CECS 378 Lab 1 - Symmetric Cryptography

60 points

Assignment Description. This assignment is designed to allow you to get some practice with cryptanalysis of substitution ciphers. Write a program that will attempt a brute-force decryption attack on an encrypted phase that uses the simple substitution cypher. The following encrypted quotations are provided for you to test out your code (and I will attempt to run and evaluate your program using these phrases). Your program *must* make an honest attempt at cracking the phrases–any pre-programming of the resulting phrases that will "match" when the program is run will result in zero points being assigned for the lab. You may use any programming language that you like for your submission, but I recommend using something that makes text manipulation easy, like *Python.*

```
1. fqjcb rwjwj vnjax bnkhj whxcq nawjv nfxdu mbvnu ujbbf nnc

2. oczmz vmzor jocdi bnojv dhvod igdaz admno ojbzo rcvot jprvi oviyv
   aozmo cvooj ziejt dojig toczr dnzno jahvi fdiyv xcdzq zoczn zxjiy

3. ejitp spawa qleji taiul rtwll rflrl laoat wsqqj atgac kthls iraoa
   twlpl qjatw jufrh lhuts qataq itats aittk stqfj cae

4. iyhqz ewqin azqej shayz niqbe aheum hnmnj jaqii yuexq ayqkn jbeuq
   iihed yzhni ifnun sayiz yudhe sqshu qesqa iluym qkque aqaqm oejjs
   hqzyu jdzqa diesh niznj jayzy uiqhq vayzq shsnj jejjz nshna hnmyt
   isnae sqfun dqzew qiead zevqi zhnjq shqze udqai jrmtq uishq ifnun
   siiqa suoij qqfni syyle iszhn bhmei squih nimnx hsead shqmr udquq
   uaqeu iisqe jshnj oihyy snaxs hqihe lsilu ymhni tyz
```

Additionally, you must write two smaller programs. The first will be a simple-substitution encrypter that will take in two arguments: an existing plain-text phrase and a key in the form of the modified alphabet. The second will be a decrypter for the same type of crypto and take in the encrypted phrase and the modified alphabet "key" as arguments.

Use the two smaller programs that you write to encrypt the following phrases. Make sure to provide me with the keys that you use and the resulting crypto phrase:

```
1. He who fights with monsters should look to it that he himself does
   not become a monster. And if you gaze long into an abyss, the abyss
   also gazes into you.

2. There is a theory which states that if ever anybody discovers
   exactly what the Universe is for and why it is here, it will
```

```
   instantly disappear and be replaced by something even more bizarre
   and inexplicable. There is another theory which states that this
   has already happened.

3. Whenever I find myself growing grim about the mouth; whenever it is
   a damp, drizzly November in my soul; whenever I find myself
   involuntarily pausing before coffin warehouses, and bringing up the
   rear of every funeral I meet; and especially whenever my hypos get
   such an upper hand of me, that it requires a strong moral principle
   to prevent me from deliberately stepping into the street, and
   methodically knocking people's hats off - then, I account it high
   time to get to sea as soon as I can.
```

Kudos if you can tell me who said these quotes without searching the Internet for them.

Deliverables. Submit your source code to Beachboard along with the decrypted phrases. *Do not compress your files for submission.* Make sure that all code is **commented** with your own explanations or it will not be graded and you will receive zero points for this lab.