Vigenere Cipher

Published by **Edward Clark** in **Java**

arrays cryptography loops strings

The **Vigenere Cipher** is a poly-alphabetic substitution cipher that uses a set of shift ciphers and a keyword.

One of the simplest ciphers is the Caesar/shift cipher, where each letter in the plaintext message is replaced by the letter a particular number of positions up, or downstream in the alphabet. Shift 1 Caesar cipher:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

The Vigenere table is generated by doing a shift-1 Caesar cipher as many times as the number of letters in the alphabet (English alphabet, for this challenge).

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	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	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	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	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	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	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	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	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	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E				

ProTip

Ctrl + Enter to check code.

Skip

English

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

To encipher the message, first, spaces and punctuation are removed to create the plaintext. All characters are transformed to uppercase to match the table:

```
message = "Soylent Green is people."
plaintext = "SOYLENTGREENISPEOPLE"
```

A keyword is chosen, in this case, "spoiler" and repeated as many times as necessary to match the length of the plaintext:

```
key = "SPOILERSPOILERSPOILE"
```

The last "r" is dropped as the plaintext length has been reached.

The plaintext and key are lined up. To encipher the 1st letter, a search is done across the *first row* to find the column of the plaintext letter, in this case `"S"`, in the *19th column*. Then a search is done down the *first column* to locate the row of the 1st key letter, in this case also `"S"`, in the *19th row*. The letter at the intersection between column 19 and row 19, `"K"`, will be the 1st letter in the ciphertext.

The 2nd plaintext letter `"O"` is at column 15, while the 2nd key letter `"P"` is at row 16. The letter at the intersection is `"D"`. And so on.

Plaintext	S	O	Y	L	E	N	T	G	R	E	E	N	I	S	P	E	O	P	L	E
Key	S	P	O	I	L	E	R	S	P	O	I	L	E	R	S	P	O	I	L	E
Ciphertext	K	D	M	T	P	R	K	Y	G	S	M	Y	M	J	H	T	C	X	W	I

Create a function that takes two strings: a message or ciphertext, and a keyword. Return the ciphertext if the input is a message, or the deciphered text (without spaces or punctuation) if the input is in ciphertext.

Examples

```
vigenere("Soylent Green is people.", "spoiler"
vigenere("Darth Vader is Luke's father.", "spo
vigenere("HMRSSAIEKLSAXQILCCAC", "python") → "
```

Notes

N/A

SUGGEST EDIT