Encryption non-PKE

Homework Assignment Overview

There are two tasks to complete for homework. The first task is to decode a message that was encoded using a simple shift/caesar cipher. The second task is to create your own simple code using a symmetric cipher that is something other than a simple shift/caesar cipher. You should attempt to create code for one of these tasks (if you can't get it working in a reasonable amount of time just submit what you have and then explain what you were trying/planning for it to do in code comments). For the other task, write a detailed explanation of the algorithm you would use to encode/decode..

File Types:

For written explanations: text, markdown or pdf files
We prefer if you submit the coding component as shared repl.it links in a document.
For code, these are the languages we are comfortable grading: **python, javascript, java, snap, scratch**

1) Decoding a Message

- The message was coded using a basic shift cipher (caesar cipher)
- Create some algorithm to attempt to decode the message
    - Try all 25 shift values with a sample test and print out the results.
    - Use letter frequency analysis to make educated guesses about the shift amount.

https://www3.nd.edu/~busiforc/handouts/cryptography/letterfrequencies.html

    - Look for common short words (Example: the word "the" is in the text over 50 times

https://www.espressoenglish.net/the-100-most-common-words-in-english/)

    -

Starter Code Options

Encoded Message with numbers, spaces and punctuation:
https://replit.com/@ajprado/Encoded-Message#main.py

Encoded Message with only letters (numbers, spaces, and punctuation removed)
https://replit.com/@ajprado/encoding-message-no-punctuation#main.py

2) Encoding a Message

- Select a symmetric cipher other than shift/caesar cipher.
- Create a program or design an algorithm to take a string and encode it using your method.
- Here are some possible options:
    - transposition: https://www.youtube.com/watch?v=sHsnH1u03e4 (just until 2:20)
      https://www.youtube.com/watch?v=bcyUJK1BvHw
    - substitution/cryptogram: https://www.youtube.com/watch?v=1P8Xpxm76e8 :
      https://cryptograms.puzzlebaron.com/play.php
    - playfair cipher: https://www.youtube.com/watch?v=quKhvu2tPy8
    - Any other type of cipher or encryption you are interested in, just explain it in the comments!

Check List (Rubric)

- ☐ There is either a program or detailed explanation for an algorithm to attempt to decode the message that was encoded using a basic caesar/shift cipher. (2 options for starter code)
- ☐ There is either a program or detailed explanation for an algorithm that encodes a string using some method other than the basic caesar/shift cipher.

- [ ] At least one of the two tasks was coded in one of the languages we can grade (python, javascript, java, snap, scratch), preferably as a repl.it link.
- [ ] Code is explained using comments for major components.
- [ ] Written algorithm is detailed and explains the step-by-step process from start to finish.
- [ ] Work is saved in your “encryption_non_pke” folder of your github for the class.