GARCIA, MICHAEL TYRONE T. **2012 - 59168**

CS 153 THV – Susan Pancho-Festin **May 25, 2017**

Project – Galois Field Calculator

Project Writeup

1) Name: Garcia, Michael Tyrone T.

Student #: 2012-59168

2) Programming Language Used: Python 2.7

3) Operating System used in development: Windows 10 (Version 1703 – Creators Update)

4) Git Repository Link: https://github.com/garciamighty/CS-153-THV-2017-Festin-Project-Galois-Field-Calculator

5) Reflection on the development process:

a. Which part(s) of the project, if any, did you find easy to do? Why do you think did you find these easy to do?

- I found asking and saving user input easy to do. Printing output was also easy to do. These parts are the founding basis of User Interaction and Experience.
- Without using numpy, I found polynomial addition and subtraction easy to do. As I saved the coefficients of the polynomial inputs in an array, it was simple enough to just add or subtract

them as is and manipulate their indices as powers of ‘x.’ After deciding to use numpy, the built-in functions as part of the library validated my previous solution.

- Without using numpy, I found basic polynomial multiplication easy to do. It was simply a matter of looping withing a loop to manipulate data (coefficients and indices) from both inputs and create a product of the two. I found polynomial division hard however. It was needed as part of galois field multiplication.

b. Which part(s) of the project, if any, did you find challenging to do? Describe how you solved these challenges?

- Without using numpy, I found polynomial division challenging to do. It was hard for me to imagine how to manipulate efficiently the coefficients and indices needed for each polynomial formed by polynomial division. It was at this point where I got stuck the longest without resorting to external libraries. As I re-read the project specifications, I noticed the line “You are not to use any special-purpose (crypto) libraries.” specifying illegal use of *cryptographic* libraries. As numpy is not such a library, I had decided to use it to aid my problem. The numpy library had built-in functions to deal with polynomial inputs, and in this particular problem, polynomial arithmetic as well.

6) References used:

a. GaloisFields.pdf you had sent the class via email

b. Relevant functions in the Numpy manual - https://docs.scipy.org/doc/numpy/reference/routines.polynomials.poly1d.html#arithmetic

c. py2exe tutorial in order to create a python executable - http://www.py2exe.org/index.cgi/Tutorial