Assignment 5 Writeup

Caitlin Smith

February 26, 2023

1 What I Learned

1.1 GMP

Using the GNU MultiPrecision library was really interesting. It was definitely a learning curve to remember to use all of the very specific MultiPrecision integer functions. For example, I had to make sure to remember to initialize, set, and clear each mpz_t I used. The first time I tried to run my main files with main functions I got segmentation faults because I hadn't cleared the right variables or the clear function wasn't called in the right spot. It also took me a while to fully understand that mpzs kind of act like pointers. The variable you want the return value of a function in actually gets passed into the function as a parameter. I learned about the usage of GMP random state. It uses the Mersenne Twister algorithm to produce pseudo-random numbers. Overall, after this assignment, I am pretty comfortable with using mpzs.

1.2 Schmidt-Samoa (SS) Algorithm

The algorithm used for cryptography in this assignment was the Schmidt-Samoa algorithm. I thought it was very interesting to learn how all of the math behind it works. It was cool to read about each component and how slight changes can make it very easy for someone to crack the code. For example, publishing the value of pq publicly would make it very easy for the private key to be determined.

1.3 Reading and Writing Files

Though we have read from and written in files in past assignments, there were some new things I learned in this program. This included the use of blocks. Reading in certain sizes of information at a time was something I hadn't implemented before. The math to find the correct size of the block was also new. Finding the log of square root n was a challenge for me. I was able to look at Discord and get some tips on how to manipulate existing functions. Using hexstring was also a first.

2 Application of Cryptography

Public-private cryptography is used constantly. It helps ensure the information and messages are only received and accessible to the person that it is intended for. Things like secure websites and encrypted and secure emails use this kind of cryptography. Gmail has an enhanced encryption system that uses public and private key cryptography. It is called S/MIME and it uses signature verification. This kind of encryption can also be used for secure purchases online to protect sensitive information like a credit card number.