

PROBLEM 2: DECRYPTION (15/15 points)

Your friend, who is also taking 6.00.1x, 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 `ps6_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](#)

[Test Cases](#)

```
1 def findBestShift(wordList, text):
2     """
3     Finds a shift key that can decrypt the encoded text.
4
5     text: string
6     returns: 0 <= int < 26
7     """
8     ### TODO
9     max_valid_words, best_shift = -1, -1
10    for shift in range(26):
11        decrypted_text = applyShift(text, shift)
12        for c in string.punctuation:
13            decrypted_text = decrypted_text.replace(c, ' ')
14        words = decrypted_text.split(' ')
15        valid_words = len([word for word in words if word.lower() in wordList])
16        if valid_words > max_valid_words:
```

Correct

Test results

[Hide output](#)

CORRECT

Test 1: findBestShift(<edX wordList>, 'TqxXa, iADxp!')

Output:

Test 2: findBestShift(<edX wordList>, 'The quiz is... haRd!')

Output:

Test 3: findBestShift(<edX wordList>, "Dro dokmrob'c xkwo sc DKlsdrK?")

Output:

Test 4: findBestShift(<edX wordList>, 'Jk, xqp pdana eo w PW jwiaz Whrej!')

Output:

Test 5: findBestShift(<edX wordList>, 'mzagzxodjI')

Output:

Test 6: findBestShift(<edX wordList>, 'ejgcr dGcp rWRkn ugpvGpeg PqvjKpI')

Output:

Test 7: findBestShift(<edX wordList>, 'tPnfxiFsF uibu tubUf qJqf qspqfS tbjmps')

Output:

Test 8: findBestShift(<edX wordList>, 'qbcmnfY QbCWbypyl qcHa gullCuay qLCmN guwbChyIS volh lyncLY qyUfnb uhmqyl')

Output:

6

Test 9: findBestShift(<edX wordList>, 'ojAlw caFyvge sDGfy sLljsulagf klsaf dahklauc kaj vsfywj kgjjgo escw ymwkk vjsY oggv sddGosfuw fWuwkKalq')

Output:

8

Test 10 (No valid shift available): findBestShift(<edX wordList>, 'smgsn Tphihm reEjgD')

Output:

0

[Hide output](#)

Check

Save

You have used 3 of 30 submissions

Show Discussion

 New Post



About (<https://www.edx.org/about-us>) Jobs (<https://www.edx.org/jobs>)
Press (<https://www.edx.org/press>) FAQ (<https://www.edx.org/student-faq>)
Contact (<https://www.edx.org/contact>)



EdX is a non-profit created by founding partners Harvard and MIT whose mission is to bring the best of higher education to students of all ages anywhere in the world, wherever there is Internet access. EdX's free online MOOCs are interactive and subjects include computer science, public health, and artificial intelligence.



(<http://www.meetup.com/YourMeetup>)



(<http://www.facebook.com/EdxOnline>)



(<https://twitter.com/YourPlatformTwitterAcco>)



(<https://plus.google.com/YourGooglePlusAcco>)



(<http://youtube.com/user/edxonline>)

© 2014 edX, some rights reserved.

Terms of Service and Honor Code -
Privacy Policy (<https://www.edx.org/edx-privacy-policy>)