Celia Liberman

May 1st, 2020

Computer Science Final Project:

**Encryption and Decryption of a String Using Matrices**

**Summary of Program**

This project consists of a pair of programs that preform manipulation of matrices, such as matrix multiplication and matrix inversion, in order to encrypt and decrypted a user-inputted message.

The first program except two pieces of information from the user, the name of a file containing the user’s chosen key matrix and a string that is the message that is desired to be encrypted, and tests for different necessary matrix properties to insure the defined key can be used to encrypt the message. The program then reads the key matrix file and converts the lines of strings to a two-dimensional list of integers representing the matrix, where the inner lists represent the rows in the matrix. The characters of the message, that is in string form, are then separated and converted into the corresponding unique number for each character and add to a list of all the numbers in the correct order. The list of numbers is then transformed into a two-dimensional with a number of rows (inner lists) equal to the number of columns and rows of the key matrix. If the number of elements in the list is not divisible by the number of columns, and therefore does not form even rows, the program adds the number 27 to the list, which corresponds to a white space. The key matrix and converted message matrix are then multiplied through matrix multiplication which results a matrix representing the encrypted message. A file is then created with the encrypted message after it was converted to the same format as the key matrix file (lines of strings).

The second program basically reverses the process of the first. It receives the name of two files, one containing the key matrix and the other containing the encrypted message matrix. The program reads the files, converts the string of matrix rows and converts the two matrices to two two-dimensional lists. The key matrix must then be inversed using the python package ‘numpy’. The inverse of the key matrix and the encrypted message matrix are then multiplied and result in the original decrypted message matrix. This is followed by the translation of the decrypted message matrix to letters and symbols. The program then asks the user if they want the message displayed in python or to open a new text file with the message. If the user choses to open a file, they get to name it.

**Testing Instructions**

How to use the first program:

After running the program, the user is asked for the name of the file containing the key matrix. The user must include the filename extension when entering the filename. I provide a text file with a key as an example called key\_matrix.txt. There are a few requirements for the key matrix so that the encryption and decryption can work:

* Matrix must be square and invertible
* Matrix must contain only integers
* Matrix can be of any size
* The matrix file must be formatted in the following way: each line of text represents each row of the matrix where each entry is separated by a single space

Once the user enters the filename of the key matrix file, a new input is required. The user is then prompt to enter the message they want to be encrypted. To limit the size of my character list, I allowed the user to include in their message only upper and lower case letters, whitespaces, and a limited number of characters (. , ! ?). The message then is encrypted, the user is asked for a name for the file (with extension), and a text file with the encrypted message matrix is created.

How to use the second program:

After the desired message was encrypted the second program can be used to decrypt it. This program prompts the user for the name of two files, once again the key file is required along with the text file of the encrypted. So to test this program, enter the key matrix file name with extension (key\_matrix.txt if using the one I provided) and the name of the encrypted message file, which will be the name you gave the file in the previous program with the extension. The program decrypts the message and present you with the option to etiher display the message in python or create a new text file containing the message. To make that choice, enter either the word ‘display’ or ‘file’. If file is chosen, you must enter the desired name for the new file with the extension.

I added three key files, a 3x3 invertible matrix file called key\_matrix.txt, a 5x5 invertible matrix file called key\_matrix\_2.txt, and a 4x4 non-invertible matrix file called non\_invert\_key\_matrix.txt to show what happens when a non-invertible matrix is used as a key. You can also create your own key file.

**Citations**

Gaddis, Tony. (2018). *Starting out with Python,* 4th Edition. Pearson Education.

SciPy community. (2018). *Quickstart tutorial,* Simple Array Operations. Retrieved April 30, 2020, from https://numpy.org/doc/stable/user/quickstart.html

Williams, Gareth. *Linear Algebra* with Applications, 9th Edition. Jones & Bartlett LEARNING.

**Special Thanks**

Just wanted to give thanks to Scotti Day for telling me about the ‘numpy’ package that contained the inverse matrix function and to Austin from UVM Tech Support for helping me diagnose an issue with my computer and helped me redownload python, pip, and the ‘numpy’ package.