Applications of Crytography in the Real World and my Daily Life

Alex Yeh

February 24, 2023

1 Introduction

Assignment 5 was centered around public-private cryptography. This assignment was to create three programs (keygen, encrypt, and decrypt), two libraries (numtheory and ss), and a random state module (randstate). The keygen program is in charge of key generation, producing SS public and private key pairs. The encrypt program encrypts files using a public key and the decrypt program decrypts the encrypted files using the corresponding private key. The numtheory library holds functions relating to the mathematics behind SS and ss contains implementations of rountines for SS. The randstate module is a library that contains the implementation of the random state interface for the SS library and number theory functions. In order to complete all of these programs/libraries, I needed to learn how to use the GNU multiple precision arithmetic library (GMP).

2 What I Learned From This Assignment

A huge thing I learned in this assignment was how to use the gmp library. I utilized the gmp library to do calculations with mpz_t variables as if they were integers. I learned how to use functions such as mpz_inits, mpz_sub_ui, mpz_mod, mpz_cmp_ui, and mpz_clears just name a few. I learned how to get a random number in a certain range which was very useful in ss_make_pub. In addition, I learned more about how to scan in a file, how to read a file, how to write to a file. Overall, I learned a lot about cryptography, how to generate a key, and how to encrypt and decrypt a message which was basically what this assignment was about.

After completing this assingment, my understanding of cryptography has changed a lot. If you asked me before starting this assignment what cryptography was, I would have told you it is a method used to send messages back and forth to each other securely. I would not have known the method behind how the messages were sent back and forth either. However, after completing this assignment, I now know that cryptography utilizes a public key and a private key to encrypt and decrypt messages. An individual can encrypt a message using the intended's

receiver's public key and that encrypted message can only be decrypted with the receiver's private key. What makes cryptography secure is that the public key is known to everyone and the private key is only known to the receiver.

3 Applications of Public-Private Cryptography in the Real World

Public-private cryptography is used in the internet to secure data such as login credentials, credit card numbers, social security numbers, and other sensitive information. For example, when you log into a website, you must enter your username and password. The website will then encrypt your password using the website's public key and send it to the server. This ensures that your login credentials are secure and hackers cannot access your account. Another applicaiton of public-private cryptography is bank transactions. When you make a bank transaction, the bank will encrypt your transaction using your public key and send it to the server. This transaction may have your account number, the amount of money you are transferring, and the account number of the person you are transferring money to. The server will then decrypt the transaction using your private key and process the transaction securely. A third application of public-private cryptography is sending emails. When you send an email, the email is encrypted using the recipient's public key and sent to the server. The server will then decrypt the email using the recipient's private key and deliver the email to the recipient.

4 How I Take Advantage of Public-Private Cryptography in my Daily Life

All of the applications I described in the section above are how I take advantage of public-private cryptography in my daily life. I use public-private cryptography to secure my login credentials when I log into websites such as my UCSC Canvas account, shopping on Amazon, and logging into my bank account. I use Zelle and Venmo to transfer money to my friends and family and public-private cryptography allows me to securely transfer money to them. Lastly, I use public-private cryptography to send and receive emails to and from whoever I need to.

5 Conclusion

Overall, I really enjoyed learning about cryptography in this assignment and using this knowledge to generate keys, encrypting files, and decrypting files. Learning how to use the gmp library was interesting because in a way, it was like learning a new programming language. If it wasn't for cryptography, I don't think the real world would function the way it does and my daily life would be much harder. I'm glad I learned about cryptography because I didn't realize how much myself and the world rely on it.