

Suppose Alice and Bob decide to communicate using the Substitution Cipher. However, they decide that it's too cumbersome for them to use a fully random permutation of the alphabet as their key. So they instead agree that they will use keys of the form (ℓ, w) , where ℓ is a letter, and w is a word or phrase. Using ℓ and w they will then generate their permutation via the following procedure:

1. If any letters are repeated in w , then delete each occurrence subsequent to the first. Call the resulting string w' .
2. Begin to define the permutation π , such that $\pi(\ell)$ is the first letter of w' , π maps the letter after ℓ to the second letter of w' , and so on.
3. Let w' have length n . Then the n^{th} letter after ℓ will be mapped by π to the first letter of the alphabet not used by w' . The $(n + 1)^{\text{th}}$ letter after ℓ is mapped by π to the second letter of the alphabet that is not used by w' , and so on.

So, for instance, if $(\ell, w) = (\mathbf{x}, \mathbf{holidays})$, then we would have the permutation:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ  
idaysbcefjgjkmpqrstuvwxyzhol
```

You are Eve, and you have intercepted a ciphertext that Alice sent to Bob. Determine the key that Alice and Bob are using, and decipher their message.

Note that each student in the course will have a different ciphertext to decrypt, so you'll need to tell me which one is yours when you turn in your solution (which only needs to be the key that Alice and Bob are using).

Copies of the ciphertexts are available on the course website. There is also a web-based utility that you might find helpful. As an example, ciphertext number 00 was encrypted using the key $(\mathbf{x}, \mathbf{holidays})$.