Chann Makara Han
CSC 226 Final Projecyt: Scott Heggan
https://drive.google.com/drive/folders/1JHmh0moQ9ydTLVQc_xTv3gvNbiypI2vu?usp=sharing

MOTIVATION:

I am highly fascinated in security algorithm as I feel powerless in this modern era without strong background in what is going on behind the virtual world. This class introduce few topics on encryption and decryption algorithm and heavily on logical thinking still, so it is the closest think I could do for the final project that is related to cyber security.

I want to challenge myself to build an encryption and decryption algorithm that is extremely hard to hack or reverse engineer if the translation keys are not specifically given. This program will lead me into further creation of languages and imagination as well as understand one of the most complicated world we are living in and dependent on which eventually leads to one question: “What information do you know?”

PURPOSE:

The primary purpose of my project is to create an encryption and decryption algorithm from the lessons I have learnt in class and minor research, and see how hard of an algorithm I can generate. Then, this algorithm can reuse in many application such as message, apps, and emailing sensitive information. The algorithm will includes class, dictionary, loop, and other important topics we covered in classes so I can show that I have learnt what my instructor has taught, and also able to learn by myself on other topics when needed. The result of my code will involve background algorithm running and interacting with user interface.

RESOURCES:

I mainly wrote the algorithm from scratch but based my idea on a8 assignment, CaesarCipher, and a7 assignment using dictionary. Other sources are chapter 16 about Tkinter and stackoverflow. I also watched Youtube on how to use tkinter text boxes and labels.

From a8, I took the idea of the __init__ for my main class HancSecurity, so I have the same parameter as CaesarCipher. Dr. Scott Heggan is the producer or owner of CaeserCipher original codes.

I also got some idea from wikipedia on how to generate Affine cipher, which I modified and implement a little part from in on my dictionary. https://en.wikipedia.org/wiki/Affine_cipher

The last sources is youtube. I watched how to use tkinter from youtube by a channel named thenewboston. From here, I know how to use frame, labels, buttons, entry, and text. I also know a little bit on how to organize the layout. https://youtu.be/wNBqM28MMjs
FILES: https://github.com/hanchannmakara/csc101_project_hanc

INITIAL DESIGN PLAN:

We will complete this assignment by adding the following functions:

The original implementation of A8 included the following functions:

- `class CaesarCipher`
  - `alphabet`
  - `def import_file`
  - `def export_file`
  - `def encrypt`
  - `def decrypt`

Our implementation for the final project will include:

- Adding more complicated and irreversible translation for encrypting using classes
- Figure out how to crack the library made giving the encryption method, keep in mind the decryption is not simply the reverse method of the code
- Adding mathematics function into encrypting and decrypting

SUMMARY:

In order to start my project, I started with building dictionaries that can update itselfs keys and values. Started with one dictionary, called dict1, I converted each letter in the English alphabet into a specific values, from 1 to 26. In order for conveniences, I also created the second dictionary, called dict2, which reversed the keys and values of the original dictionary. For the values I got from dict1, I built in 26 equations, each will take in one value and two other variables from the user, word count and encryption/decryption key. These 26 equations then spitted out 26 news translation keys for a new dictionary, called dict3. Similarly, I also built a dictionary, called dict4, which reverse the keys and values of dict3.

From dict1, dict2, dict3, and dict4, I then created my encryption and decryption algorithm called encrypt and decrypt respectively. This is very challenging in the beginning because now I got all the keys and values I need, but I do not know how to convert them from one form to another yet. I looked at CaesarCipher and Affinity Cipher methods and jointed the two in a way that is unique to my code. The result is amazing. Now, I got my encryption and decryption dictionary that works very well and reusable in many application. The proceeding step is to use these algorithm in a class I called HancSecurity, so I can call the functions and other properties needed to interact with user conditions.

Finally, I used tkinter to build a frame and allow users to input key, encryption type, and their intended messages, and I extracted their information to evaluate and perform either encryption or decryption accordingly. Lastly, I returned the result to the tkinter screen. I spended over three days on this whole project from making plan, thinking of the steps, and actually writing the codes. I would say, I have implemented my initial plan mentioned above very vell.

INSTRUCTIONS:

My program is very user-friendly and fast. First, user will enter the key they want to use for crypting their message, the type of encryption/decryption they want and then type the message in the boxes provided with clear labels. When they think they are done, just pless the crypting button, and the result will appear almost instantly in the text box below. If they want to check whether the program works correctly, just copy the resulting message, and change the encryption type they initially put, and pless crypting again to see if they have the initial message coming out.

ERRORS:

1. My code cannot takes large value key like greater than 100 if the messages are long
2. Entered key needed needed to be integer
3. I have not implement method to export data into text.txt file yet

REFLECTION:

After completing this project, I felt very tired but pleasing because I have created the program I wanted to have and although it is not perfect and the ideal one, it is very close. I also felt motivated to working on security algorithm longer. Some difficulties such as reverse algorithm in decryption is very hard to figure out. I also have some difficulties with class and how to use it. Although I can use it and have used it, I am not very confident in it. I will work more on it.

Overall, this project is very challenging and inspiring. I like working on challenging topics like this because it teaches me a lot of things and builds my confidence as well as my coding experience. The program itselfs is not close to being perfect as what I wished but it is for now, as good as I have the energy for and the time limit. Thank you for allowing me to work on this topic and always be kind and supportive.

REFERENCES:

1. “*A8:CaesarCipher”* by Scott Heggan. Berea College Computer Science Department, CSC 226. Fall 2017.

In this one, I used the idea for the class parameters in my program.

2. *“Affinity Cipher”* by Wikipedia. https://en.wikipedia.org/wiki/Affine_cipher

This one, I used the idea of double translation.

3. “Tkinter” by Youtube. https://youtu.be/wNBqM28MMjs

This one, I learn how to use tkinter module to interact with use.