Assignment 5

Michael Kamensky

February 20, 2023

1 What I learned

For this assignment:

- I learned how to work with the gmp library
- I learned how to create mpz_t variables manipulate them and then clear their allocated memory
- I learned how to work with the Schmidt-Samoa (SS) Algorithm
- I learned the importance of randomness in encryption to keep communications safe
- I learned how to create two large prime numbers
- I learned how to check if a number is a pseudo prime through the MILLER-RABIN algorithm
- I learned the algorithms for power mod and inverse power mod
- I learned how to use fchmod() and fileno() to set file permissions for certain files
- I learned how to get a person user name through the getenv() command

2 Applications of Public and Private cryptography

Where are public and private cryptography used in the world? In short, the answer is everywhere in computational systems. For example, something I use and everyone uses every day https. When you login into a bank how do you and your bank keep your password and username are safe? The answer is cryptography using public, private, and then finally symmetric keys. The bank has a private and public key. Using the public I or you can send encrypted information that only they can read. We give our public key through this encryption and the bank can send a symmetric key. Once a symmetric key is set up you and the bank can have an encrypted channel of communication. The reason the symmetric key is used the entire time is cause public and private key cryptography is way more computationally expensive. Another personal example of using is the ssh protocal that I use to log into my virtual machine for this course, which uses a similar public, private, and symmetric key to provide secure communication. More examples of using public and private key encryption include cryptocurrencies, digital signing, digital commerce, etc. In summary, public and private key encryption is everywhere in our modern-day world, without it secure communication on the internet would not be possible.