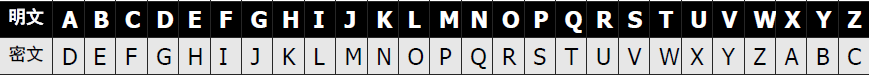
**重点： Caesar、Playfair、S-DES、RSA、MD、Email Security、IPsec、Intrusion**

**Caesar密码**：**PPT1.1**

c=(m+3) mod 26



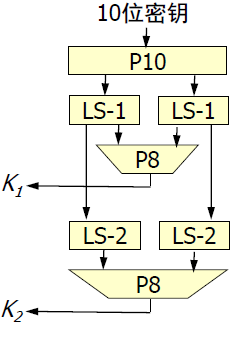
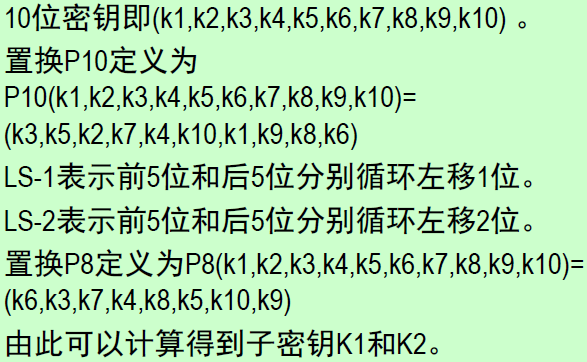
**Playfair密码**：**PPT1.1**

基于密钥词构成的5×5字母矩阵。填充矩阵是密钥词从左至右、从上至下填充，剩余字母按顺序从左至右、从上至下填充剩余格子。字母I和J 当作一个字母。

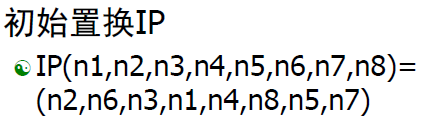
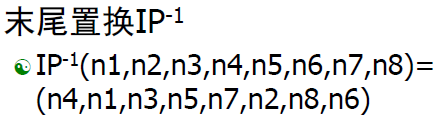
加密规则：一次加密两个字母，如果字母对是两个相同的字母，添加一个填充字x。落在同行的明文字母对中的字母，由其右边字母代换。落在同列的明文字母对中字母，由其下面字母来代换。其它明文字母对中的字母，行是该字母所在行，列是另一字母所在列。

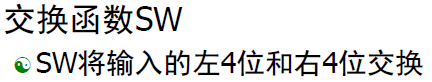
**S-DES算法**：**PPT1.2**

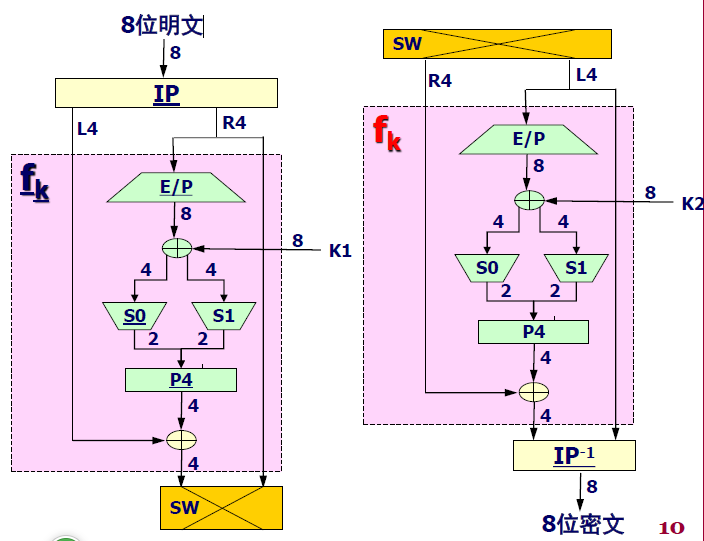
首先，计算子密钥：

其次，进行加密：





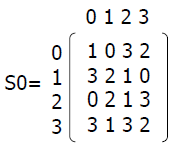
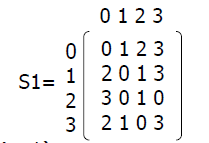
计算映射fk：



与子密钥异或，前后4位分别查找S盒。第1、4位作为二进制数决定S盒的行，第2、3位作为二进制数决定S盒的列，输出即是二进制的2位输出。

由S0和S1输出构成4位再进行置换**P4(n1,n2,n3,n4)=(n2,n4,n3,n1)。**

P4的输出再和L4按位异或，和R4组合在一起就是函数F的输出了。

**RSA算法**：PPT1.3

产生密钥：

取两个大素数p和q，保密；

计算n=pq，公开n；

计算欧拉函数ф(n) =(p-1)(q-1)；

任意取一个与ф(n) 互素的小整数e，即 gcd (e, ф(n) )=1，1<e< ф(n)；

寻找d, d< ф(n)，使得 de ≡1 mod ф(n)，即de =k ф(n) +1；

公开密钥：KU={e, n}

秘密密钥：KR={d, n}

加密过程：

把待加密内容分成k比特分组，k≤log2n，并写成数字，设为M。

则：C= M^e mod n

解密过程：

M = C^d mod n