简单密码系统

置换密码（substitution cipher）

基本思想

- 保留明文符号顺序，将明文伪装起来。
- 每个字母或者每组字母被另一个字母或另一组字母取代。

恺撒密码：每个字母被字母表中固定位移为3的另一个字母替代。

示例1：

- 明文 a t t a c k
- 密文 D W W D F N

明文字母	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
密文字母	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

加密方法：循环移动字母表
密钥：移动的位移数

恺撒密码一般方法：每个字母被字母表中固定位移为k的另一个字母替代。

单字母置换方法

单字母置换：“符号-符号”的置换策略。

单字母置换

- “符号-符号”的置换策略
- 凯撒密码：错开3个位置
- 无规律的映射

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

- **加密方法：单个字母被置换成另一个**
- **密钥：密钥是对应于整个字母表的26字母串**

示例2：

- **明文** a t t a c k
- **密文** Q Z Z Q E A

替代密码（transposition cipher）

基本思想

- 打乱明文符号的顺序，重新对符号进行排序，但不进行伪装
- 密钥在字母表中的出现顺序就是明文的发送顺序
- 将明文排成矩阵形式，按上面顺序按列发送

密钥 | n e t w o r k

密钥字母在字母表中的排列顺序 | 3 1 6 7 4 5 2

待发送的明文 | h e l l o w o
r l d a b c d

示例3：

- 明文：hello world
- 密文：？

发送的密文 | e l o d h r o b w c l d l a

替代密码示例

示例4：给定密钥为 MEGABUCK
明文：please transfer one million dollars to my swissbank account sixtwotwo

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

密钥
密钥顺序

① 计算密钥在字母表中的顺序
② 将明文排成以密钥长度为列数的矩阵
③ 按密钥字母依次发送列

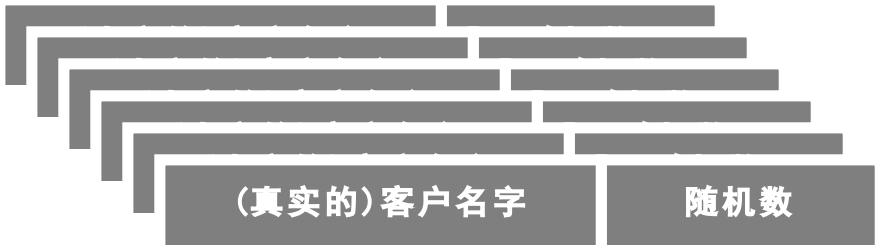
AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRCXB

基本密码学两大原则——冗余度

示例5：某家玩具公司的订单管理采用部分加密方法.

心怀不满
离职员工

虚假订单

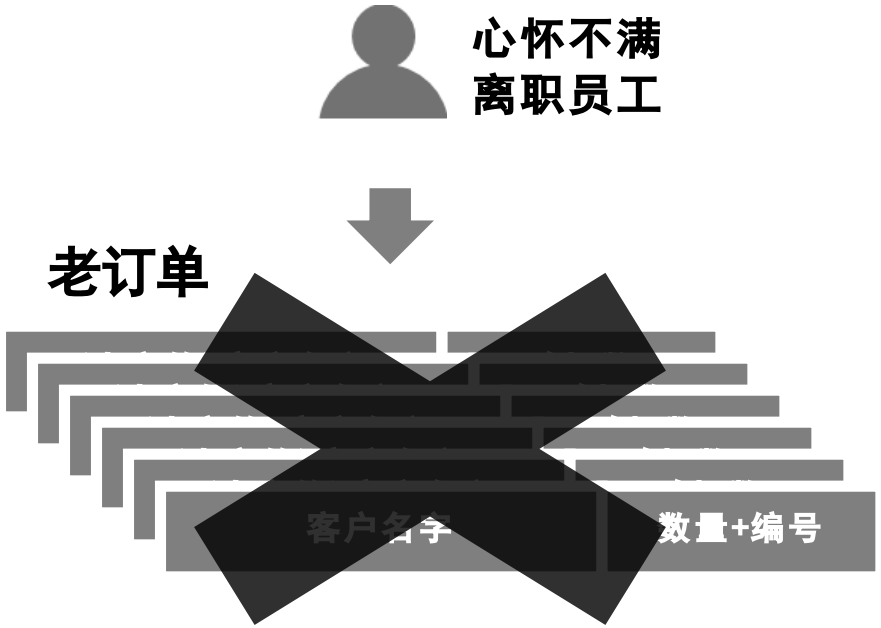


解决方法：增加冗余的0

密码学原则一：消息必须包含一定的冗余度。

基本密码学两大原则——抗重放攻击

示例6：某家玩具公司的订单管理采用部分加密方法。



解决办法：设置消息的时间戳和有效期（比如仅发出后10秒有效）.

密码学原则二：需要采取某种方法来对抗重放攻击.

很短时间内有效的时间戳可以预防重放攻击。