4. Vigenère Cipher

Vigenère Cipher เป็นวิธีการเข้ารหัสข้อความที่ประกอบด้วยตัวอักษร โดยใช้รูปแบบการเข้ารหัสแบบ polyalphabetic substitution อย่างง่าย ๆ Polyalphabetic Cipher หมายถึง การเข้ารหัสที่ใช้การแทนที่ตัวอักษร โดยใช้อักษรแทนหลายชุด การเข้ารหัสข้อความต้นฉบับจะทำโดยใช้ตาราง Vigenère

สำหรับปัญหานี้ใช้ตาราง Vigenère ที่แสดงด้านล่างนี้

	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

ข้อความที่จะเข้ารหัสจะถูกป้อนตามด้วยคีย์การเข้ารหัส การจับคู่ระหว่างตัวอักษรในข้อความและตัวอักษรในคีย์ (key) จะให้ค่าดัชนีของแถว (row) และคอลัมน์ (column) ในตาราง Vigenère ตามลำดับ เพื่อค้นหาตัวอักษรที่เข้ารหัส ตัวอย่างเช่น หากข้อความที่ต้องการเข้ารหัสคือ “no pets” และคีย์ (key) คือ “dog”

ตัวอักษรตัวแรกของข้อความที่เข้ารหัสจะอยู่ที่ตำแหน่ง [d][n] หรือ q จากตารางด้านบน

ตัวอักษรที่เข้ารหัสตัวที่สองจะอยู่ที่ตำแหน่ง [o][o] หรือ c

ตัวอักษรที่เข้ารหัสตัวสามจะอยู่ที่ตำแหน่ง [g][p] หรือ v

ตัวอักษรที่เหลือในข้อความที่เข้ารหัส แสดงไว้ด้านล่าง

[d][e] ⟶ h

[o][t] ⟶ h

[g][s] ⟶ y

ดังนั้น ข้อความ “no pets” เมื่อเข้ารหัสด้วยวิธี Vigenère Cipher โดยมีคีย์ คือ “dog” จะได้ข้อความที่ถูกเข้ารหัส คือ “qc vhhy”

<u>โจทย์</u> เขียนโปรแกรมเพื่อเข้ารหัสข้อมูลนำเข้าที่ป้อนจากแป้นพิมพ์ โดยใช้รูปแบบการเข้ารหัสแบบ polyalphabetic substitution ด้วยตาราง Vigenère ที่กำหนดให้ข้างต้น

<u>ข้อมูลนำเข้า</u>

ข้อมูลนำเข้ามี 2 บรรทัด โดยป้อนจากแป้นพิมพ์ (keyboard)

บรรทัดที่ 1 ป้อนข้อความที่ต้องการเข้ารหัส โดยข้อความประกอบไปด้วยตัวอักขระ (character) ที่เป็นตัวอักษรภาษาอังกฤษตัวพิมพ์เล็ก และอักขระที่เป็นช่องว่าง (space) เท่านั้น และมีจำนวนตัวอักขระอย่างน้อย 1 ตัวอักษร

บรรทัดที่ 2 ป้อนคีย์ (key) โดยคีย์ประกอบไปด้วยตัวอักขระ (character) ที่เป็นตัวอักษรภาษาอังกฤษตัวพิมพ์เล็กเท่านั้น มีจำนวนตัวอักขระอย่างน้อย 1 ตัวอักษร

<u>ข้อมูลส่งออก</u>

ข้อมูลส่งออกมี 1 บรรทัด โดยแสดงข้อความที่ถูกเข้ารหัสแล้วทางจอแสดงผล

สำหรับช่องว่าง (space) จะไม่ถูกนำมาเข้ารหัส โดยช่องว่างจะปรากฏในตำแหน่งเดียวกันทั้งก่อนและหลังการเข้ารหัส

ตัวอย่างข้อมูลนำเข้า และข้อมูลส่งออก

ข้อมูลนำเข้า	ข้อมูลส่งออก
no pets dog	qc vhhy
do not repeat yourself zrtkp	cf gyi qviops phegrvep