Autokey

In cryptography, the **autokey cipher** (also known as the **autoclave cipher**) is one of the classic methods to encode and decode text messages. The cipher uses a polyalphabetic substitution that replaces letters on the basis of several alphabetic series. To do so, a table is used in which each row shifts the letters of the alphabet one position to the left.

	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

To encode a given text message, all characters that are not letters are removed from the message at the start of the encoding procedure. We then choose a keyword that only contains letters, for example WATER, and append the message (restricted to letters only) to it. So if the keyword is WATER and the message is "MEET ME AT THE FOUNTAIN" , the keyword becomes WATERMEETMEATTHEFOUNTAIN. The message and the key are then written on top of each other.

```
 plaintext:  MEETMEATTHEFOUNTAIN
   keyword:  WATERMEETMEATTHEFOU
             -------------------
ciphertext:  IEXXDQEXMTIFHNUXFWH
```

We then look up each letter of the plain text in the vertical alphabet of the table and the letter at the corresponding position in the keyword in the horizontal alphabet. The encrypted letter is found at the corresponding position in the table.

In order to decrypt an encoded message (that only contains letters), we start with the original keyword that is extended letter by letter with the already decoded part of the message. This means that if a single error is made during decoding, the remainder of the decoded message will be wrong as well. This makes it extremely hard to decode messages that have been encoded by the autokey cipher without having the keyword at hand.

Assignment

- Write a function `substitute` that takes two single-letter arguments. The function must return the upper case letter that corresponds in the autokey table with the position of the first letter in the horizontal alphabet and the position of the second letter in the vertical alphabet. The function should be case insensitive with respect to the letters that are passed to the function.
- Write a function `encode` that encrypts a given text message t according to the autokey cipher with given keyword s that only contains letters. The text message t and the keyword s must be passed as arguments to the function. The function must return the encrypted text message.
- Write a function `decode` as the dual function of the function `encode`. This function must therefore decrypt a given text message t according to the autokey cipher with given keyword s that only contains letters. The encrypted text message t and the keyword s must be passed as arguments to the function. The function must return the decrypted text message.

Example

```
>>> substitute('M', 'K')
'W'
>>> substitute('e', 'I')
'M'
>>> substitute('E', 'l')
'P'

>>> encode('MEETMEATTHEFOUNTAIN', 'WATER')
'IEXXDQEXMTIFHNUXFWH'
>>> encode('And now for something completely different!', 'SHRUBBERY')
'SUUHPXJFPSBPRHDNBXUCYTELBRRARUUQIKIYR'

>>> decode('IEXXDQEXMTIFHNUXFWH', 'WATER')
'MEETMEATTHEFOUNTAIN'
>>> decode('SUUHPXJFPSBPRHDNBXUCYTELBRRARUUQIKIYR', 'SHRUBBERY')
'ANDNOWFORSOMETHINGCOMPLETELYDIFFERENT'
```

Het **autosleutelcijfer** (ook autoclavecijfer of autokeycijfer) is in de cryptografie één van de klassieke methoden om teksten te versleutelen. De versleuteling maakt gebruik van een polyalfabetische substitutie, waarbij letters worden vervangen aan de hand van verschillende alfabetische reeksen. Daarbij wordt een tabel gebruikt, waarin elk alfabet één letter verschoven is

	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