Cryptography.

CYB 5678

LAB – 1

Caesar, Substitution Ciphers

Name: Rusheel Raj Panakadan

1. Implement the Caesar cipher in C, Java, or Python, as a program that reads a Latin string from standard input and encrypts each low case a-z character encountered, returning the result as uppercase. All other characters are left unchanged.

**Run it on the following alphabet string:**

*a b c d e f g h i j k l m n o p q r s t u v w x y z*

**and on**

*te amo  
meet me after the toga party*

**Screenshot of the source code in Python 3.10:**

Text

Description automatically generated

Output for first task:

Encrypting the string: “*a b c d e f g h i j k l m n o p q r s t u v w x y z*”

A screenshot of a computer

Description automatically generated with medium confidence

Encrypting the string: “*te amo*”

Text

Description automatically generated with medium confidence

Encrypting the string: “*meet me after the toga party*”

Text

Description automatically generated

Encrypting the string: “*te amo\nmeet me after the toga party*”

Text

Description automatically generated

2. Change your code at task 1 to obtain a shift cipher with key passed as command line argument.

**Source Code for encrypting the string with key passed as command line argument:**

Text

Description automatically generated

Encrypt with *key 4* the message at task 1.

A screenshot of a computer

Description automatically generated with medium confidence

Text

Description automatically generated

Also encrypt with the same key: ***“brutus sets up the stage tonight.”***

Text

Description automatically generated

What if the key is -4? Show how you use the same code to decrypt the ciphertext.

Text

Description automatically generated

I have also created a separate code called DecryptCaesar.py which will automatically convert the negative key shift to positive key shift and decrypt the message.

In below code, when we pass ‘4’ as command line argument, the program automatically assumes that the integer is a negative shift key to ‘-4’.

Text

Description automatically generated

3. Use brute force to break the ciphertexts:

* "GCUA VQ DTGCM"
* "LGEGJJGO OW OADD ESJUZ GF HSFLZWJ VAFAFY"
* "GO QOD K YB NOKDR"

**Screenshot of the source code to Brute-force a Caesar Cipher in Python 3.10:**

Text

Description automatically generated

3.1 Brute forcing and decrypting a string “***GCUA VQ DTGCM***”

Text

Description automatically generated with medium confidence

3.2 Brute forcing and decrypting a string “***LGEGJJGO OW OADD ESJUZ GF HSFLZWJ VAFAFY***”

A screenshot of a computer

Description automatically generated with medium confidence

3.3 Brute forcing and decrypting a string “***GO QOD K YB NOKDR***”

Text

Description automatically generated with low confidence

***Note***: Source Codes for the algorithm are attached to another word file.