

Project 7: The Caesar Cipher

Please read and follow ALL the instructions in this handout.

This project counts as an individual project. But you make work with a partner of your choosing if you wish. You and your partner will submit one project together (with both names on it). Please complete this project using only your partner for help. You should not consult other students (in or out of the class), tutors, or other people. You may seek assistance from your class professor or the course assistant. Seeking help that is not permitted is considered a violation of our academic integrity code.

The purpose of this project is to practice our skills with strings and textfiles. There is no report with this project.

1 Overview

You will be a hacker for this project. Your goal is to decipher a secret message. Fortunately you know that the message was created using the a shift cipher. Recall the Caesar Cipher is a shift cipher with a key (shift) of 3. However, you do not know the key that was used to encode the message. You will have to discover the correct key, use it to recover the secret message, and then do some research to find out who wrote that message.

In order to decode the message, you will write a program that tries different keys to see what plaintext messages are produced. Each key will decode the secret message differently, but only the real key will result in a plaintext message that is legible; the rest will look like gibberish. In order to find the right key, you try different keys in your program to see which one works. Plaintext messages from the wrong key are mostly gibberish.

2 Project Outline

The project has the following primary parts.

1. Decode a secret message.
2. Encode a plain text message for your professor.

3 Functions to Write

Write the following functions in your program:

- `decode(cipher, key)`
The decode function has two parameters. The first is a string that is an encoded message. The second parameter is a key (integer). Your function will use the shift cipher with the indicated key to produce a plaintext message. Your function should return this plaintext message as a string.
- `encode(plain, key)`
The decode function has two parameters. The first is a string that is a regular plaintext message. The second parameter is a key (integer). Your function will use the shift cipher with the indicated key to produce a ciphertext message. Your function should return this ciphertext message as a string.
- `readFile(filename)`
This function has one parameter, a string indicating the file name. This function should open the file, read the entire file contents into a single string variable, close the file, then return the string.
- `main()`
This function calls all the others. See more details below. a single string variable, close the file, then return the string.

4 Operations in main()

Part 1:

To decode the secret message.

- Use your readfile command to open and read a file called `cipher.txt`. You must obtain this file from the professor. Do not edit or change this file. This is an encoded message using a secret key.
- Use a loop in your main program to try different keys. What is the range of valid keys to try?
- For each key, call your `decode()` function to produce a plaintext. Print the key and the plaintext for each possible key you try.
- Examine the output for different keys and find the one that is the correct key.
- **In the comment block at the top of your program, have a line that says 'key=x' where you replace x with the key you found.**
- **In the comment block at the top of your program, have a line that says 'source=x' where you replace x with the source of where the secret text comes from.** You might have to do a search on the text to see where it comes from if you do not recognize the source.

Part 2:

To encode a secret message.

- Use your readfile command to open and read a file called `plain.txt`. You must obtain this file from the professor. Do not edit or change this file.
- Use your encode function to encode this text **using the key=11**. You must use this key value.
- The **LAST THING** your program should print is the cipher text message you created in the above step.
- **In the comment block at the top of your program, have a line that says 'source=x' where you replace x with the source of where the plain text comes from.** You might have to do a search on the text to see where it comes from if you do not recognize the source.

You are to submit a program with all the required parts. Do not submit the text files. Be sure to follow the special commenting requests.