Encryption and decryption of a Vignère cipher

Overview. You will encrypt a short message using a Vignère cipher with a keyword of your choice. Then you'll decrypt someone else's Vignère-encrypted message.

Example. Let's encrypt the message "The dish ran away with the spoon" using the keyword "flange." To begin, we write our message on graph paper in lower-case letters (since it's plaintext) and write the keyword, repeated as many times as necessary, below it:

```
t h e d i s h r a n a w a y w i t h t h e s p o o n
F L A N G E F L A N G E F L A N G E F L A N G E F L
```

Now we encrypt each letter of the messsage using a shift cipher, but *each letter gets its own key* – namely, the letter directly below it. Using either the cipher disk or a Vignère table, we complete the encryption:

```
Y S E Q O W M C A A G A F J W V Z L Y S E F V S T Y
t h e d i s h r a n a w a y w i t h t h e s p o o n
F L A N G E F L A N G E F L A N G E F L A N G E F L
```

The ciphertext of our message is `YSEQO WMCAA GAFJW VZLYS EFVST Y`. A recipient who knows the keyword can decrypt this without difficulty. Without the keyword, it's rather more difficult to recover the plaintext.

Things to do:

1. Compose a message of about twenty-five letters, choose a keyword, and encrypt your message as in the example above. Write your ciphertext and your keyword on an index card.
2. When you receive an index card from another group, decrypt the message on the card. For decryption, it will probably be easiest to write the keyword (repeated as many times as necessary) *above* the ciphertext, so that you can fill in the plaintext below the ciphertext.