

## 1. 代换密码

加密：将明文字符按照对应关系代换成另外的密文字符

解密：将密文字符按照对应关系还原成明文字符

密钥：对应关系。

例子：棋盘密码，将字母带换成他的坐标。凯撒密码：每个字母向后推移三位

对于密码体制的五元组  $(M, C, K, E, D)$