**Substitution**

**Background**

In a substitution cipher, we “encrypt” (i.e., conceal in a reversible way) a message by replacing every letter with another letter. To do so, we use a key: in this case, a mapping of each of the letters of the alphabet to the letter it should correspond to when we encrypt it. To “decrypt” the message, the receiver of the message would need to know the key, so that they can reverse the process: translating the encrypt text (generally called ciphertext) back into the original message (generally called plaintext).

A key, for example, might be the string NQXPOMAFTRHLZGECYJIUWSKDVB. This 26-character key means that A (the first letter of the alphabet) should be converted into N (the first character of the key), B (the second letter of the alphabet) should be converted into Q (the second character of the key), and so forth.

A message like HELLO, then, would be encrypted as FOLLE, replacing each of the letters according to the mapping determined by the key.

**Implementation Details:**

The program I wrote is called substitution. It enables you to encrypt messages using a substitution cipher. At the time the user executes the program, they should decide, by providing a command-line argument, on what the key should be in the secret message they’ll provide at runtime.

Here are a few examples of how the program might work. For example, if the user inputs a key of YTNSHKVEFXRBAUQZCLWDMIPGJO and a plaintext of HELLO:

A picture containing logo

Description automatically generated

Here’s how the program might work if the user provides a key of VCHPRZGJNTLSKFBDQWAXEUYMOI and a plaintext of hello, world:

Text

Description automatically generated