**USC UPSTATE**

**CSCI 455: Computer Security**

**Spring 2019**

**Lab 2**

**Problem 1**

Suppose that the Shift Cipher is modified so that for *each* letter of the message, a fresh random key is chosen and applied to shift just that letter.

1. Implement the modified scheme using any programming language of your choice.
2. Suppose that FJAV is the ciphertext of a *common English word* produced by the modified Shift Cipher, but the secret key is unknown. What could its plaintext be? Output as many “meaningful” plaintexts as you can (you need to print out the keys you use to generate the plaintext as well) using the program you developed in part a).
3. Does the resulting scheme satisfy Shannon’s notion of perfect secrecy? Justify your answer. What are the drawbacks of the modified scheme? (**Hint**: Compare the resulting scheme with the *one-time pad* scheme.)

Yes. Even though the possibilities are all alphabetic, to decrypt the scheme produces too many meaningful results to try. The drawbacks are