哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY
立足航天，服务国防，面向国民经济主战场

计算机网络之危机四伏

主讲人：李全龙

本讲主题

密码学基础（2）

传统加密方法

替代密码(substitution cipher): 利用一种东西替代另一种东西

- 凯撒密码(Casesar cipher)：一个字母替代另一个字母
  - 将一个字母利用字母表中该字母后面的第*k*个字母替代
  - 如*k=3*，“bob. i love you. alice”→“ere, l oryh brx. dolfh”
- 单码(字母)替代密码(monoalphabetic cipher)

明文:abcdefghijklmnopqrstuvwxyz

密文:mnbvcxzasdfghjklpoiuytrewq

e.g.: 明文: bob. i love you. alice

密文: nkn. s gktc wky. mgsbc

加密秘钥: 26个字母集合向26个字母集合的映射

传统加密方法

替代密码(substitution cipher): 利用一种东西替代另一种东西

- 多码(字母)替代加密(polyalphabetic encryption)：使用多个单码替代密码，明文中不同位置的字母使用不同的单码替代密码
- 例如，使用采用两个凯撒密码的多码替代加密：

Plaintext letter:	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
$C_1(k = 5)$:	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
$C_2(k = 19)$:	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

加密秘钥: (C_1=5, C_2=19); C_1, C_2, C_2, C_1, C_2;……

明文：bob. i love you.

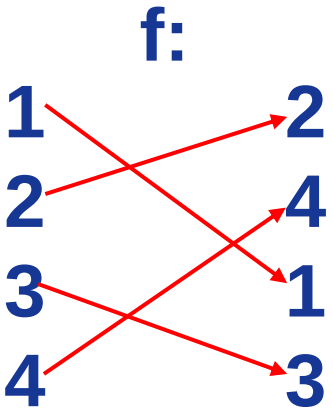
密文：ghu. n etox dhz.

传统加密方法

换位(transpositions)密码: 重新排列明文中的字母

- 置换法(permutation method)
  - 将明文划分为固定长度(d)的组，每个组内的字母按置换规则(f)变换位置
  - 密钥：(d, f)
- 例如：

秘钥: d=4, f:=(1→3,2 →1,3 →4,4 →2)



明文(m)： i love you.

ilov eyou

密文(c)： lvio yueo

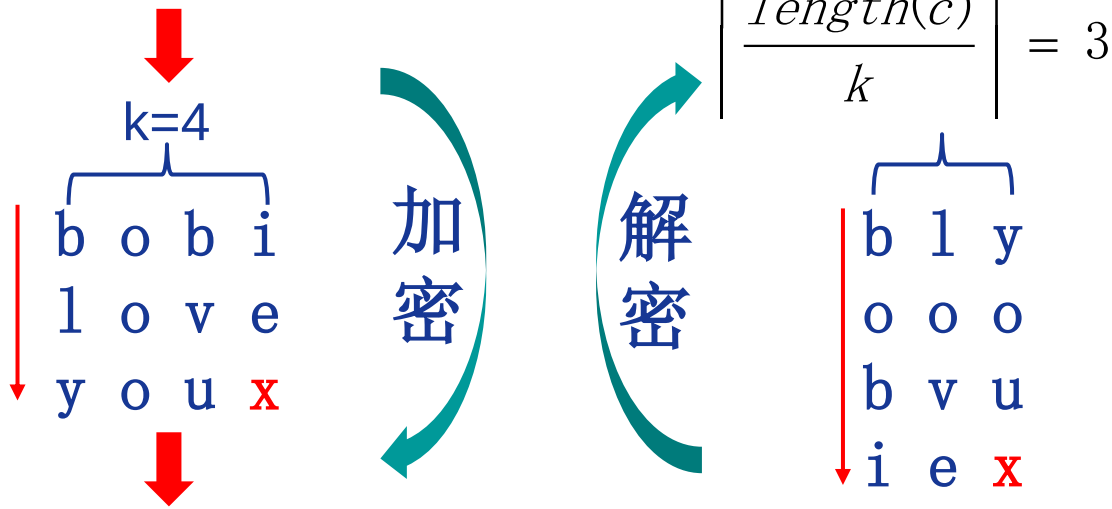
传统加密方法

换位(transpositions)密码: 重新排列明文中的字母

- 列置换加密
  - 将明文按行组成一个矩阵，然后按给定列顺序输出得到密文
- 例如：

秘钥: k=4(矩阵列数), (2, 3, 1, 4)(输出顺序)

明文(m): bob. i love you.



密文(c): ooo bvu bly iex

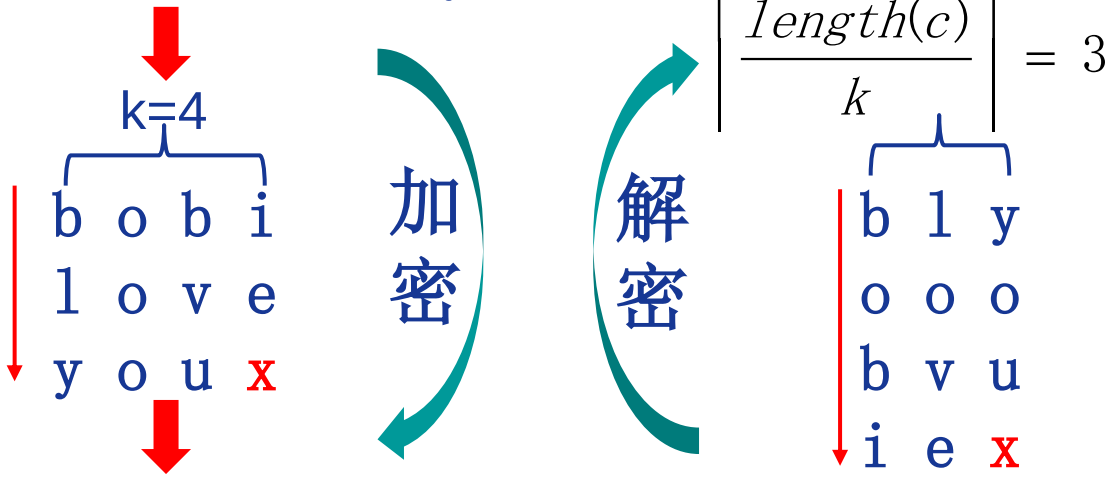
传统加密方法

换位(transpositions)密码: 重新排列明文中的字母

- 列置换加密的密钥包括列数和输出顺序
  - 可以用一个单词来表示
  - 单词长度表示列数，单词中的字母顺序表示输出顺序
- 例如：

秘钥: nice

明文(m): bob. i love you.



密文(c): bvu iex ooo bly

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

立足航天，服务国防，面向国民经济主战场

谢 谢！