

Python Cryptography Course

Dr Andrew French January 2018

- This is a themed course which is intended as a motivational vehicle for learning some practical programming skills using Python (v3)
- Basic methods will be taught with the goal of building up to a project (see below)



Course workflow

1. Accessing Python
2. Accessing course resources
3. Project #1: **Caesar shift** substitution cipher
4. Project #2: **Random key substitution cipher**
5. Project #3: **Vigenere** polyalphabetic cipher
6. Project #4: Random key **polyalphabetic** cipher
7. Project #5: Text **frequency analysis**
8. Project #6: Substitution cipher **codebreaking**
9. Project #7: **Steganography** with bitmap images
10. Project #7: Hiding text files in **sound files**

Accessing Python

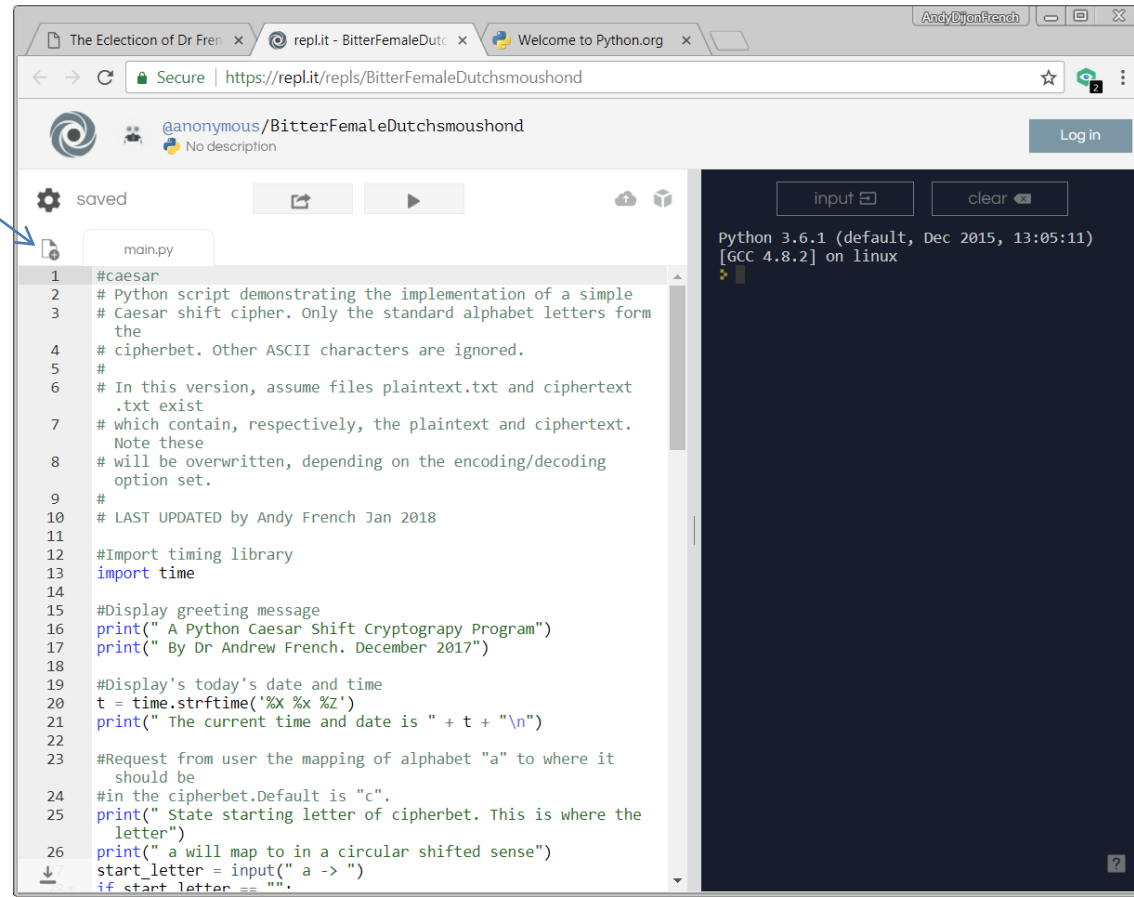
<https://repl.it/languages/Python3>

Method #1 (use this if you are not allowed to install any software)

Using a web browser, navigate to **repl.it** and choose Python 3. This is an online coding environment.

Click on the **file add** button and choose **Project** mode. This will enable you to add and save files etc.

You can type Python code in the left hand screen, which can then be run in the console on the right.



```
1 #caesar
2 # Python script demonstrating the implementation of a simple
3 # Caesar shift cipher. Only the standard alphabet letters form
4 # the cipherbet. Other ASCII characters are ignored.
5 #
6 # In this version, assume files plaintext.txt and ciphertxt
7 # .txt exist
8 # which contain, respectively, the plaintext and ciphertxt.
9 # Note these
10 # will be overwritten, depending on the encoding/decoding
11 # option set.
12 #
13 # LAST UPDATED by Andy French Jan 2018
14
15 #Import timing library
16 import time
17
18 #Display greeting message
19 print(" A Python Caesar Shift Cryptograpy Program")
20 print(" By Dr Andrew French. December 2017")
21
22 #Display's today's date and time
23 t = time.strftime('%X %x %Z')
24 print(" The current time and date is " + t + "\n")
25
26 #Request from user the mapping of alphabet "a" to where it
27 # should be
28 #in the cipherbet.Default is "c".
29 print(" State starting letter of cipherbet. This is where the
30 # letter")
31 print(" a will map to in a circular shifted sense")
32 start_letter = input(" a -> ")
33 if start_letter == "":
```

Method #2 (use this if you can install software)

<https://www.python.org/>



Go to the main Python website and download the latest edition of Python.

Make sure you download version 3.

Run the installer, which will enable you to edit and run code using the **IDLE** editor, which will be installed by default.

You can run Python (.py) files just by double-clicking on them.

However, if you want to do some de-bugging, run from within IDLE (press function key F5)

A screenshot of the IDLE Python editor window. The title bar reads "caesar.py - E:\AndyFrench\Documents\AF\Programming\A Course in Coding\4. Python\08 Cryptography\01. Caesar shift su...". The menu bar includes "File", "Edit", "Format", "Run", "Options", "Window", and "Help". The code is as follows:

```
#caesar
# Python script demonstrating the implementation of a simple
# Caesar shift cipher. Only the standard alphabet letters form the
# cipherbet. Other ASCII characters are ignored.
#
# In this version, assume files plaintext.txt and ciphertext.txt exist
# which contain, respectively, the plaintext and ciphertext. Note these
# will be overwritten, depending on the encoding/decoding option set.
#
# LAST UPDATED by Andy French Jan 2018

#Import timing library
import time

#Display greeting message
print(" A Python Caesar Shift Cryptograpy Program")
print(" By Dr Andrew French. December 2017")

#Display's today's date and time
t = time.strftime('%X %x %Z')
print(" The current time and date is " + t + "\n")

#Request from user the mapping of alphabet "a" to where it should be
#in the cipherbet.Default is "c".
print(" State starting letter of cipherbet. This is where the letter")
print(" a will map to in a circular shifted sense")
start_letter = input(" a -> ")
if start_letter == "":
    start_letter = "c"
print(" a -> c ")

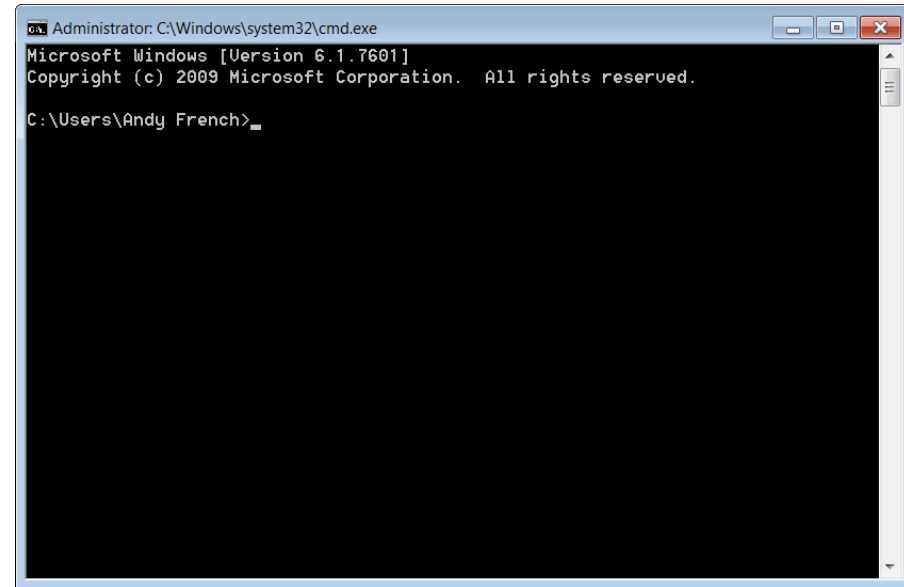
#Define lower-case alphabet
alphabet = list("abcdefghijklmnopqrstuvwxyz")
N = len(alphabet)
```

The status bar at the bottom right shows "Ln: 1 Col: 0".

IDLE editor

If you are able to install software, bring up a system console (or command window in Windows) and type some PIP code to install extra Python libraries. You will need these extra libraries in this course. **Obviously, install Python first!**

In Windows, go to the Start menu, click on Run and type `cmd`



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Andy French>_
```

Type the following and press return. You will need to be connected to the internet!

```
python -m pip install --user numpy scipy matplotlib xlwt xlrd
```

and a few other extras too for good measure...

```
python -m pip install --user ipython jupyter pandas sympy nose soundfile pydub
```

Resources for this course can be downloaded from

http://www.eclecticon.info/programming_coding_course_python_pi.htm

