Assignment 5

Kat Pe Benito
kpebenit

I gained knowledge of the mathematical concepts, such as the challenge of factoring big prime numbers, that underlie the security of the SS algorithm. Message encryption and decryption use public and private keys, which I also learned about in terms of their construction. This subject captured my interest because it offered a look into the intricate mathematics that underlies contemporary cryptographic systems. I started by setting up the development environment, which involved installing the GMP library. This was a bit challenging at first, since I had never used GMP before, but I was able to find some helpful resources online, such as documentation, to guide me through the process. I began using GMP to implement the different parts of the SS algorithm. This required executing the algorithm's necessary cryptographic operations, such as producing large prime numbers, computing modular exponentiation, and more. As dealing with very large numbers that could not be represented using common data types like integers or longs was needed, I found this to be a little difficult. However, GMP offered a variety of methods for dealing with large integers, which greatly simplified the implementation.
A majority of errors I ran into with this assignment were memory allocation errors: Because the SS algorithm requires working with very large integers, I needed to allocate enough memory to store these numbers. However, when I tried to allocate memory using the GMP library, I sometimes encountered errors related to insufficient memory. To solve this, I had to increase the amount of memory allocated or optimize my code to reduce the memory footprint. Other errors were type conversion errors: The GMP library provides a variety of data types for working with large integers, such as mpz_t and const mpz_t However, sometimes I encountered type conversion errors when trying to convert between these data types. This could happen if I accidentally used the wrong data type in a function call or if I tried to assign a value of one type to a variable of a different type. To solve this, I had to carefully check my code and ensure that I was using the correct data types throughout. This homework assignment was a challenging, but rewarding experience.