§2.2 代替密码

代替密码是使用替换法进行加密所产生的密码。

代替密码就是明文中每一个字符被替换成密文中的另外一个字符，替换后的各字母保持原来位置。接收者对密文进行逆替换就恢复出明文来。

在替换密码加密体制中，使用了密钥字母表。它可以由明文字母表构成，也可以由多个字母表构成。

§2.2 代替密码

在传统密码学中，有四种类型的代替密码：

1、单表（简单）替换密码：就是明文的一个字符用相应的一个密文字符替代。加密过程中是从明文字母表到密文字母表的一一映射。例：恺撒（Caesar)密码。

2、多表替换密码：由多个单字母密码构成，每个密钥加密对应位置的明文。 例：维吉尼亚密码。

3、多字母组替换密码：字符块被成组加密，例如“ABA”可能对应“RTQ”，ABB可能对应“SLL”等。例：Playfair密码。

4、同音（多名码）替换密码：它与简单替代密码系统相似，唯一的不同是单个字符明文可以映射成密文的几个字符之一，同音替代的密文并不唯一。

§2.2 代替密码

➢ 单表替换密码

1、恺撒（Caesar)密码

凯撒密码，又叫循环移位密码。它的加密方法就是把明文中所有字母都用它右边的第k个字母替代，并认为Z后边又是A。这种映射关系表示为如下函数：

$$F(a)=(a+k) \bmod 26$$

其中：a表示明文字母；k为密钥。

§2.2 代替密码

设k＝3，则有

明文	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	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

对于明文P = computer systems

有密文C = frpsxwhu vbvwhpv

显然，由密文C恢复明文非常容易，只要知道密钥K，就可构造一张映射表。其加密和解密均可根据此映射表进行。

凯撒密码的优点是密钥简单易记。但它的密文与明文的对应关系过于简单，故安全性很差。

§2.2 代替密码

2、密钥短语密码

选择一组有助于记忆的英文字符串作为密钥，从中筛选无重复的字符按原顺序记下字符串，写在明文字母表下，然后将未出现在字符串的字母按顺序依次写在密钥短语后。

如选择密钥短语network security

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

若明文为data access

则密文为wnln nttojj

§2.2 代替密码

➢ 多表替换密码

多表替换密码是一种用多组替换表依次对明文消息的字母进行替换的加密方法。

维吉尼亚（Vigenere）密码是一种常用的多表替换密码。这种替换法是循环的使用有限个字母来实现替换的一种方法。这种加密的加密表是以字母表移位为基础把26个英文字母进行循环移位，排列在一起，形成26×26的方阵。该方阵被称为维吉尼亚表。采用的算法为

$$f(p_i) = (p_i + k_i) \bmod 26$$

优点：能抵抗简单的字母频率分析攻击。

§2.2 代替密码

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

例：P = *h o w a r e y o u*

K= *y o u r y o u r y*

C = *f c q r p s s f s*

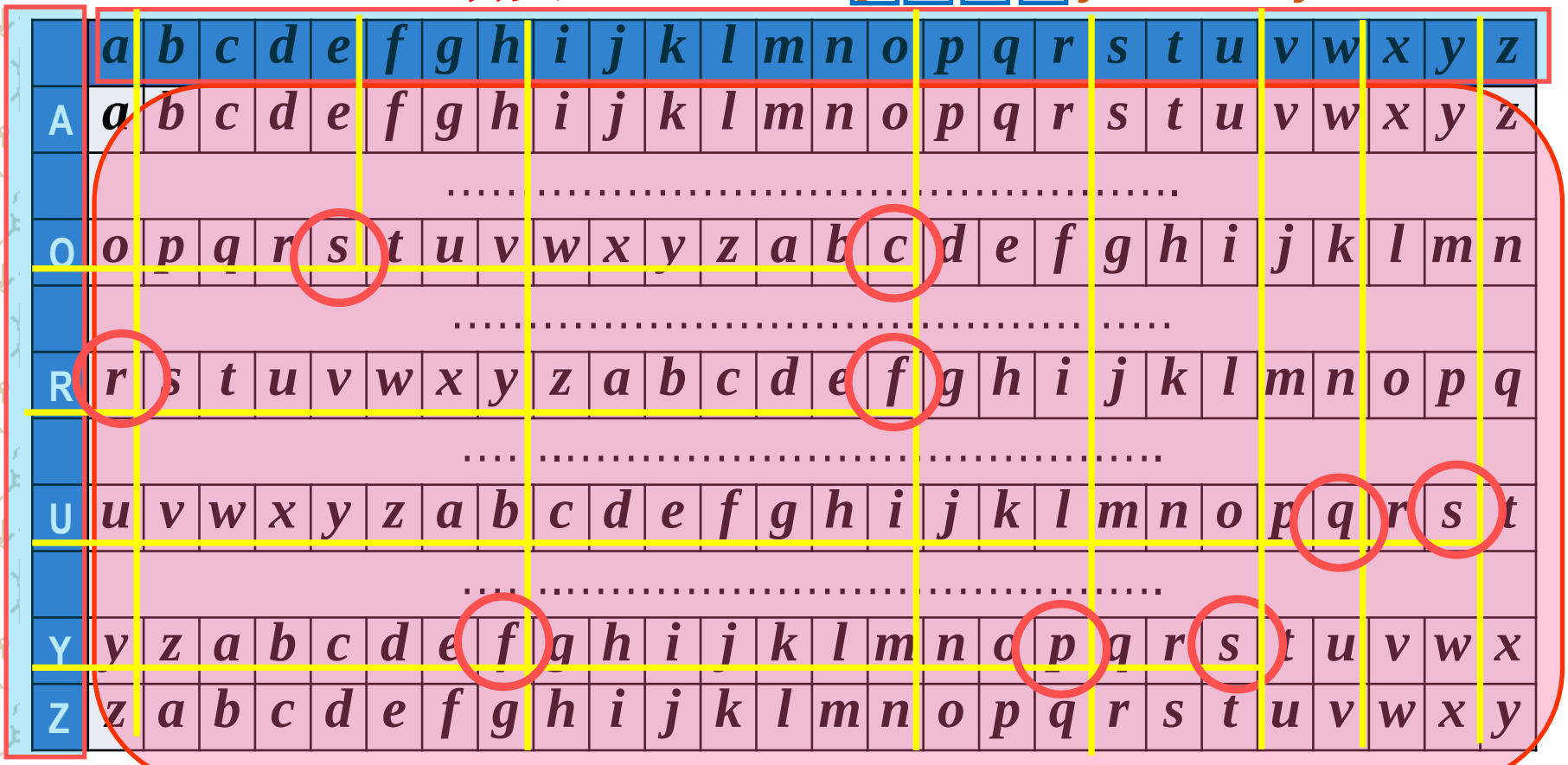
§2.2 代替密码

例：P = h o w a r e y o u

K= y o u r y o u r y

Vigenere密码表

明文P



密钥K

密文C

C = f c q r p s s f s

§2.2 代替密码

➢ 多字母替换密码

多字母替换密码每次加密一组（两个以上）字母串。

Playfair密码是此类密码，密钥由25个英文字母（j与i相同）组成的5阶方阵。密钥方阵P导出取决于给定密钥，重复不写，余下按字母顺序填充。

明文划分如下：将明文字母串按两个字母一组进行分组，每组中的两个字母不同。每一对明文字母 m_1和m_2，对应的密文为c_1和c_2。

§2.2 代替密码

每一对明文字母 m_1和m_2，按下面的规则进行加密。

（1）若m_1和m_2在P的同一行，则密文c_1和c_2分别是m_1和m_2右边的字母。第一列看作最后一列的右边。

（2）若m_1和m_2在P的同一列，则密文c_1和c_2分别是m_1和m_2下边的字母。第一行看作最后一行的下边。

（3）若m_1和m_2在P的不同行、不同列，则密文c_1和c_2是m_1和m_2确定的长方形的另两个顶点的字母。其中c_1与m_1同行， c_2与m_2同行。

（4）若$m_1=m_2$，则在m_1和m_2之间加一个无效字母（如x）。

（5）若明文字母为奇数个，则在末尾加一个无效字母。

§2.2 代替密码

例：以*firewall security*为密钥，

加密明文*how are you*

由密钥导出密钥矩阵为

$$P=\begin{pmatrix} F & I & R & E & W \\ A & L & S & C & U \\ T & Y & B & D & G \\ H & K & M & N & O \\ P & Q & V & X & Z \end{pmatrix}$$

明文分组处理*ho wa re yo ux*

密文*kh fu ew gk cz*

明文*happy*

分组处理*ha px py*

密文*pt qz qt*