Lab 10 Security (Python)

General Information

Equipment Borrowing

• Students should borrow the equipment from our teaching assistant at the beginning. To borrow the equipment, the student should give his/her student ID card to the teaching assistant and then the teaching assistant will lend the equipment to the student. At the end of the lab session, the student should return the equipment to the teaching assistant and get back his/her student ID card. In this lab, the equipment required is a notebook. Student can either borrow a notebook from the teaching assistant or use his/her own notebook.

Help Seeking

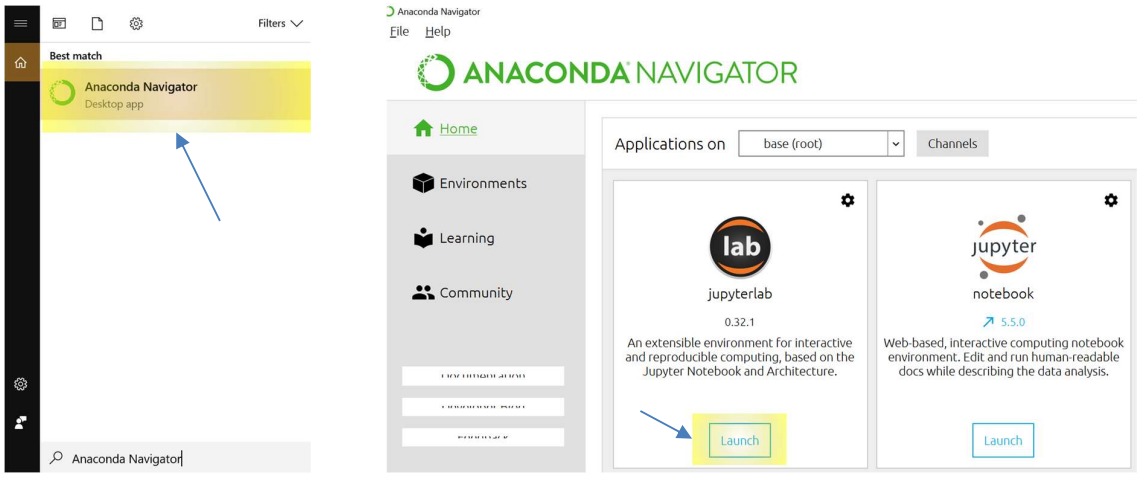
• At any time if you are lost or if you have any questions, feel free to ask the instructor, tutor, or teaching assistant and we will be very happy to help you.

Introduction

In this lab, your goal is to recover a secret message from its encryption in the file `topsecret.txt`. You will accomplish this using a text programming language called **Python**, which is a popular tool among hackers and scientists. You will do the lab in an interactive coding environment called the **Jupyter Lab**, which allows you to run code in different languages and typeset your notes and equations at the same time. You will learn how to use *conditional*, *loop*, *list*, *unicode*, and *module* to *encrypt*, *decrypt* and launch a *dictionary attack*. This will cover the basic idea of *cryptology* (*cryptography* and *cryptanalysis*) in **cyber-security**.

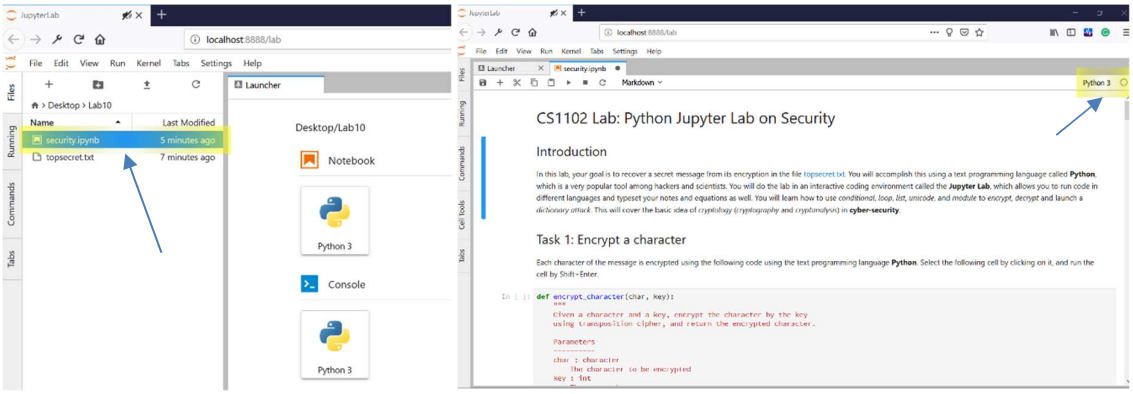
Task 0. Getting started

1. Download Lab10.zip from the Canvas course website and unzip it. It should contain two files:
   - `security.ipynb` (The Jupyter notebook file to do the tasks.)
   - `topsecret.txt` (The text file containing the encrypted secret.)
2. Run the Anaconda Navigator and Launch the Jupyter Lab application.



Additional notes if you want to use your computer: You can install Anaconda on your computer but you should use Chrome/Firefox/Edge as your default browser instead of IE.

3. You should see a web browser opened up with the address http://localhost:8888/lab. In the file panel on the left of the browser window, locate the file `security.ipynb` and double click the file to run the notebook. (The default working directory is your home directory, so your downloaded files should be under the Downloads folder. Select Python 3 as the Kernel if asked.)



4. Save your changes frequently by pressing CTRL+S, click , or choose `File > Save Notebook` from the top menu bar. Remember to take all your files with you after the Lab.

You can now follow the instructions in the Jupyter notebook to complete the tasks. The following provides additional hints if you need.

Task 1. Encrypt a character

The following is the solution to task 1 but with some parts covered up.

```
# Task 1 solution
print(encrypt_character(   ,   ))
print(encrypt_character(   ,   ))
print(encrypt_character(    ,   ))
print(encrypt_character(    ,    ))
```

Task 2. Decrypt a character

The following is the solution to task 2 but with some parts covered up.

```
def decrypt_character(encrypted_char, key):

    # Step 1 solution
    char_int_code =    (encrypted_char)
    # Step 2 solution
    shifted_char_int_code = (char_int_code   key)   1114112
    # Step 3 solution
    decrypted_char =    (shifted_char_int_code)
    # Last step solution
    return
```

Task 3. Decrypt a ciphertext

The following is the solution to task 3 but with some parts covered up.

```
def decrypt(ciphertext, key):

    # Task 3 solution
    plaintext = ''
    for char in ciphertext:
        decrypted_char = decrypt_character(    ,    )
        plaintext +=
    return plaintext
```

Task 4. Decrypt without the secret key

The following is the solution to task 4, step 2, but with some parts covered up.

```
def get_score(text):

    # when text is empty
    if len(text) == 0:
        return 0

    # change all character to lower case to match the words in dictionary
    text = text.lower()

    # transform the text into a list of words
    list_of_words = text.split() # e.g. ['apple', 'is', ]

    # Get the total number of words in the sentence
    num_words = len(list_of_words)

    # Step 2 solution
    num_eng_words = 0
    for word in list_of_words:
        if     in           :
            num_eng_words +=
    return             / num_words
```

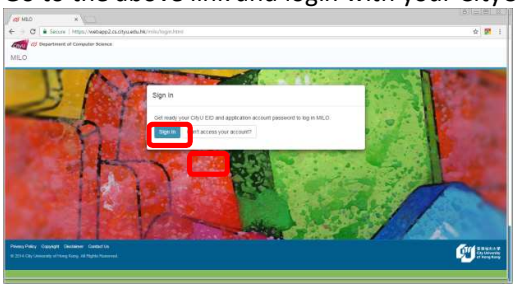
The following is the solution to task 4, step 3, but with some parts covered up.

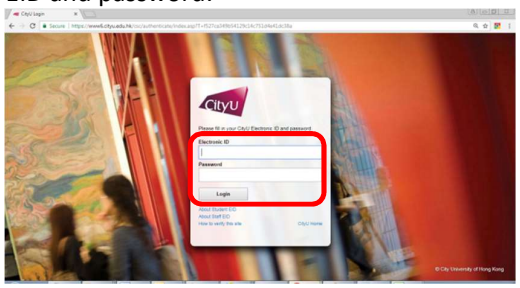
```
for    in range(       ):
    decrypted_content = decrypt(ciphertext, key)
    # Step 3 solution
    score = get_score(                 )
    if score >    :
        print('score: ', score)
        print('key: ', key)
        print('plaintext: \n', decrypted_content)
        break
```

Demonstration – There is no exit test for this lab. To get assessment, show your solutions in Jupyter.

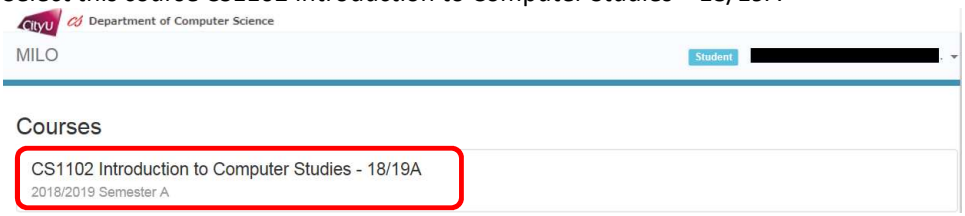
Attendance and Assessment – Starting with this lab, our TAs will take students' attendance and give assessment with the MILO system from the link https://webapp4.cs.cityu.edu.hk/milo/login.html

1) Go to the above link and login with your CityU EID and password.

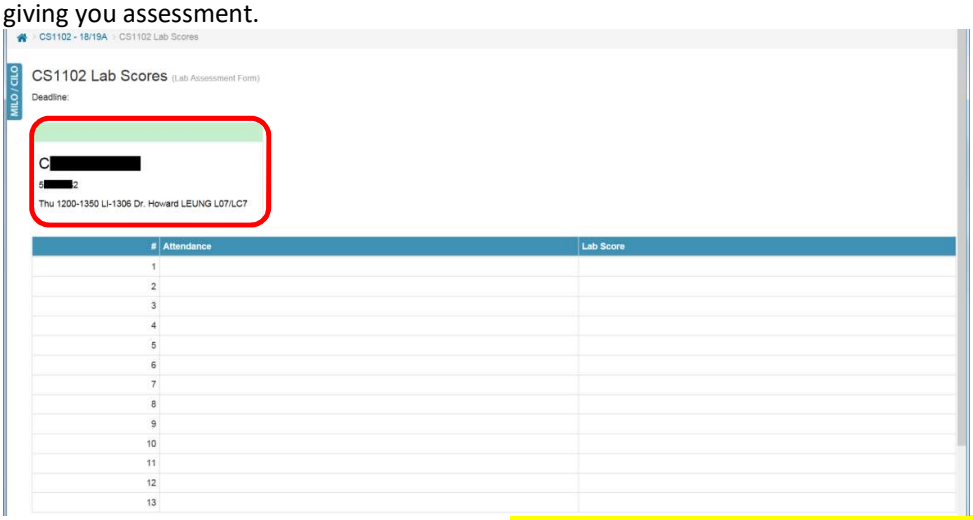




2) Select this course CS1102 Introduction to Computer Studies – 18/19A



3) Your identity information will be displayed. Show this to the TA who are taking your attendance or giving you assessment.



After the TA has taken your attendance, you should refresh your browser and see that your attendance record gets updated on your MILO screen.

4) To get assessment for this lab,
   - You should show your answers for the Exit Test and demonstrate your work of Task 4 and Task 5 to the TA **at the same time** (meaning that you should not demonstrate your work part by part at different time instants and expect that a TA would remember it).
   - The TA will give you a mark on his/her notebook.
   - You should refresh your browser and see that your grade gets updated on your MILO screen.

Students should try the optional tasks at the end of the Jupyter notebook in class if they finish the above tasks early and have already received the lab assessments. For those students who do not have enough time to try the following tasks in class, they should do them at home after class.

Note:

Before you leave,

1. check on the MILO system to verify that your attendance has been taken and your lab score has been entered
2. remember to return the notebook and get back your student card