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):

	Α	В	С	D	Е	F	G	Н	ı	J	K	L	М	N	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z
Α	Α	В	С	D	Ε	F	G	Н	Τ	J	K	L	М	N	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z
В	В	С	D	Ε	F	G	Н	1	J	Κ	L	М	N	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α
C	С	D	Ε	F	G	Н	1	J	Κ	L	М	Ν	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В
D	D	Е	F	G	Н	1	J	K	L	М	N	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	С
Ε	Ε	F	G	Н	1	J	Κ	L	М	Ν	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	С	D
F	F	G	Н	1	J	K	L	М	N	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	C	D	Е
G	G	Н	1	J	K	L	М	N	0	Ρ	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	С	D	Ε	F
Н	Н	1	J	Κ	L	М	N	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	С	D	Е	F	G
-	1	J	K	L	М	Ν	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	С	D	Е	F	G	Н
J	J	K	L	М	N	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	С	D	Е	F	G	Н	1
K	Κ	L	М	N	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	С	D	Ε	F	G	Н	1	J
L	L	М	N	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	С	D	Е	F	G	Н	1	J	K
М	М	Ν	0	Р	Q	R	S	Т	U	V	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	ı	J	K	L
Ν	N	0	Р	Q	R	S	Т	U	٧	W	X	Υ	Z	Α	В	С	D	Е	F	G	Н	1	J	K	L	М
0	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	С	D	Ε	F	G	Н	1	J	K	L	М	N
Р	P	Q	R	S	Т	U	V	W	X	Υ	Z	Α	В	С	D	Е	F	G	Н	ı	J	K	L	М	N	0
Q	Q	R	S	Т	U	V	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	١	J	K	L	М	N	0	Р
R	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	С	D	Е	F	G	Н	ı	J	K	L	М	Ν	0	Р	Q
S	S	Т	U	V	W	Х	Υ	Z	Α	В	С	D	Ε	F	G	Н	ı	J	K	L	М	N	0	Р	Q	R
Т	Т	U	٧	W	X	Υ	Z	Α	В	С	D	Е	F	G	Н	١	J	K	L	М	N	0	Р	Q	R	S
U	U	V	W	Χ	Υ	Z	Α	В	С	D	Ε	F	G	Н	ı	J	K	L	М	N	0	Р	Q	R	S	Т
V	V	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	ı	J	K	L	М	N	0	Р	Q	R	S	Т	U
W	W	Χ	Υ	Z	Α	В	С	D	Ε	F	G	Н	1	J	K	L	М	N	0	Р	Q	R	S	Т	U	V
X	X	Υ	Z	Α	В	C	D	Е	F	G	Н	-	J	K	L	M	N	0	Р	Q	R	S	Т	U	٧	W
Υ	Υ	Z	Α	В	С	D	E	F	G	Н	1	J	K	L	М	N	0	Р	Q	R	S	Τ	U	٧	W	Χ
Z	Z	Α	В	С	D	Е	F	G	Н		J	K	L	M	N	0	Р	Q	R	S	Т	U	V	W	X	Υ

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的形式(其中 C 表示密文,P 表示明文,K 表示关键词(Keyword),1 为关键词的长度):

$C_i = (P_i + k_{i \bmod l}) \bmod 26$

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**。

Plaintext	а	s	i	m	р	1	e	w	×	а	m	р	1	e
Keystream	b	а	t	t	i	s	t	а	b	а	t	t	i	s

图 2 加密密钥流

P	P	1	ain	tex	t		ſ	а	s	T	i	r	n	р	П	ı	1	e	е	I	X		а	n	n	р	Τ	ı		e
		Ke	yst	rea	m		t	b	а		t	1	t	i		s	1	t	а	T	b	-	а	t		t	T	i	s	
	_				- [- 1				. 1	.,							Τ,			. 1					,] ,		_		_
A	A	В	C	_	E	_	G	H		_	K	L	M	N	-	_	_	-	-		T		-	W	-	-	Y :			
В	_	-	D	_	-		Н			_	_	M			_	_	-	2 9	-	_	U	_	_	-	-	1 2	-	_		
C	-	0	E	-	-	H		:+	_	_	M	\rightarrow	0	_	-	R	-	-	_	U	_	_	-	_	+	_	_	_		
_	_	D		_	H	_	1	_	K L M	-	_	O	-	_	+	-	1	_		_	-	_	_	-	+	_	_	-		
D	-	E	F	-	н	-	-	-		-	\rightarrow	_		•		-	-				-	X	-	-	-	-	-	С		
E	-	F	G	Н		_	-	-				P								W :			-	-	+	-	0 1	_		
F	-	-	Н	1	_			_	N (Q			-	-	-	/ V	_	-	Y		-	-	-	-	_	E		
G	_	Н	E	_	_	LI	-	-	_	-	Q	\rightarrow	S	_	-	-	V	-	-	_	_	Α	-	-	+	_	-	F		
Н	Н	1	J	**	LI		_	0		Q		S				W			_	_	A	_	-	-	-	1	-	G		
1	1	J	К	_			_	_	Q		\rightarrow					/ X	-	-	-	A	-	_	-	-	+	-	-	Н		
J	J	K	-	-	-	-	_	•	-	_	_	_	-	W	-	-	+-	-			C				+	-	1	1		
K	-			N	_	_			S					X				I		CI				+	H	1	1	_		
L	L	M	N	0	P	Q	R	S	T	U	٧	W	X	Υ	Z	A	E	3 (0	D	E	F	G	Н	1	١.	1	K		
M	M	N	0	P	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	(1)	E I	F	G	Н	1	J	1	K	L		
N	N	0	Р	Q	R	S	Т	U	V١	N	Х	Υ	Z	Α	В	C	E) I		F	G	Н	1	J	H	(LP	VI		
0	0	P	Q	R	S	T	U	V	N	X	Υ	Z	Α	В	C	D	E	1	=	G	н	ı	J	K	L	. 1	1	N		
P	P	Q	R	S	T	י ט	٧I	N	X '	Y	Z	Α	В	C	D	E	F		3	Н	ı	J	K	L	N	1	V C	0		
Q	Q	R	S	T	U	٧V	N	X	Υ :	z	Α	В	C	D	E	F	0	i I	1	1	J	ĸ	L	M	N	1 (0	Р		
R	R	S	Т	U	٧V	N	x	Y	Z	A	В	c	D	E	F	G	Н	1		J	к	L	M	N	C)	P (Q		
S	s	Т	υ	V	w	X	Y	z .	A	В	С	D	E	F	G	Н	1		1	K	LI	M	N	0	F) (2	R		
T	Т	U	ν	w	x	Υ :	\rightarrow	-	_		\rightarrow	\rightarrow	F	G		_	J	1	(_	и	_	-	Р	C	_	R	_		
U	U	v	w	x	Y	_	-	-	CI	\rightarrow	\rightarrow	F	G	_	-	-	H	-	-	M I	-	-	-		-	•	-	_		
V	+-	w	х	_	-	_	-	-	_	\rightarrow	\rightarrow	G	-	_	-	-	-	-	-	N (_	-	-	R	+	1	-	-		
	w	x	Y	_	_	_	_	D	_		G		1	J	-					0					-	_	,	_		
X	-		z	_	-	_	-	_	F		н	1	i	K	-	M				P (+	-	/ \	_		
Y	_	7	A	\rightarrow	C	_	_	-	GI	-	1		K	_	M	+	_	0 1	-	Q	-	-	-		+	-	V	_		
Z	-	Δ	В	\rightarrow		_	-	G	_	-	-	_		М		-	F	-	2		S			V	-	-	-	Y		
	12	A	О	·	U	_	'	u		•	,	n	L	IVI	IN	U	1,	1	4	A .	,	•	Lu	V	V	v 1	٠.			

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:

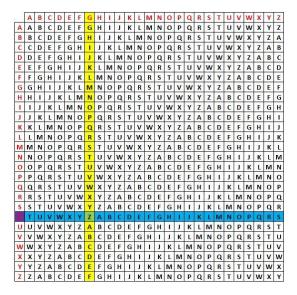
$P_i = (C_i - k_{i \bmod l}) \bmod 26$

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。

Ciphertext	Z	Р	S	Р	N	0	Х	M	0	F	Α	0	R	М	Q	D	Р	U	K	Z
Keystream	g	i	0	٧	а	n	g	i	0	٧	а	n	g	i	0	٧	a	n	g	i

图 5 解密密钥流



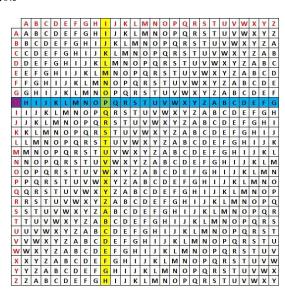


图 6 解密操作

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

Ciphertext	Z	P	S	P	N	0	Χ	M	0	F	Α	0	R	M	Q	D	P	U	K	Z
Keystream	g	i	0	٧	а	n	g	i	0	٧	а	n	g	i	0	٧	а	n	g	i
Plaintext	t	h	е	u	n	b	r	e	а	k	а	b	1	e	С	i	р	h	e	r

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: this is an additional question for cprogramming

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