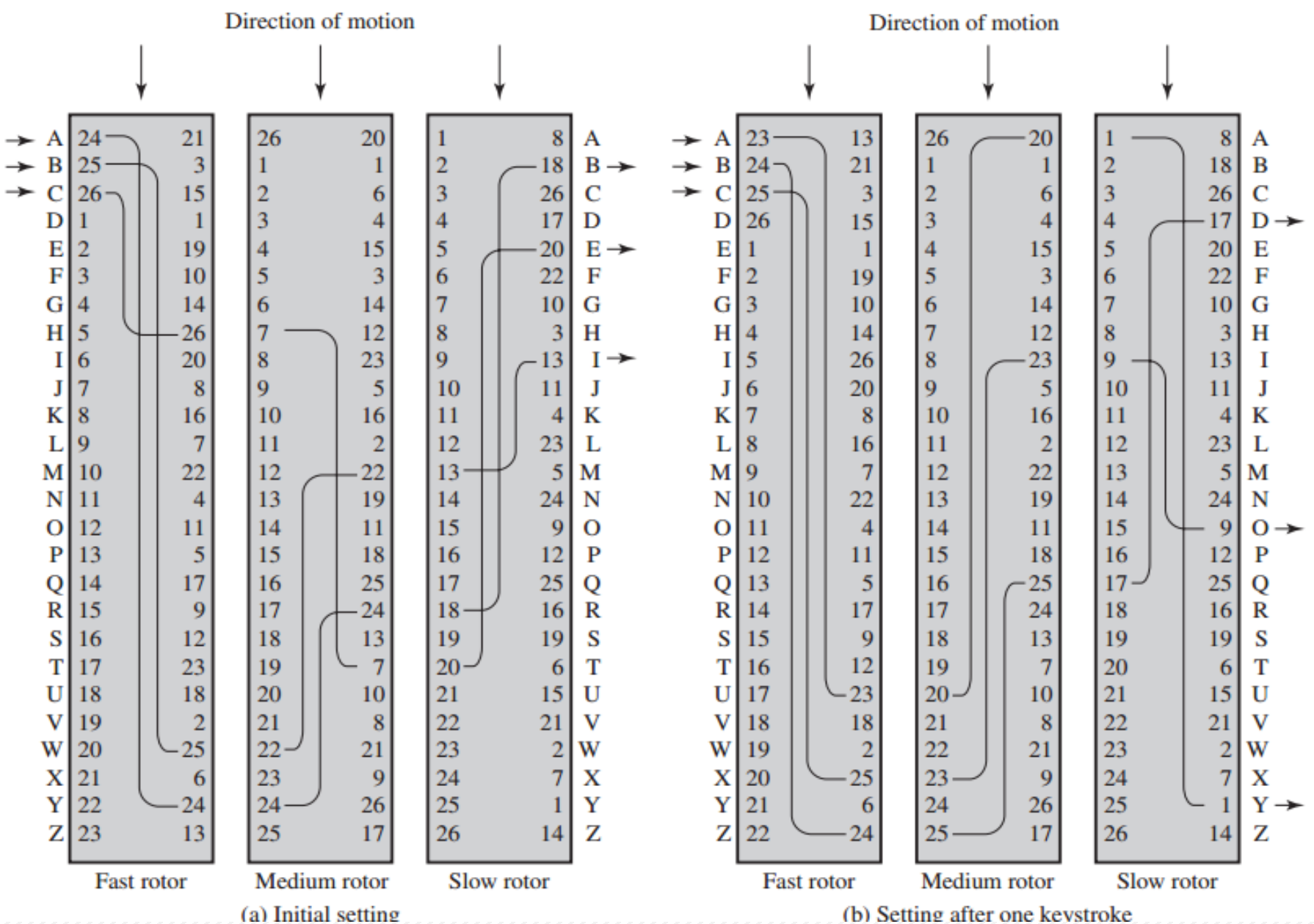
最著名的转轮装置是**Enigma**（恩尼格马，源 自希腊语**Enigma**，意指“不可思议的东西”）。

– Enigma在第二次世界大战期间由德国人使用。

2.4 轮转机



从1925年开始，谢尔比乌斯的工厂开始系列化生产ENIGMA，1926年德军开始使用这些机器。



发信人首先要调节三个转子的方向，使它们处于17576个方向中的一个（事实上转子的初始方向就是密匙，这是收发双方必须预先约定好的），然后依次键入明文，并把闪亮的字母依次记下来，然后就可以把加密后的消息用电报的方式发送出去。

2.5 隐写术

2.5 隐写术

◆《唐伯虎点秋香》

我康宣,今年一十八岁,姑苏人氏,身家清白,素无过犯。只为家况清贫，鬻身华相府中，充当书僮。身价银五十两，自秋节起，暂存账房，俟三年后支取，从此承值书房，每日焚香扫地，洗砚、磨墨等事，听凭使唤。从头做起。立此契为凭。

2.5 隐写术

隐写术不是严格意义上的加密，其实现方式是将秘密消息隐藏在其他消息中 。

常用的隐写术：

- **字符标记**：选择一些印刷字母或打字机打出的文本，用铅笔在其上书写一遍。这些标记需要做得在一般场合下辨认不出，除非将纸张按某个角度对着亮光看。
- **不可见墨水**：有些物质用来书写后不留下可见痕迹，除非加热或加之以某种化学物质。
- **针刺**：在某些字母上刺上小的针孔，这一般是分辨不出来的，除非对着光线。
- **打字机的色带校正**：用黑色的色带在行之间打印。用这种色带打印后的东西只在强光下可见。

2.5 隐写术

◆**图像中隐藏秘密消息**：即用消息比特来替代图像的每个字节中最不重要的比特。因为大多数图像标准所规定的颜色等级比人类眼睛能够觉察到的要多得多，所以图像并没有多大改变，但是，秘密消息却能够在接收端剥离出来。用这种方法可在1024*1024灰色度的图片中存储64K字节的消息。

2.5 隐写术

- 隐写术的主要**缺点**是：它要**用大量的开销来隐藏相对少量的信息比特**；且一旦该系统被发现，就会变得毫无价值。
- 隐写术现代使用其实很普遍，既有**合法的应用**也有非法的应用。合法使用的应用程序包括**保护知识产权**（如版权） —— 给图片加上所谓的**水印**。相反，违法的目的包括出于法律原因隐藏信息。

3、仿射密码（affine cipher）

密钥$k=(k_1,k_2)$

- 加密：

$$c=e_k(p)=k_1p+k_2 \pmod{26}$$

$$\gcd(k_1,26)=1$$

- 解密：

$$p=d_k(c)=k_1^{-1}(c-k_2) \pmod{26}$$

k_1^{-1}为k_1的乘法逆，满足：$k_1^{-1}k_1=1 \pmod{26}$

仿射密码的密钥量与乘法逆元k_1^{-1}

- **密钥量** $\gcd(k_1, 26) = 1$

  k_1：1，3，5，7，9，11，15，17，19，21，23，25

  k_2：0~25

$$k_q = 12 \times 26 = 312$$

- **k_1的乘法逆（mod 26）**

$1^{-1}=1$，　$3^{-1}=9$，　$5^{-1}=21$，　$7^{-1}=15$，

$9^{-1}=3$，　$11^{-1}=19$，　$15^{-1}=7$，　$17^{-1}=23$，

$19^{-1}=11$，　$21^{-1}=5$，　$23^{-1}=17$，　$25^{-1}=25$

仿射密码加密实例

- 密钥：$k=(7,3)$ $k_1^{-1}=7^{-1} \pmod{26}=15$
- 加密函数：$c=e_k(p)=7p+3 \pmod{26}$
- 解密函数：$p=d_k(c)=15(c-3) \pmod{26}$
- 明文：cryptography
- 加密、解密过程

$$c = e_k(p) = 7p + 3 \pmod{26}$$

$$p = d_k(c) = 15(c - 3) \pmod{26}$$

- 明文字符y（24）的加密、解密过程：

加密：7×24+3=171≡15=P （mod 26）

解密：15×（15-3）=15×12=180≡24=y （mod 26）

表 3-5 仿射密码实例的加密和解密过程

加密	明文字符	c	r	y	p	t	o	g	r	a	p	h	y
	明文数字	2	17	24	15	19	14	6	17	0	15	7	24
	密文数字	17	18	15	4	6	23	19	18	3	4	0	15
	密文字符	R	S	P	E	G	X	T	S	D	E	A	P
解密	密文字符	R	S	P	E	G	X	T	S	D	E	A	P
	密文数字	17	18	15	4	6	23	19	18	3	4	0	15
	明文数字	2	17	24	15	19	14	6	17	0	15	7	24
	明文字符	c	r	y	p	t	o	g	r	a	p	h	y

试一试

- 假设k_1=7，k_2=3，明文为secret，利用仿射密码算法给出对应的密文
- （18,4,2,17,4,19）

练习

3-9 用频数法破译下面的一段仿射密码密文（不含空格）：

FMXVE DKAPH FERBN DKRXR SREFM ORUDS DKDVS HVUFE DKAPR KDLYE VLRHH RH

练习

3-9　用频数法破译下面的一段仿射密码密文（不含空格）：

FMXVE DKAPH FERBN DKRXR SREFM ORUDS DKDVS HVUFE DKAPR KDLYE VLRHH RH

解：（1）密文字母频数统计

该段仿射密码密文一共有 57 个密文字符，密文字母出现的频数如下表所示：

字母	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
频数	2	1	0	7	5	4	0	5	0	0	5	2	2	1	1	2	0	8	3	0	2	4	0	2	1	0

练习

字母	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
频数	2	1	0	7	5	4	0	5	0	0	5	2	2	1	1	2	0	8	3	0	2	4	0	2	1	0

从上表可见频数比较高的密文字母：R：8 ； D：7； E、H、K：5 ； F、V：4

而明文字母频数比较高的几个英文字母依次为 e、t、a、o、i、n、s、h、r。

练习

（2）假设与推论、证实

第一次假设：频数最高的密文字母 R（17）对应频数最高的明文字母 e（4），频数次高的密文字母 D（3）对应频数次高的明文字母 t（19）。第二次假设：频数最高的密文字母 R（17）对应频数最高的明文字母 e（4），频数第三高的密文字母 E（4）对应频数次高的明文字母 t（19）。第三次假设：频数最高的密文字母 R（17）对应频数最高的明文字母 e（4），频数并列第三的密文字母 H（7）对应频数次高的明文字母 t（19）。

第四次假设：频数最高的密文字母 R（17）对应频数最高的明文字母 e（4），频数并列第三的密文字母 K（10）对应频数次高的明文字母 t（19）。根据仿射密码的加密公式，列出密文和明文的关系方程组如下：

练习

$$\begin{cases} 17 = 4k_1 + k_2 \pmod{26} & ⑦ \\ 10 = 19k_1 + k_2 \pmod{26} & ⑧ \end{cases}$$

⑧-⑦得：$15k_1 = -7 = 19 \pmod{26}$

解得：$k_1 = 15^{-1} \times 19 = 7 \times 19 = 133 = 3 \pmod{26}$

由于 $\gcd(k_1, 26) = \gcd(3, 26) = 1$，因此 $k_1 = 3$ 存在乘法逆元，且 $k_1^{-1} = 3^{-1} = 9$，说明第四次假设正确。

将 $k_1 = 3$ 代入⑦式，得：$k_2 = 17 - 4k_1 = 17 - 4 \times 3 = 5 \pmod{26}$

因此，破译得到该仿射密码的加密密钥为 $k_1 = 3$，$k_2 = 5$。将它们代入仿射密码的解密公式，得到：$p = k_1^{-1}(c - k_2) = 9 \times (c - 5) = 9c - 45 = 9c - 19 \pmod{26}$ ⑨

练习

将密文字母代入⑨式，得到对应的明文字母，如下表所示：

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

例如，密文字母 U（20）代入⑨式，得到明文字母为

$$9c-19=9\times 20-19=180-19=161=5=f \pmod{26}$$

对照题上表，将密文变换为明文，得到如下的一段具有明确意义的明文：

algorithms are quite general definitions of arithmetic processes

2.7 Hill 密码

练习

3-6 选择希尔密码的加密密钥矩阵 k 为：$k=\begin{bmatrix}03 & 02\\ 05 & 07\end{bmatrix}$试以明文 love 为例

练习

3-6 选择**希尔密码**的**加密密钥矩阵 k** 为：$k=\begin{bmatrix}03 & 02\\ 05 & 07\end{bmatrix}$试以明文 love 为例

解：将明文字符 love **变换为数字**，分别为 11、14、21、4。 因为加密密钥矩阵 k 为

2 阶矩阵，所以应将明文分成 $p_1=(11 \quad 14)$ 和 $p_2=(21 \quad 4)$ 两组分别进行加密。

练习

（1）确定解密密钥矩阵 k^{-1}

$$|k| = \begin{vmatrix} 03 & 02 \\ 05 & 07 \end{vmatrix} = 3\times 7 - 2\times 5 = 21 - 10 = 11$$

$$|k|^{-1} = 11^{-1} \mod 26 = 19$$

$$k^* = \begin{bmatrix} 07 & -02 \\ -05 & 03 \end{bmatrix} = \begin{bmatrix} 07 & 24 \\ 21 & 03 \end{bmatrix} \pmod{26}$$

$$k^{-1} = |k|^{-1} k^* = 19 \begin{bmatrix} 07 & 24 \\ 21 & 03 \end{bmatrix} = \begin{bmatrix} 133 & 456 \\ 399 & 57 \end{bmatrix} = \begin{bmatrix} 03 & 14 \\ 09 & 05 \end{bmatrix} \pmod{26}$$

练习

（2）加密

$$c_1 = p_1 \bullet k = (11 \quad 14) \bullet \begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix} = (103 \quad 120) = (25 \quad 16) = (Z \quad Q) \pmod{26}$$

$$c_2 = p_2 \bullet k = (21 \quad 4) \bullet \begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix} = (83 \quad 70) = (5 \quad 18) = (F \quad S) \pmod{26}$$

因此，明文字符 love 的加密密文为 ZQFS。

练习

（3）解密

$$p_1 = c_1 \bullet k^{-1} = (25 \quad 16) \bullet \begin{bmatrix} 03 & 14 \\ 09 & 05 \end{bmatrix} = (219 \quad 430) = (11 \quad 14) = (l \quad o) \pmod{26}$$

$$p_2 = c_2 \bullet k^{-1} = (5 \quad 18) \bullet \begin{bmatrix} 03 & 14 \\ 09 & 05 \end{bmatrix} = (177 \quad 160) = (21 \quad 4) = (v \quad e) \pmod{26}$$

因此，密文字符 ZQFS 的解密明文为 love，即解密后恢复了原来的明文。


海南大学
Hainan university