**C语言附加题-维吉尼亚密码（Vigenere Cipher）**

维吉尼亚密码是单字母多表密码（Polyalphabetic cipher）的一种，其在密文字母表之间切换的想法是革命性的。在加密时，相同的明文字符会被不同的密文字符（即多字母字符）所代替。恩尼格玛密码机（Enigma）是历史上最著名的用于加密与解密文件的密码机之一，它就是使用了一种改进的单字母多表密码（Polyalphabetic cipher）。

自其发明以来的许多世纪，它以一种非常安全的密码而闻名，并且在很长一段时间内被认为是牢不可破的，故其赢得了它的绰号“le chiffre indéchiffrable”（法语为“牢不可破的密码”）。虽然事实并非如此（Friedrich Kasiski在1863年完全破译了它），但在通过纸笔为通信工具的情况下，它仍然是一种非常安全的密码。

# 维吉尼亚方阵（Vigenere Square）：

# C:\Users\Administrator\Desktop\Vigenere-Cipher-Table.png

# 图1 维吉尼亚方阵

**加密（Enc）：**

使用数字0-25代替26个字母A-Z，维吉尼亚密码的加密文法可以写成[同余](https://baike.baidu.com/item/%E5%90%8C%E4%BD%99" \t "_blank)的形式（其中C表示密文，P表示明文，K表示关键词（Keyword），l为关键词的长度）：

***Ci* = (*Pi* + *ki* mod *l*) mod 26**

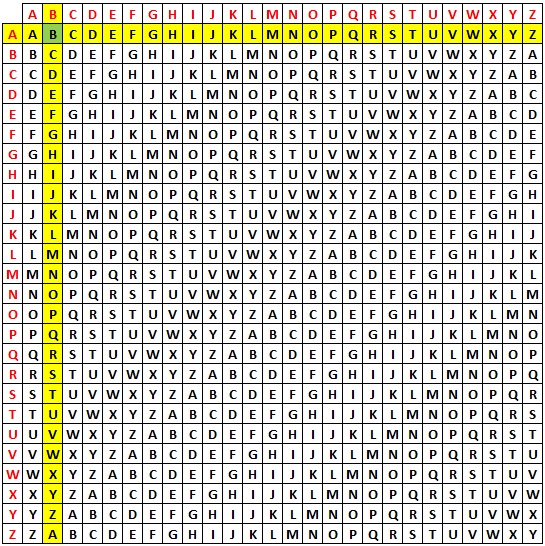
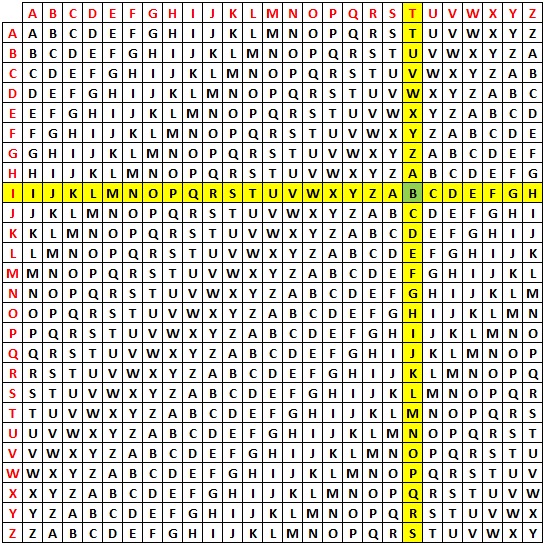
对于每个明文字母，找到其在维吉尼亚方阵（Vigenere Square）中左侧第一列的位置，并从密钥流（Keystream）中取出相应的字母，并在维吉尼亚方阵（Vigenere Square）的顶部第一行中找到它。方阵中这两条线交叉的地方就是使用的密文字母。

**例：**选择一个关键字（或关键短语），反复重复此关键字，直到它与明文（Plaintext）的长度相同。 这被称为密钥流（Keystream）。本例中密钥流选择了关键字：**battista**。

**Picture**

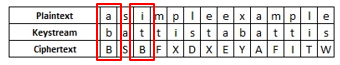
# 图2 加密密钥流

** **

# 图3 加密操作

继续这一操作，我们最后能得到密文“BSBF XDXEYA FITW”，注意到：“a”和“i”都加密为“B”，并且出现的三个“e”分别被加密为“X”，“E”和“W”。



# 图4 加密后的密文

**解密（Dec）：**解密方法则能写成：

***Pi* = (*Ci* - *ki* mod *l*) mod 26**

要使用关键字（Keyword）解密密文，我们首先必须通过重复关键字来生成密钥流（Keystream），直到我们有一个与密文长度相同的密钥流。然后，在维吉尼亚方阵（Vigenere Square）的顶部第一行中找到带有密钥流字母的行，并在此行中向下寻找，直到找到密文（Ciphertext）字母。最后对应维吉尼亚方阵（Vigenere Square）中最左侧的列，即为明文（Plaintext）字母。

**例：**我们将解密使用关键字（Keyword）：**giovan**，编码的密文“ZPSPNOXMOFAORMQDPUKZ”。 我们首先生成密钥流。

Picture

# 图5 解密密钥流

# Picture Picture

# 图6 解密操作

继续这一操作，我们最后能得到明文“the unbreakable cipher”。

# Picture

# 图7 解密后的明文

**题目要求：**

本题要求实现维吉尼亚密码（Vigenere Cipher）中的加密与解密操作。其中，使用图1的维吉尼亚方阵。

**数据格式：**

明文与关键字为小写字母，密文为大写字母。

**输入：**

明文（Plaintext）为：thisisanadditionalquestionforcprogramming

关键字（Keyword）为：hitsz

**输出：**

明文

关键字

密钥流（Keystream）

密文（Ciphertext）

密文经过解密后的明文