ECE6280
Programming Project #3
Due by Mon Nov 4, 2019

Sep. 20, 2019

1 Problem 1

Do Problem 6.28 in Stinson.

2 Problem 2

Do Problem 7.9 in Stinson

3 Problem 3

In the project, you will solve a discrete logarithm problem ($\beta = \alpha^a \bmod p$) using the index calculus method. Each student in the class will find a different a. I will send you a personalized β. Your task is to find a.

You will use $p = 10930889$, and perform calculations the subgroup formed by $\alpha = 2317547$. This subgroup has order 59407. This means that the element in question is not a primitive element, which means you need to slightly modify the index calculus method. This modification is the primary "new" work of the project. Please notice that this makes it easy to solve the problem without using the index calculus method. So it is easy to get the right answer via exhaustive calculation and use this as a check on your program.

Please submit and electronic version of your code (which is not an exhaustive search), a description of what you did, and a hard copy of your program.