Q1 Explanations:

1. What is the difference between *authorization* and *authentication*?
2. What is the difference between the following two authorization models: *access control list* and *capability model*.
3. What is the authorization model employed in the UNIX file system? Explain what each symbol means in the following "`ls -l`" output:

   ```
   -rwxrw-r-- 1   pepperpotts   staff  125   Mar 02 12:05   somefile.txt
   ```

Q2 Are mono-alphabetic ciphers secure against the following:

1. ciphertext only
2. known plaintext
3. chosen plaintext

attacks?

Programming Problem Implement in Python (2.7) a mono-alphabetic cipher. The input to the program should consist of two text files, as in:

```
python mac key plaintext
```

The file `key` should consist of the permutation of [26], that is, it should be a text file consisting of a comma-separated list of all the numbers in [26], without repetitions. For example:

```
3,15,1,2,..., 23
```

meaning that the first letter is mapped to the third; the second to the fifteenth, the third to the first, etc. Of course, the actual key file has no ellipsis (dots).

The second input file, `plaintext` consists of letters [a-z], lower case English alphabet, plus spaces. The spaces are not encrypted; only the letters are. The output of running the program should be a new file called `ciphertext` containing the mono-alphabetic encoding of plaintext according to the key.

Once you have a working program, add it to the file containing the answers to questions 1 and 2. Put the names of your team members on the file; each team member should submit his own copy of the final solution.