Cyber Security Interest Group

Lab sheet

**Classical Cipher Implementation**

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

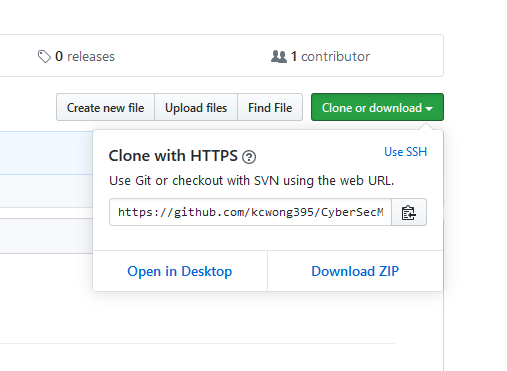
**About this Lab:**

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 or cryptanalysis 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
3. To run the code, right click on caesar\_encrypt.py and open with Python
4. Input the plaintext, i.e. I came, I saw, I conquered
5. Input the key, i.e. 3
6. Observe the output ciphertext, does it fit your expectation?
7. Copy the ciphertext and open the caesar\_decrypt.py file
8. Input the received ciphertext in previous file, and the key 3
9. Can you retrieve the original plaintext?
10. What if the key is larger than 25?

**Extension:**