Let’s Play Scrabble! (part 1)
by madness

Here is a little toy cipher that can be done with pen and paper, or with Scrabble™ tiles. It is a substitution cipher in which the alphabet is shuffled after each character is encrypted or decrypted. Like a monoalphabetic substitution cipher, we start with a key that is an ordering of the 26 letters. But unlike a monoalphabetic cipher, the key is altered after each character is encrypted.

Choosing a key

First, we start with an alphabet (the key). The alphabet will be used in the substitutions as we encrypt or decrypt a message. We have several choices on how to choose an alphabet. Here are four of them:

1. An alphabet based on a keyword

In this case, we simply take a keyword and follow it by the remaining letters of the usual English alphabet. For example, if our keyword is KEYWORD, then the keyed alphabet is

```
KEYWORDABCFGHIJLMNPQSTUVXZ
```

If there are repeating letters in the keyword, we drop all but the first occurrence. So if the keyword is INFINITY, we would drop the second N, and all but the first I, to get INFTY. The keyed alphabet is

```
INFTYABCDEGHJKLMOPQRSUVWXZ
```

2. Shuffling the alphabet based on a keyword

In this case, we begin with the standard alphabet,

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

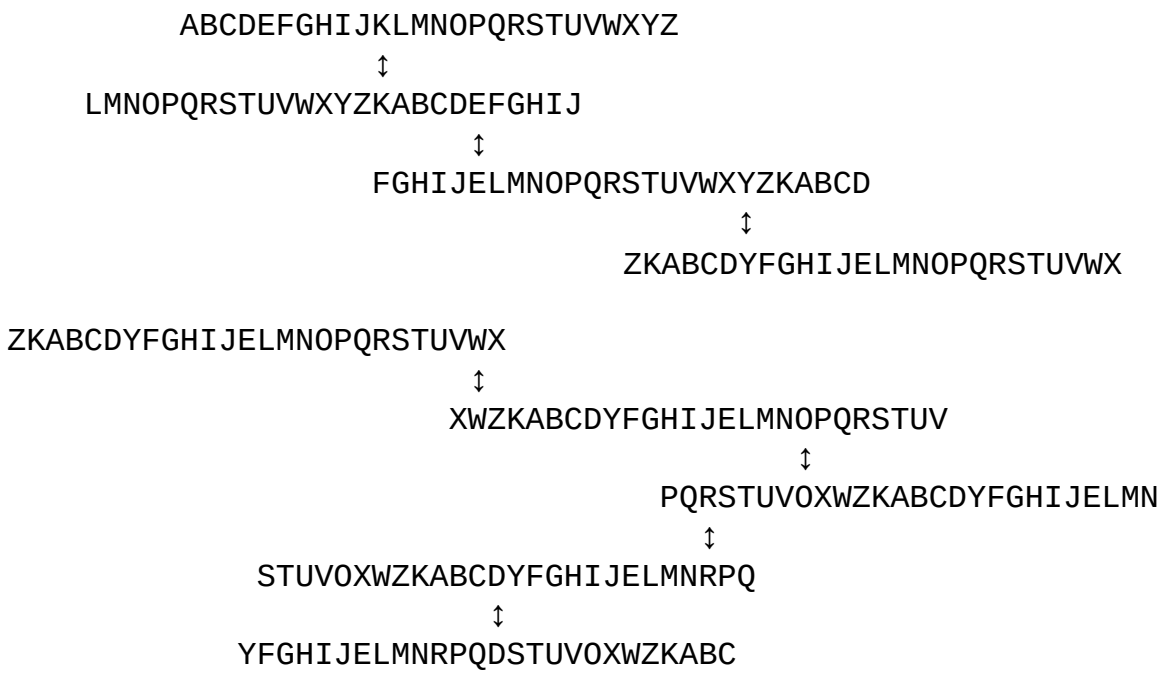
and a keyword. For example, let’s use KEYWORD. For each letter in the keyword, we do a shuffling step that swaps the letters before and after our key letter. If there are no letters in one of those groups, we just do the swap anyway, with one set being empty. So, we start with the standard alphabet and swap around K:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
                ↕
LMNOPQRSTUVWXYZKABCDEFGHIJ
```

Then we take the result and apply a swap around the next key letter, E:

```
LMNOPQRSTUVWXYZKABCDEFGHIJ
                ↕
FGHIJELMNOPQRSTUVWXYZKABCD
```

To belabor the point, here is the full shuffling using KEYWORD:



The final alphabet of this process becomes the initial alphabet of the encryption or decryption.

3. Shuffling an alphabet based on a keyword

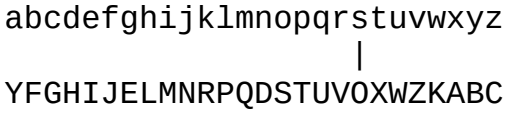
Start with a keyed alphabet as in (1), and shuffle it with another keyword as in (2).

4. A randomly generated alphabet

We could use a randomly generated alphabet as the key for the cipher. Of course, the person decrypting must know this key in order to decrypt.

Description of the cipher

The encryption process employs the same shuffling step as we used above in creating type 2 keys. For each character of the plaintext, a substitution is made, and then a shuffling. Each shuffling is swapping the block of letters before the plaintext character with the block of letters after it. As an example, suppose we want to use the key/alphabet from (2) above and encrypt the message “send help”. First, find the substitution for “s”:



We get an “O”. Next, shuffle the alphabet around the letter S:

```
YFGHIJELMNRPQDSTUVOXWZKABC
          ↕
TUVOXWZKABCSYFGHIJELMNRPQD
```

This new alphabet will be used to encrypt the next letter of the message.

```
abcdefghijklmnopqrstuvwxyz
    |
TUVOXWZKABCSYFGHIJELMNRPQD
```

We get “X”. Another shuffling, this time around the plaintext letter “e”:

```
TUVOXWZKABCSYFGHIJELMNRPQD
          ↕
LMNRPQDETUVOXWZKABCSYFGHIJ
```

This continues until the entire message is encrypted.

```
sendhelp
OXWDZMSA
```

The challenge

The following ciphertext was encrypted with a key that was created by using method 2. The flag is contained in the plaintext and takes the form “FLAG-” followed by a series of digits. For example, if you see

```
FLAGHYPHENONETWOTHREEFOURFIVESIXSEVEN
```

then you would report the flag to be

```
FLAG-1234567
```

The ciphertext:

```
TQSBAODTTABMRUHDKNVUORAKATOZLFBFDWPHQLANSZIKOSEDESXZLDYEUBJRROAVZRBSL
WESCEGGOCEMLFMAHAYSRNMCXATHGNZQBCLSCEMKIVELCRXCJTBBTXGBRNDQTLJMLUOEQW
THWVBAZHAABXPZELKBNWSNCZLNSBELFFKDLVFWOWNDQWMLFXEQWAQOQRIAAVSXAADYEUU
AMTHYLSCVILMNE
```