

## ❖ 加密解密

如果一个密码加密后只有一种解密方法,则称为好的. Dima 发明了一种密码,将俄文字母表(由 33 个字母组成)中每个字母用至多 10 个字母组成的序列来表示.借助于计算机的帮助, Dima 的朋友 Serjozha 检查了这种加密方案,发现任何一批至多 10 000 个字母组成的电文至多可用一种方法(即 Dima 的方法)来解密.问 Dima 的密码是好的吗?

**解** 用反证法.如果 Dima 的密码不是好的.由题设,一定有一批电文,这批电文中每个电文必须是由超过 10 000 个字母组成的电文,即至少是由 10 001 个字母组成的电文,它们可以用 Dima 的方法和 Serjozha 的方法来解密.

题目要求每个俄文字母用至多 10 个字母组成的序列来表示,这至多 10 个字母组成一个“单词”.由于每个“单词”最多由 10 个字母组成,所以用 Dima 方法解密的文件,至少由 1 001 个单词组成.因此这个文件的所有单词的初始字母至少有 1 001 个.由于俄文字母由 33 个符号组成,由抽屉原理,所以其中至少有 31 个字母是相同的.现在用 Serjozha 方法解密.这些字母可能是一个单词的第  $i$  个字母,  $1 \leq i \leq 10$ .再由抽屉原理,它们中至少有 4 个字母有相同的位置  $i$ .在这 4 个字母中选两个,去掉这两个字母之间的所有字母和这两个字母中的一个.用 Dima 方法解密,完整的单词被改变了,但仍可解密.但是这两个字母的选

取,保证了这两个部分单词将组成一个新的完整的单词,因此改变后的文件,仍可用 Serjozha 的方法解密.这是一个比原来文件还要短的文件,却可用两种不同方法解密,这和题设矛盾,所以证明了 Dima 的加密方案是好的.