(/) MITx: 6.00x Introduction to Computer Science and Programming

Ankit_Aggarwal (/dashboard) ▾

Courseware (/courses/MITx/6.00x/2012_Fall/courseware) Course Info (/courses/MITx/6.00x/2012_Fall/info)

Textbook (/courses/MITx/6.00x/2012_Fall/book/0/) Discussion (/courses/MITx/6.00x/2012_Fall/discussion/forum)

Wiki (/courses/MITx/6.00x/2012_Fall/course_wiki) Progress (/courses/MITx/6.00x/2012_Fall/progress)

PROBLEM 2: DECRYPTION : 15.0 POINTS

Your friend, who is also taking 6.00x, is really excited about the program she wrote for Problem 1 of this problem set. She sends you emails, but they're all encrypted with the Caesar cipher!

If you know which shift key she is using, then decrypting her message is an easy task. If the string `message` is the encrypted message and `k` is the shift key she is using, then calling `applyShift(message, 26-k)` returns her original message. Do you see why?

The problem is, you don't know which shift key she is using. The good news is, you know your friend only speaks and writes English words. So if you can write a program to find the decoding that produces the maximum number of real English words, you can probably find the right decoding (there's always a chance that the shift may not be unique. Accounting for this would use statistical methods that we won't require of you.)

PSEUDOCODE

Right now, you should take time to write some pseudocode! Think about an algorithm you could use to solve this problem and write the steps down. Then, you can verify your algorithm with the supplied pseudocode in `ps5_pseudo.txt` before coding.

After you've done writing and checking your pseudocode, implement `findBestShift()`. This function takes a wordList and a sample of encrypted text and attempts to find the shift that encoded the text. A simple indication of whether or not the correct shift has been found is if most of the words obtained after a shift are valid words. Note that this only means that *most* of the words obtained are actual words. It is possible to have a message that can be decoded by two separate shifts into different sets of words. While there are various strategies for deciding between ambiguous decryptions, for this problem we are only looking for a simple solution.

To assist you in solving this problem, we have provided a helper function, `isWord(wordList, word)`. This simply determines if word is a valid word according to the wordList. This function ignores capitalization and punctuation.

Hints

Using string.split

You may find the function `string.split` useful for dividing the text up into words.

```
>>> 'Hello world!'.split('o')
['Hell', ' w', 'rld!']
>>> '6.00x is pretty fun'.split(' ')
['6.00x', 'is', 'pretty', 'fun']
```

Test Cases

```
>>> s = applyShift('Hello, world!', 8)
>>> s
'Pmttw, ewztl!'
>>> findBestShift(wordList, s)
18
>>> applyShift(s, 18)
'Hello, world!'
```

```
Hello, world.
```

```
import string

def findBestShift(wordList, text):
    """
    Finds a shift key that can decrypt the encoded text.

    text: string
    returns: 0 <= int < 26
    """
    ### TODO

```

Unsubmitted

Check Save *You have used 0 of 30 submissions*

Show Discussion New Post

Find Courses (/courses) About (/about) Blog (http://blog.edx.org/) Jobs (/jobs) Contact (/contact)

(http://youtube.com/user/edxonline) (https://plus.google.com/108235383044095082735)

(http://www.facebook.com/EdxOnline) (https://twitter.com/edXOnline)

terms of service (/tos) *privacy policy (/privacy)* *honor code (/honor)* *help (/help)*