Myszkowski Cipher

http://www.scytale.xyz/ciphers/myszkowski/

Myszkowski ciphers are interesting transposition ciphers that use a code word to shuffle letters in a message.

Encrypting

The key to a Myszkowski cipher is a code word that has repeated letters in it. A memorable word, like TOMATO, might be used, but you could also make up a random code word, like AAFIFK

To encrypt a message, write your code word at the top of a grid. Beneath the codeword, write your message from left to right, moving down a column when you reach the end of a row.

For example, with code word TOMATO and message "WATCH OUT" (I've written the spaces as underscores below, so it's easier to see what's going on):

T	O	M	A	T	O
W	A	T	C	H	_
O	U	T	_	_	_

When you have written your entire message out beneath the codeword organise your columns so that your code word at the top is now in alphabetical order.

A	M	O	O	T	T
C	T	A	_	W	H
_	T	U	_	O	_

Now merge the columns that have matching code word letters:

A	M	O	T
C	T	A_	WH
_	T	U_	O_

Finally, read out your cipher text column by column; left to right. Don't forget to include the spaces: C_TTA_U_WHO_

Decrypting

To decrypt a message, write the code word at the top of a grid. To see how many rows your grid will need, divide the length of the cipher text by the length of the code word.

Now write your cipher text into your grid, filling up the columns in alphabetical order. When you fill up columns with repeated header letters, you'll have to fill all the repeated columns in simultaneously.