

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, 并且在很长一段时期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):

	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

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语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), l 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	a	s	i	m	p	l	e	e	x	a	m	p	l	e
Keystream	b	a	t	t	i	s	t	a	b	a	t	t	i	s

图 2 加密密钥流

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

Ciphertext	Z	P	S	P	N	O	X	M	O	F	A	O	R	M	Q	D	P	U	K	Z
Keystream	g	i	o	v	a	n	g	i	o	v	a	n	g	i	o	v	a	n	g	i
Plaintext	t	h	e	u	n	b	r	e	a	k	a	b	l	e	c	i	p	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: thisisanadditionalquestionforprogramming

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