National College of Ireland

CONFIGURATION MANUAL

MSc Research Project

MSc in Cyber Security

Sunil Gangula

X20189800

School of Computing

National College of Ireland

Supervisor: MICHAEL PRIOR

National College of Ireland

Project Submission Sheet – 2021/2022

Student Name: ……SUNIL GANGULA..……

Student ID: ……X20189800……

Programme: ……MSC IN CYBERSECURITY…… **Year:** ……2022……

Module: ……CONFIGURATION MANUAL…..……

Lecturer: ……MICHAEL PRIOR……

Submission Due Date: ……19-09-2022……

Project Title: COMPUTATION OF NUMBERS USING HOMOMORPHIC ENCRYPTION

Word Count: 430

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
<u>ALL</u> internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature: ……SUNIL G……

Date: ……18-09-2022……

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**
5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

CONFIGURATION MANUAL

SUNIL GANGULA

X20189800

1. Introduction

This manual gives a detailed information regarding all necessary hardware and software setup required to build the entire system from scratch. The configuration manual will help in replicating the research done by using a more practical way. We are going to evaluate the complete working of the system with its user interface. (That is, how a user will interact with our system using the system user interface).

This document provides the steps to replicate the implementation of the "Homomorphic encryption".

The Configuration Manual will be divided into following sections

- Environmental Setup
- Libraries Required
- Implementation
- User

2. Environmental Setup

2.1 Hardware Requirements

- 8GB RAM.
- 250 GB HDD.
- 2.1 GHz Intel. Core i5

2.2 Software Requirements

- Windows 10
- Python 3.6.3

2.3 Programming Prerequisites

- Python(Version 3.6.3)
- Visual Studio Code

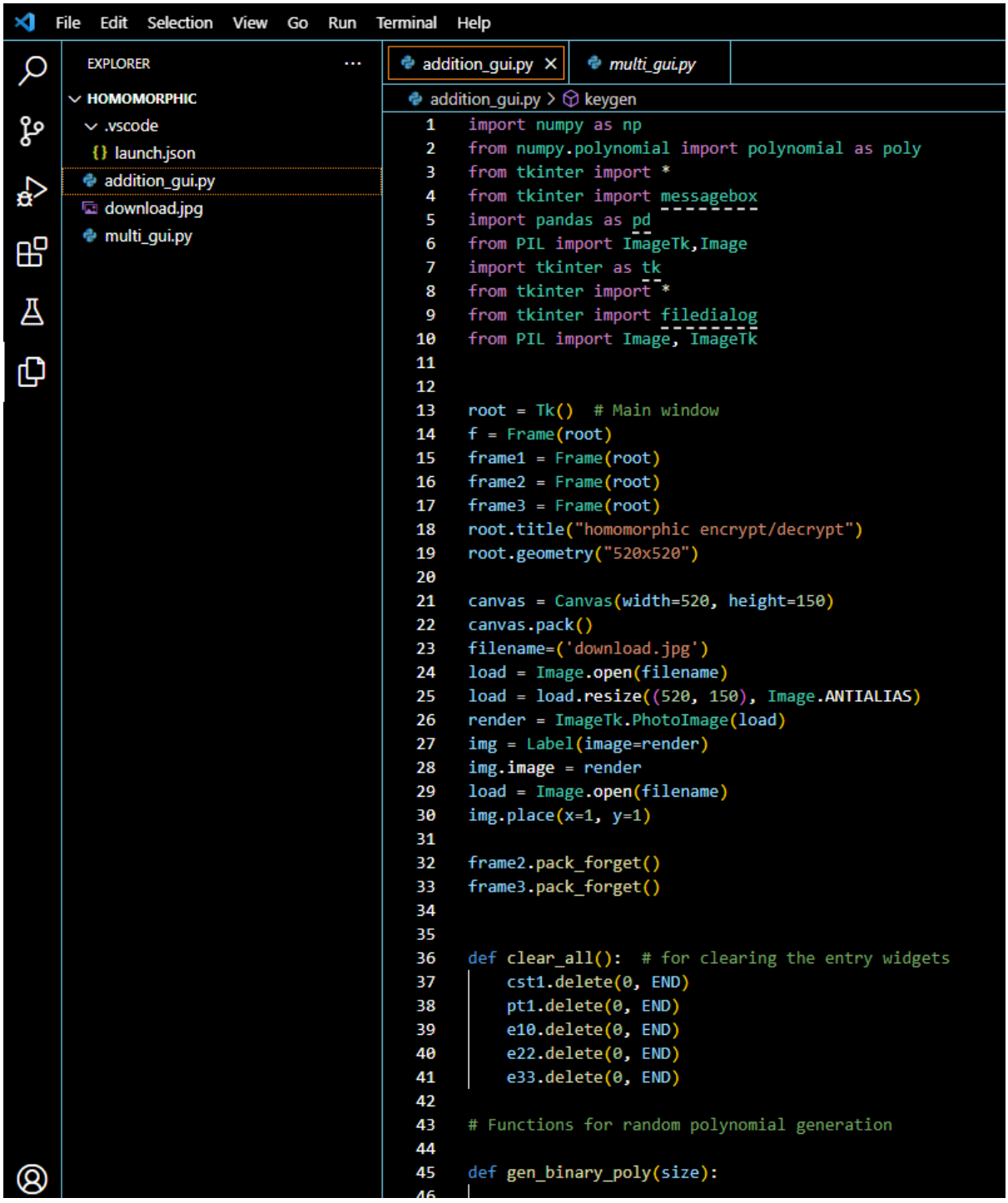
Libraries Required

All the libraries required for building this research project are mentioned in table 1 along with their usage:

Pandas	It offers data structures and operations for manipulating numerical tables and time series
Numpy	It is used for working with arrays. It also has functions for working in domain of linear algebra, fourier transform, and matrices
Tkinter	Python with tkinter is the fastest and easiest way to create the GUI applications. Creating a GUI using tkinter is an easy task. Tkinter is the standard GUI library for Python. Python when combined with Tkinter provides a fast and easy way to create GUI applications. Tkinter provides a powerful object-oriented interface to the Tk GUI toolkit.
Pillow	Python Imaging Library (expansion of PIL) is the de facto image processing package for Python language. It incorporates lightweight image processing tools that aids in editing, creating and saving images.

3. Coding Implementation:

In this section, we go through an implementation of a homomorphic encryption scheme. We have split the whole scheme into basic functionalities, key-generation, encryption, decryption, and evaluation. In order to run the program, we need to open the folder containing the code in visual studio code and it contains 2 program one for performing addition on encrypted numbers and the other is to perform multiplication. Below screenshots shows the code being loaded in in the visual studio code.



4. User interface

To load the user inputs, we used the Python Tkinker image. Depending on the purpose of an image in a Tkinter application, different code may be necessary for a Tkinter function to show a text-based message or an image-based message. The below screenshots show the images of the tkinter where an user loads the input for both addition and multiplication operations.

homomorphic encrypt/decrypt

homomorphic encrypt/decrpt

Enter First Number:

Enter Second Number:

Encrypt

Addition

Decrypt

Clear

homomorphic encrypt/decrypt

homomorphic encrypt/decrpt

Enter First Number:

Enter Second Number:

Encrypt

Multiplication

Decrypt

Clear