EECE 455: Final Report

Project 1: Classical Encryption

Project Work Done:

For this project we divided the work between the three members of the group. Serge Ohannessian implemented the algorithms for parts 1 and 3 of the project (Affine cipher, crack affine cipher and Vigenere cipher), Rami Dgheim implemented the algorithms for parts 2 and 5 of the project (Mono-Alphabetic cipher and Hill Cipher), Mohammad Kachmar implemented parts 4 and 6 of the project (Playfair cipher and Extended Euclid Algorithm).

In order to ease the way we work on the project we created a GitHub folder for our project and used git to push and pull changes to the code.

All the programming was done using the python programming language, while the GUI interface was implemented using Tkinter which is a standard python interface.

One minor change was done in Playfair cipher, in case we have 2 identical letters that should be encrypted, instead of inserting an ‘x’ we inserted a ‘q’, for example, “ee” would become “eqe”. A couple of other small changes similar to this one were done. All those changes were done in the playfair.py fixText function.

How to run the application?

In order to run the application:

- download the source code from Moodle and save it in a directory on your pc.
- Open command prompt and go to the folder where you saved the downloaded source code.
- Run the command: pip3 install tk
- Run the command: pip3 install numpy
- Run the command: python main.py

Some test results of our application

For the Affine cipher encryption

Plaintext = This is a test!

b = 11

a = 17

Output = Warf rf l wbfw!

For the Affine cipher decryption

Ciphertext = Warf rf l wbfw!

b = 11

a = 17

Output = This is a test!

For the Crack Affine

First letter = j

second letter = x

Output = 20 7

For the Vigenere cipher encryption

Key = vigenere

Plaintext = help me please

Output = cmrt qv ktkefi

For the Vigenere cipher decryption

Key = vigenere

Plaintext = cmrt qv ktkefi

Output = help me please

For the monoalphabetic cipher encryption

Key = azertyuiopqsdfghjklmwxcvbn

Plaintext = help me to test

Output = itsh dt mg mtlm

For the monoalphabetic cipher decryption

Key = azertyuiopqsdfghjklmwxcvbn

Ciphertext = itsh dt mg mtlm

Output = help me to test

For the Playfair encryption

Key = largest

Plaintext = must see you over cadogan west

Output = uztb dlug wqpz nwlg tgtuerpv zatb

For the Playfair Decryption

key = largest

ciphertext = uztb dlug wqpz nwlg tgtuerpv zatb

Output = must see you over cadogan west

For the Hill cipher 2x2 encryption

Key = $\begin{matrix} 7 & 8 \\ 17 & 3 \end{matrix}$

Plaintext = a test for our project

Output = w fqsr aad ymf wxtrjkn

For the Hill cipher 2x2 decryption

Key = $\begin{matrix} 7 & 8 \\ 17 & 3 \end{matrix}$

Ciphertext = w fqsr aad ymf wxtrjkn

Output = a test for our project

For the Hill cipher 3x3 encryption

Key = $\begin{matrix} 1 & 2 & 5 \\ 5 & 9 & 7 \\ 2 & 2 & 3 \end{matrix}$

Plaintext = a test for our project

Output = g rydk loj azu pmolzpr

For the Hill cipher 3x3 decryption

Key = $\begin{matrix} 1 & 2 & 5 \\ 5 & 9 & 7 \\ 2 & 2 & 3 \end{matrix}$

Ciphertext = g rydk loj azu pmolzpr

Output = a test for our project

For the extended Euclid algorithm

b = 3456

m = 4321

output = 1079

Resources used for the project

The resources used in this project are:

- python programming language
- tkinter python GUI tool
- numpy python library
- git and Github