WRITEUP

Ananya Batra

February 26, 2023

In assignment 5, I learned about cryptography. Cryptography is incredibly useful for confidentiality (keeping information secure), message integrity (ensuring that the information was not tampered with), and user authentication (ensuring that the information sender is who they say they are). In this assignment specifically, I implemented public key cryptography, which uses a private and public key. The public key is available for everyone to see but the private key is kept private and is only accessible by the user the key is associated with. These keys are generated through one-way mathematical functions, meaning that someone can't take a public key and reverse the math to find the components to then be able to generate the private key. The mathematical algorithms used are incredibly difficult (almost impossible) to reverse.

I learned about the Schmidt-Samoa algorithm to generate the public and private keys for this assignment. The public key is n = p^2q where p and q are randomly generated primes. The private key d is the inverse of n mod lcm(p-1,q-1). The encrypted message is given by c = $m^n mod n$ and the decrypted message is given by m = $c^d mod pq$. This algorithm deals with incredibly large integers, however all information (images, text, etc) can be represented with numbers so all information can be encrypted.

To work with large integers (larger than what C can support), I learned how to use the integer functions as well as the input and output functions in the GMP library. I used these functions to perform mathematical operations in order to generate the public and private keys. I also used the formatted input and output functions to read in and write out the public and private keys. Learning to handle file input and output was very important in this assignment. I learned how to read in characters from a file, store them in an array and convert the array into an mpz_t to encrypt the message. I also learned to write a file using fwrite(), fprintf() and gmp_printf().

I never realized how prevalent public private encryption is in my day-to-day life. Before this assignment, I didn't quite understand cryptography. I thought that all information was transferred through secure channels. I didn't have a clear idea of what this meant but I assumed that

bad agents could not access the channels of communication and information transfer, keeping them private. I essentially thought of information being transferred through opaque "internet tunnels" that could not be looked into or broken, connecting the sender to the receiver and keeping communication private. For this reason, I didn't think cryptography was extremely common or necessary in day-to-day activities. However, I know now that information being sent over the internet can be accessed by anyone which is why encryption is so important. While anyone can access the message, because it is encrypted, only the intended receiver can decode it. I now understand the importance of cryptography and have a better understanding of how it works.

Cryptography is everywhere. To ensure security and privacy, it is a necessary component to the digital world. Without it, industries such as online banking, healthcare, and many others count not exist. All in all, cryptography affects the world because it is needed in almost all industries, providing privacy, authentication, security, and much more. I personally take advantage of public key cryptography every time I send a message. Modern texting platforms like WhatsApp use this kind of encryption for secure messaging. The contents of any message I send can only be read by me and the person receiving my message. This is incredibly important to keep communication secure and private. Even social medial companies and other third party companies who help with sending messages can't decipher the texts sent on their platforms because they don't have access to the receiver's private keys.