COSC 4343: Computer Security and Privacy

Assignment # 1: due on Tue. 9/07/2020 at 11:59 pm

Remaining late days may be used in this assignment if needed.
Check "Late Days" policy in syllabus for more details.

Question 1:

Write a Python program that encrypts and decrypts a text file using a modified version of Caesar cipher by shifting each letter in the plaintext by a given shift value n. Don't worry about punctuations or numbers or spaces for now, just work on the alphabet letters (lower case only). You will need two text files "plaintext.txt" and "ciphertext.txt".

Your program should display the following menu:

1- Encrypt
2- Decrypt
3- Break
4- Exit

In Option 1, Alice is trying to encrypt a message to Bob through an agreed secret key value n. Your program should ask for the key value n and then uses it to encrypt the contents of "plaintext.txt" and writes them in "ciphertext.txt".

In Option 2, Bob is trying to decrypt Alice's message. Your program should ask for the key value n and then uses it to decrypt the contents of "ciphertext.txt" and writes them in "plaintext.txt".

In Option 3, Trudy is trying to figure out the secret key value n so it can decrypt "ciphertext.txt". Trudy may choose to perform an exhaustive search to try all values of n, may use repetitive patterns such as "ing" and "the", or may use the "English Letter Frequency Count" to break into the encryption. Your program should use any or all of these methods to return the key used for encrypting "ciphertext.txt".

Option 4 should exit the program. Note that this is the only way you can exit the program, and the menu should be inserted in a loop that will always be displayed to the user until option 4 is chosen.

Question 2:

What is the topic of your special topic presentation that you will provide your own recorded presentation? Topics need to be in the field of computer security and privacy. List two topics under the comment section of this assignment, one as preferred topic and a second topic in case of conflict or disapproval of the first topic. Check the presentation schedule on Canvas under "assignments", which also contains more details about the presentation assignment.

<u>What to submit:</u> 3 files + 1 submission comment as follows:

1- "HW01-JohnSmith.py": This is your main Python program file. Your filename should be named in the format of HW01-FirstLastname.py. For example, if your name is John Smith, then your python program file should be "HW01-JohnSmith.py".
2- "plaintext.txt" and "ciphertext.txt": These files are the input/output text files that your Python program will use.
3- The comment is for your listing of two presentation topics (preferred and backup).

<u>Submission instructions:</u>

1- Make sure that your Python program is written in Python 3.X version and runs well on Mac OSX terminal (command line) using python3 command prompt.
2- Make sure that your Python program is well tested and runs without any errors or warnings. Include in your submission the Python source code and any text files you may use.
3- Make sure your program is not using built-in functions that solve the major required components of the assignment, in which it may defeat the purpose of the assignment. When in doubt, ask me.
4- Clean up your code and remove any unnecessary code segments.
5- Add any necessary comments to explain some of your code segments.
6- Your program should be submitted through Canvas.
7- All your submission files (source code and .txt files) should be named exactly as specified in the instructions above: "HW01-JohnSmith.py", "plaintext.txt", and "ciphertext.txt".

<u>Grading: (Total points: 10 pts.)</u>

- (6 pts.): Program satisfies requirements and program components are functioning as expected.
- (2 pts.): Program is error free (no crashing), runs without any errors or warnings, and handles incorrect input appropriately without crashing the program.
- (1 pt.): Program is user friendly and easy to exchange input and output with the user.
- (1 pt.): Program contains comments explaining various sections of the source code.
- (-5 pts.): Program does not compile or run successfully.
- (-2 pts.): Program is not bulletproofed, i.e. does not handles input errors properly.
- (-2 pts.): Missing the submission of input & output files.
- (-1 pt.): Submitted files are not named according to instructions.
- (-1 pt.): Missing comments in program source code.
- (-1 pt.): Program menu does not loop or exits before instructed.

<u>Submission Checklist:</u>

Use this checklist to make sure your submission contains the following:

□ Source code with comments + the two input/output files
□ All source code and the input/output files are named as specified in the instructions
□ Program is bulletproof, that is, handles input errors properly without crashing
□ Program produces no errors or warnings when compiled or interpreted
□ Submission files tested using python3 command prompt
□ Submission files downloaded and checked for missing files

Always let me know if you have any questions or need more clarification on the assignment or submission instructions.

Good Luck ☺