**古典密码1——置换密码**

明文：可以很容易理解明文内容想表达的意思。如：我要打游戏

密文：无法从表面上得知内容想表达的意思。如：戏打游我要

加密：将明文转换为密文的过程。

解密：将密文还原为明文的过程。

**置换密码**：将明文中的字母重新排列，字母本身不变，但其位置改变了，这样编成的密码称为置换密码。

如：将明文按某一顺序排成一个矩阵，其中不足部分用⊘填充，然后按另一顺序选出矩阵中的字母以形成密文。

举例：

明文：I LIKE PLAYING GAMES

矩阵：ILIKEP

LAYING

GAMES⊘

密文：ILGLAAIYMKIEENSPG⊘

上面例子的矩阵大小为每行6个字母，选取顺序为从左向右按列选取。即先1行1列的I，再2行1列的L，再3行1列的G，再1行2列的L，再2行2列的A，以此类推。

破解以上密文的关键是排列出正确的矩阵，然后从矩阵提取明文。现已知每行6个字母，总字母数为18，18/6=3，总共3行，则原明文矩阵为3行6列。且已知从左向右提取，所以前3个字母为第一列，如下：

矩阵：I

L

G

接下去3个字母为第二列：

矩阵：IL

LA

GA

以此类推，得到完整的矩阵：

矩阵：ILIKEP

LAYING

GAMES⊘

从此矩阵得到内容：ILIKEPLAYINGGAMES

对单词进行分割后，即可得到明文：I LIKE PLAYING GAMES

由上面的过程可以看出，改变矩阵大小（每行字母数）和提取顺序可以得到不同的密文。所以在实际破解时，如果无法得到足够信息（通常得不到），那就只能尝试不同的情况。

如上面的例子只知道密文，不知道矩阵大小和提取顺序，则每行2个字母、3个字母、4个字母等情况都要试，从左向右提取、从右向左提取也都要试。这种时候，如果你能**借助计算机来编程实现，则效率可以千万倍地提高。**