WriteUp.pdf

Manikantanagasai Illuri

Feb 2023

Assignment 5: Public Key Cryptography

1 Introduction

For the assignment I had to develop an algorithm that will take any input and encrypt as well as decrypt it.

2 What I have learned?

The assignment required me to get in touch with Public Key Cryptography. This is a very widely used security method which uses a public and private key to authenticate users and create a secure network. For this file I had to use the Schmidt-Samoa Algorithm for which I had to implement the Keygen file which generates a private and public key and the encrypt and decrypt files that will use functions from the ss library to encrypt and decrypt the inputs.

2.1 Challenges I faced during the assignment

During this assignment I faced problems such as segmentation faults and floating point exceptions primarily. My segmentation faults primarily came from my is prime function which i had to debugg using gdb and print statements. To tackle the floating point exceptions i realized I new I had to check where I was doing division by 0. To fix this issue, I had to make sure I was setting all my variables correctly when i was using temp vairbales and make sure my mpz usage was correct.

3 Personal Though

This assignment was a very challenging one. I had to refer to my last quarters work t understand what corner cases I need to tackle. I used the help from TA's an Tutors to complete it which made it very helpful. I was also able to understand where such secure algorithms are used in the real world.