

CS 153 Project: GF Calculator

Maria Rosario Gueco
2006-64076

May 24, 2017

1 Programming Language Used

Python

2 Operating System Used in Development

Windows 10

3 Git Repository Link

https://github.com/RoseyG/CS_153_Project.git

4 Reflection

The project is a Galios Field Calculator for the operations addition, subtraction, multiplication and division. In making the project, there were varying levels of difficulty in depending on which parts of the project is being made.

The least difficult to make was the addition and subtraction component of the calculator. They both use the exclusive or bit operation which I used in my implementation.

The more difficult to implement portien was the multiplication operation. This required some thought and a lot of trial and error in implementing. Using Python however helped speed up the process. I first created a function to multiply individual coefficients then used that function inside another function to multiply the polynomial.

5 Reference Used

Christof Paar, Jan Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners

Department of Electrical and Computer Engineering, Galois Field $GF(2^m)$ Calculator. University of New Brunswick, Fredericton, NB, Canada. <http://www.ee.unb.ca/cgi-bin/tervo/calc2.pl>