西安郵電大學

XI'AN UNIVERSITY OF POSTS & TELECOMMUNICATIONS

3、多表代换与置换密码

主讲人：任方

网络空间安全学院

维吉尼亚密码

单表代换密码---移位密码、仿射密码等等

多表代换密码----维吉尼亚密码（Vigenère cipher），它是由法国人Blaise de Vigenère在16世纪提出的。

定义 维吉尼亚密码体制：

令是一个正整数，$M=C=K=(Z_{26})^m$。对任意的密钥 $key=(k_1,k_2,\cdots,k_m)\in K$ $(x_1,x_2,\cdots,x_m)\in M$ $(y_1,y_2,\cdots,y_m)\in C$ 定义：

$$e_{key}(x_1,x_2,\cdots,x_m)=(x_1+k_1,x_2+k_2,\cdots,x_m+k_m)\bmod 26$$

$$d_{key}(y_1,y_2,\cdots,y_m)=(y_1-k_1,y_2-k_2,\cdots,y_m-k_m)\bmod 26$$

如果已经在26个英文字母和之间建立了一一对应的关系，则每一个密钥都相当于一个长度为m的字母串，被称为密钥字。

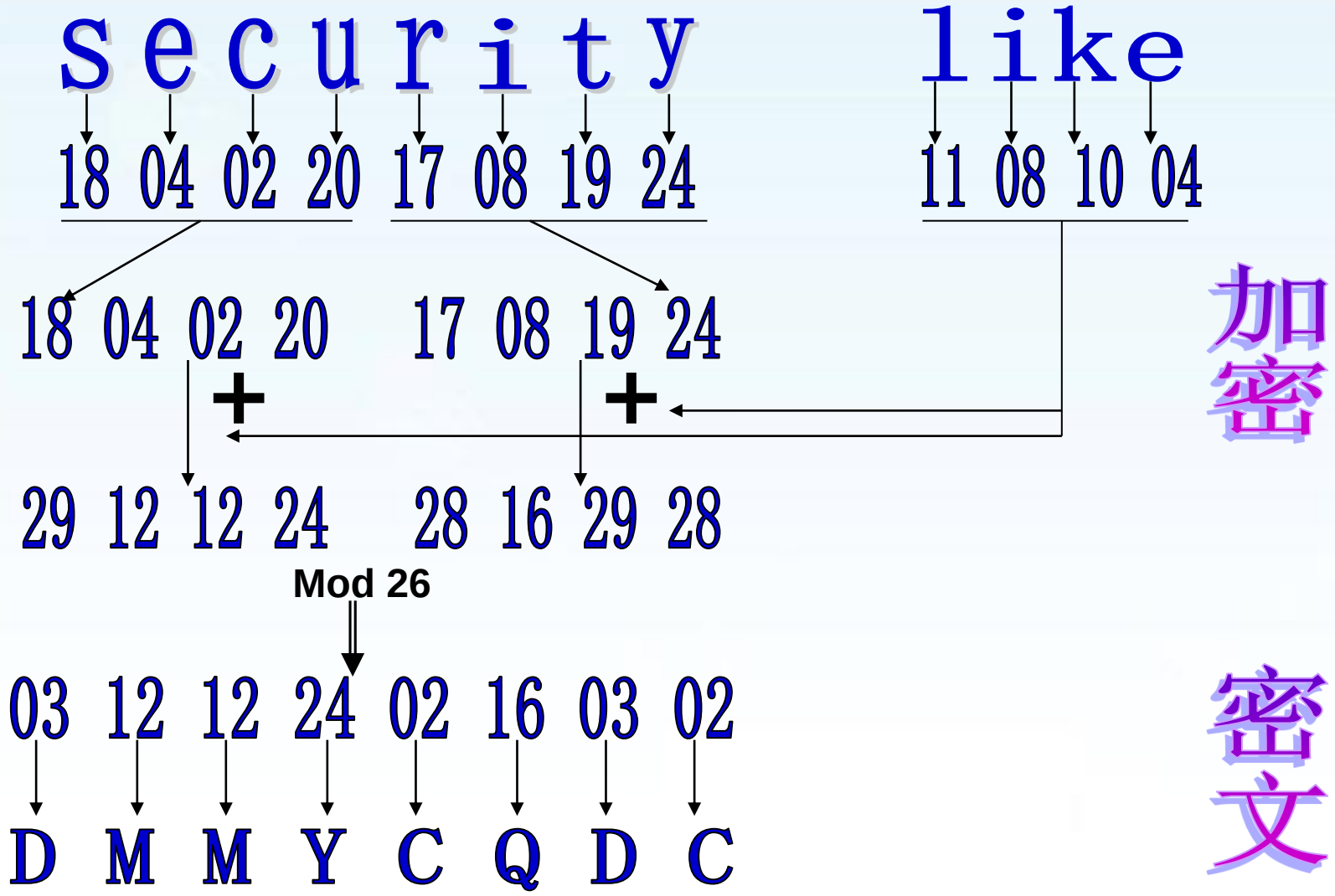
维吉尼亚密码的密钥空间大小为26^m，所以即使m的值较小，相应的密钥空间也会很大。

西安郵電大學 XI'AN UNIVERSITY OF POSTS & TELECOMMUNICATIONS

维吉尼亚方阵密表

	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	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

西安郵電大學
XI'AN UNIVERSITY OF POSTS & TELECOMMUNICATIONS



西安郵電大學
XI'AN UNIVERSITY OF POSTS & TELECOMMUNICATIONS

置换密码

通过重新排列消息中元素的位置而不改变元素本身的方式，对一个消息进行变换。这种加密机制称为置换密码(也称为换位密码)。

定义 置换密码体制

令 $m \geq 2$ 是一个正整数，$M = C = (Z_{26})^m$

K是$Z_m = \{1, 2, \cdots, m\}$上所有可能置换构成的集合。对任意的 $(x_1, x_2, \cdots, x_m) \in M$

$\pi \in K$ $(y_1, y_2, \cdots, y_m) \in C$，定义：

$$e_\pi(x_1, x_2, \cdots, x_m) = (x_{\pi(1)}, x_{\pi(2)}, \cdots, x_{\pi(m)})$$

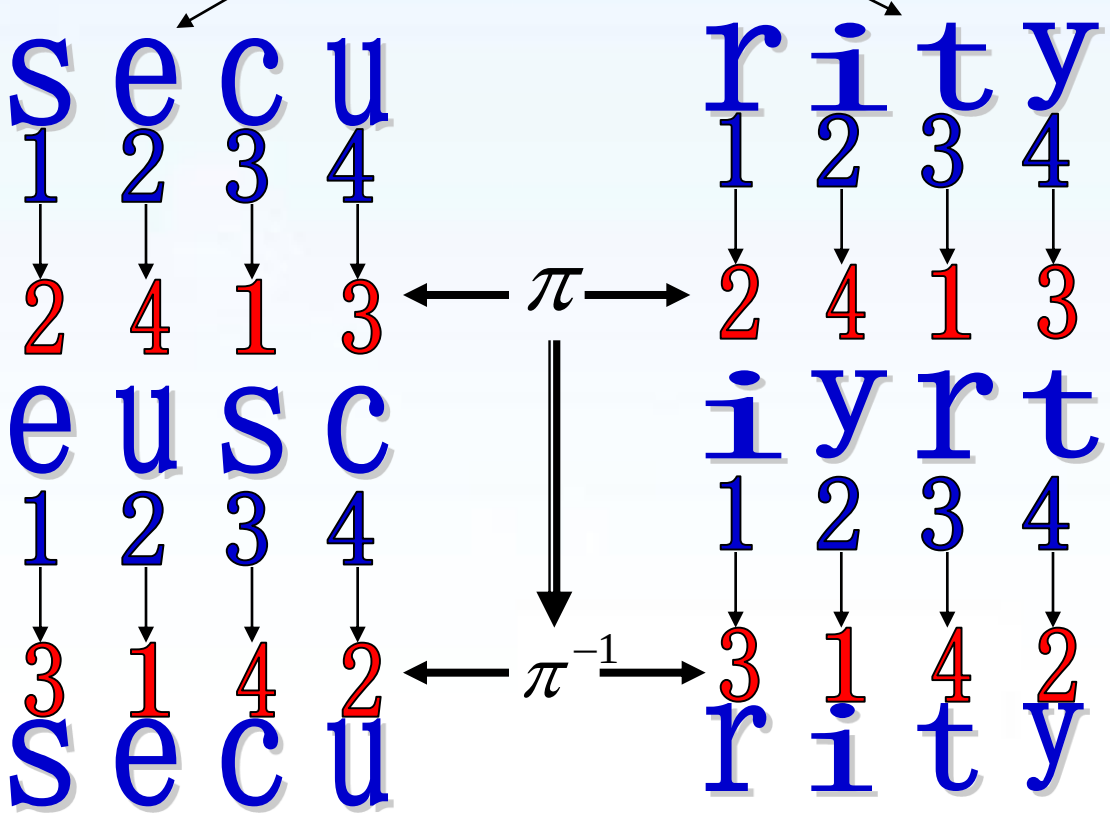
$$d_\pi(y_1, y_2, \cdots, y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, \cdots, y_{\pi^{-1}(m)})$$

其中π和π^{-1}互为逆置换，m为分组长度。对于长度大于分组长度的明文消息，可对明文消息先按照长度进行分组，然后对每一个分组消息重复进行同样的置乱加密过程，最终实现对明文消息的加密。

西安郵電大學 XI'AN UNIVERSITY OF POSTS & TELECOMMUNICATIONS

假设：$m=4$　　$\pi=(\pi(1),\pi(2),\pi(3),\pi(4))=(2,4,1,3)$

明文为：security



加密

解密

对于固定的分组长度 m，Z_m 上共有 $m!$ 种不同的排列，对应产生 $m!$ 个不同的加密密钥 π，所以相应的置换密码共有 $m!$ 种不同的密钥。

郵電大學 OF POSTS & TELECOMMUNICATIONS

- 在已经介绍的几个典型的古典密码体制里，含有两个基本操作：代换（Substitution）和置换（Permutation）。
  - 代换实现了英文字母外在形式上的改变，每个英文字母被其它字母替换；
  - 置换实现了英文字母所处位置的改变，但没有改变字母本身。
- 代换（替换）操作又可以分为单表替换和多表替换两种方法。
  - 单表替换的特点是把明文中的每个英文字母正好映射为一个密文字母，是一种一一映射，不能抵御基于英文字符出现频率的频率分析攻击法；
  - 多表替换的特点是明文中的同一字母可能用多个不同的密文字母来代替，与单表替换的密码体制相比，形式上增加了加密的安全性。

西安郵電大學
XI'AN UNIVERSITY OF POSTS & TELECOMMUNICATIONS

The end !