§2.3 换位密码

换位密码是采用换位法进行加密的。它把明文中的字母重新排列，本身不变，但位置变了，换位密码是靠重新安排字母的次序，而不是隐藏他们。

常见的换位密码主要有倒置法、列换位法、矩阵换位法。

§2.3 换位密码

- 倒置法

（1）完全倒置法

把明文中的字母按顺序倒过来写，然后以固定长度的字母组发送或记录。

明文：**computer systems**

密文：**smet sysr etup moc**

（2）分组倒置法

把明文中的字母按固定长度分组后，每组字母串倒过来写。

明文：**computer systems**

分组：**comp uter syst ems**

密文：**pmoc retu tsys sme**

§2.3 换位密码

- 换位法

（1）列换位法

（2）矩阵换位法

§2.3 换位密码

- 换位法

（1）列换位法

将明文字符分割成为若干个（例如5个）一行的分组，并按一组后面跟着另一组的形式排好，形式如下：

c1	c2	c3	c4	c5
c6	c7	c8	c9	c10
……				

最后，不全的组可以用不常使用的字符x或a,b,c…填满。

密文是取各列来产生的：c1c6…c2c7…c3c8….c4c9…. c5c10….

§2.3 换位密码

例：明文：**WHAT YOU CAN LEARN FROM THIS BOOK**

取密钥为5， 进行排列：

W	H	A	T	Y
O	U	C	A	N
L	E	A	R	N
F	R	O	M	T
H	I	S	B	O
O	K	X	X	X

则密文为：**WOLFHO HUERIK ACAOSX TARMBX YNNTOX**

§2.3 换位密码

（2）矩阵换位法

把明文中的字母按给定的顺序安排在一矩阵中，然后用另一种顺序选出矩阵的字母来产生密文。

§2.3 换位密码

例：明文ENGINEERING按行排在3 × 4矩阵中，最后一行不全用ABC…填充，给定置换 $f=\begin{pmatrix}1234\\2413\end{pmatrix}$。

明文P = ENGINEERING

密钥K = (m*n, f) = (3*4, $\begin{pmatrix}1234\\2413\end{pmatrix}$)

密文C= NIEGERNENAIG

