Cyber Security Interest Group

Lab sheet

**Classical Cipher Implementation**

**(Note: Unauthorized Hacking is Illegal!!)**

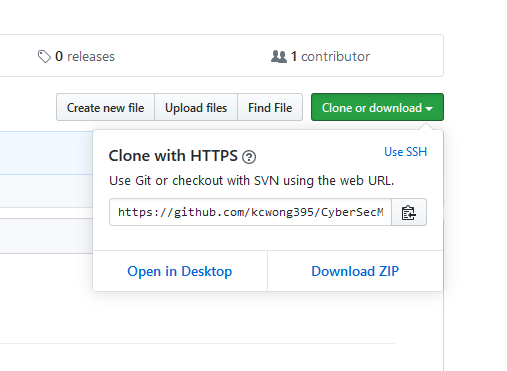
**About this Lab:**

In this lab, you will go through some simple python code to understand how classical cipher such as caesar cipher works.

As mentioned in the lecture, classical cipher is possible to break. The following examples demonstrate how bruteforce might work

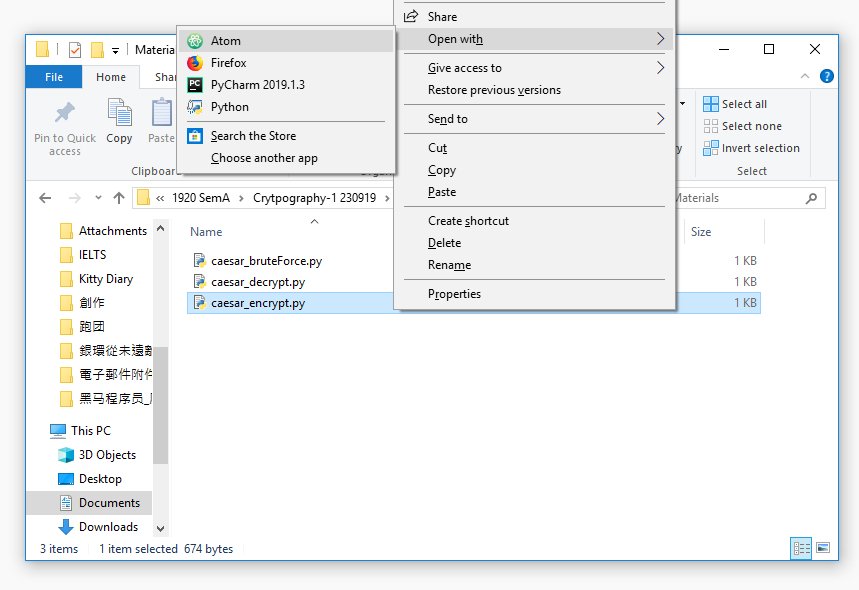
**Before the Lab:**

* Download Python from: <https://www.python.org/downloads/>
  + Choose the correct Operating System depends on your demand
* Download and install IDE or Word Editor
  + Here we use Atom from: <https://atom.io/>
* Download the materials from: <https://github.com/kcwong395/CyberSecMaterial>

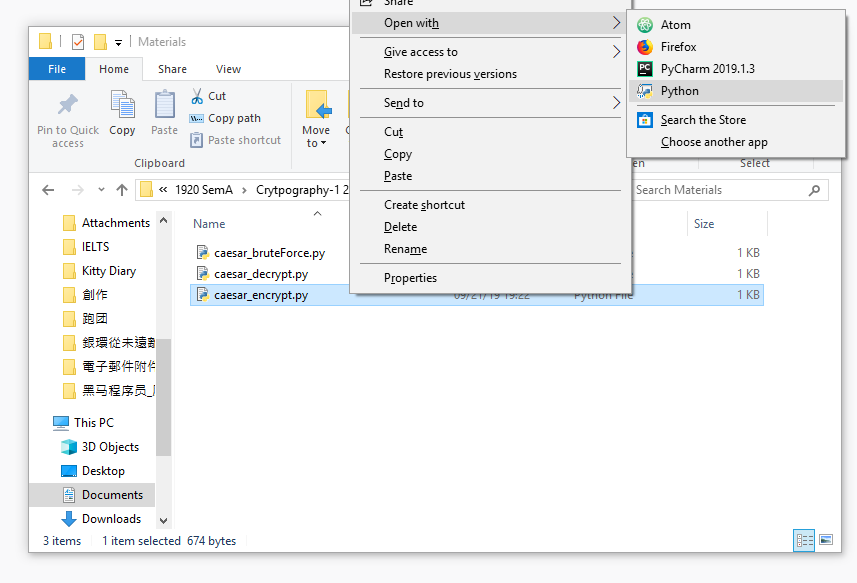


**Let’s do it:**

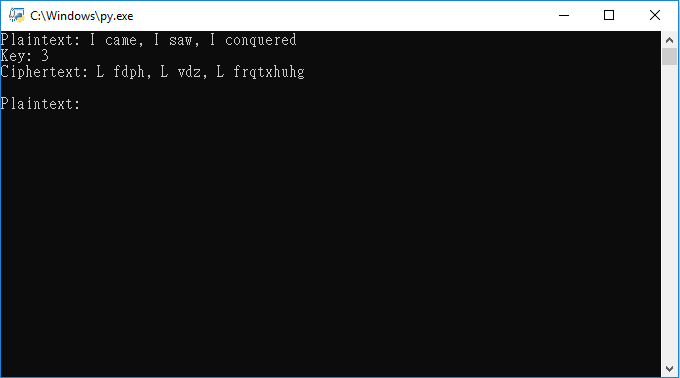
1. Open the download path, it should contain several files with .py extension.
2. Right click on caesar\_encrypt.py and open with Atom to see the file content



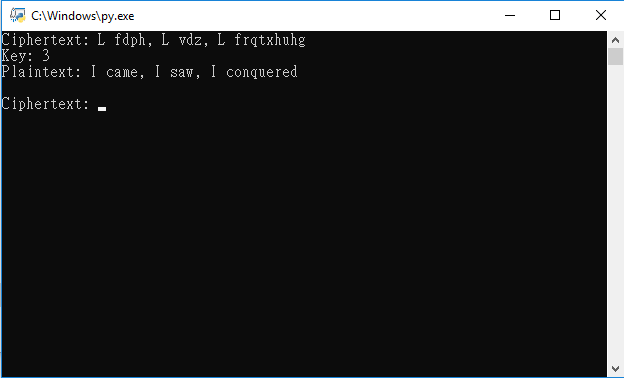
1. To run the code, right click on caesar\_encrypt.py and open with Python (or you can install some plugins to allow atom to do such task)



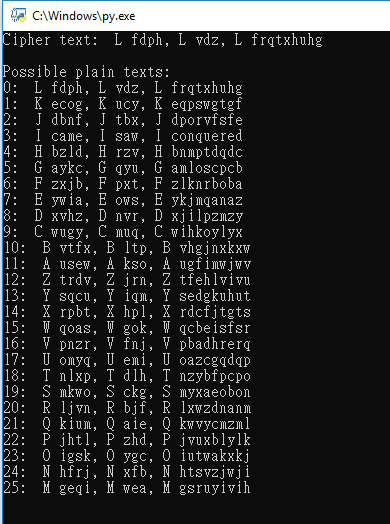
1. Input the plaintext, i.e. I came, I saw, I conquered
2. Input the key, i.e. 3
3. Observe the output ciphertext, does it fit your expectation?



1. Copy the ciphertext and open the caesar\_decrypt.py file
2. Input the received ciphertext in previous file, and the key 3
3. Can you retrieve the original plaintext?



1. Open the caesar\_bruteForce.py file and input the ciphertext again
2. Can you retrieve the original plaintext?



1. What if the key is larger than 25?

**Extra Questions:**

1. picoCTF 2018 Crypto Warmup 1

Crpyto can often be done by hand, here's a message you got from a friend, llkjmlmpadkkc with the key of thisisalilkey. Can you use this table to solve it?.

#### picoCTF 2018 caesar cipher 1

This is one of the older ciphers in the books, can you decrypt the [message](https://2018shell.picoctf.com/static/6b5626c0736d9090f5d98de74eec4543/ciphertext)?

1. picoCTF 2018 hertz

Here's another simple cipher for you where we made a bunch of substitutions. Can you decrypt it?

1. Those questions are too simple? Try this :D

Ciphertext: Q(Tw~m(Uiz|qv(ivl(Uiz|qv(tw~m(um

(don’t forget to modify the code from martin, it should be able to help you… maybe :D)

You can find all the materials in the materials folder and the answer will be discussed next week.

**Extension Reading:**

1. playfair cipher

<https://zh.wikipedia.org/wiki/%E6%B3%A2%E9%9B%B7%E8%B2%BB%E5%AF%86%E7%A2%BC>

1. rot13

<https://zh.wikipedia.org/wiki/ROT13>

1. Git Documentation:

<https://git-scm.com/doc>

1. Github User guides:

<https://guides.github.com/>

1. Python Tutorialspoint (very nice tutorial website):

<https://www.tutorialspoint.com/python/index.htm>

1. ASCII Table 😉:

<http://www.asciitable.com/>