

期中复习之一——模拟(2)

模拟题一般是比较复杂，但思路比较清晰，就是按照题意一步一步操作就行，但是要细心，把所有情况都要考虑到位。

Vigenère 密码 P1079

题目描述

16 世纪法国外交家 Blaise de Vigenère 设计了一种多表密码加密算法 Vigenère 密码。Vigenère 密码的加密解密算法简单易用，且破译难度比较高，曾在美国南北战争中为南军所广泛使用。

在密码学中，我们称需要加密的信息为明文，用 M 表示；称加密后的信息为密文，用 C 表示；而密钥是一种参数，是将明文转换为密文或将密文转换为明文的算法中输入的数据，记为 k 。在 Vigenère 密码中，密钥 k 是一个字母串， $k = k_1, k_2, \dots, k_n$ 。当明文 $M = m_1, m_2, \dots, m_n$ 时，得到的密文 $C = c_1, c_2, \dots, c_n$ ，其中 $c_i = m_i \circledast k_i$ ，运算 \circledast 的规则如下表所示：

⊗	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenère 加密在操作时需要注意：

1. \circledast 运算忽略参与运算的字母的大小写，并保持字母在明文 M 中的大小写形式；
2. 当明文 M 的长度大于密钥 k 的长度时，将密钥 k 重复使用。

例如，明文 $M = \text{Helloworld}$ ，密钥 $k = \text{abc}$ 时，密文 $C = \text{Hfnlpyosnd}$ 。

明文	H	e	l	l	o	w	o	r	l	d
密钥	a	b	c	a	b	c	a	b	c	a
密文	H	f	n	l	p	y	o	s	n	d

输入格式

共 2 行。

第一行为一个字符串，表示密钥 k ，长度不超过 100，其中仅包含大小写字母。

第二行为一个字符串，表示经加密后的密文，长度不超过 1000，其中仅包含大小写字母。

输出格式

一个字符串，表示输入密钥和密文所对应的明文。

样例 #1

样例输入 #1

```
1 CompleteVictory
2 Yvqgpxaimmklongzfwpxmniytm
```

样例输出 #1

```
1 wherethereisawillthereisaway
```

提示

对于 100% 的数据，输入的密钥的长度不超过 100，输入的密文的长度不超过 1000，且都仅包含英文字母。

NOIP 2012 提高组 第一天 第一题

代码：

```
1  #include <stdio.h>
2  #include <string.h>
3  #include <stdlib.h>
4  char word[1005];
5  char key[105];
6  char ans[1005];
7  char* translate(char* key,char* word);
8
9  int main()
10 {
11     char* str;
12     scanf("%s",key);
13     scanf("%s",word);
14
15     str = translate(key,word);
16     printf("%s",str);
17     return 0;
18
19 }
20 char* translate(char* key,char* word)
21 {
22     int len1,len2;
```

```

23     char* str = (char*)malloc(sizeof(char)*1005);
24     int i,j=0;
25     len1 = strlen(key);
26     len2 = strlen(word);
27
28     for(i=0;i<len2;i++){
29         if(*(word+i)>='A'&&*(word+i)<='Z'){
30             if(*(key+j)<='z' && *(key+j)>='a'){
31                 *(str+i)= 'A'+ (*(word+i)-'A'-(*(key+j)-'a')+26)%26;
32             }
33             else{
34                 *(str+i)= 'A'+ (*(word+i)-'A'-(*(key+j)-'A')+26)%26;
35             }
36         }
37         else{
38             if(*(key+j)<='z' && *(key+j)>='a'){
39                 *(str+i)= 'a'+ (*(word+i)-'a'-(*(key+j)-'a')+26)%26;
40             }
41             else{
42                 *(str+i)= 'a'+ (*(word+i)-'a'-(*(key+j)-'A')+26)%26;
43             }
44         }
45         j = (j+1) % len1;
46     }
47     return str;
48 }

```