Assignment 5: WRITEUP.pdf

Katrina VanArsdale

February 27, 2023

1 Description

This program contains an implementation of an SS cryptographic algorithm. It contains three different programs: keygen, encrypt, decrypt. Keygen creates a public and private key and stores them in different files. Encrypt uses the file containing the public key to encrypt a provided file. Decrypt takes in the encrypted file and outputs the decrypted file using the corresponding private key.

2 Lessons learned and Thoughts

Before starting this assignment I never really understood how encryption worked especially with computers but the first lecture about it was very helpful. Learning how a cipher text works was pretty simple but this assignment has been a lot more complicated. At first, I didn't really understand how to use an mpz_t but once I got the hang of it it was pretty easy to understand and use.

One problem that I had which really threw me for a loop was with my pow_mod function. My is_prime function wasn't working correctly and after hours of looking through the code and pinning down the problem, I finally found that when I called pow_mod(y,y,2, n) (pow mod takes in o, a, b, n) I would set 'o' to 1 which was setting 'y' to 1 before I saved 'a' which was also 'y' into a different variable. So I somehow changed a const mpz_t because the same mpz_t was being passed as the output.

Another problem I had was with decrypt_file because my original understanding of what encrypt_file was doing was that block k was just each line of the text. This was backed up by the fact that the text file I was testing only had two lines of text and encrypt was outputting two lines as well. So when I was writing my decrypt_file I printed a newline after every block and I couldn't understand why it was outputting incorrectly. I messed with my code so much before realizing I just had to get rid of the newline. Seeing that encrypt would print a lot more lines if n was smaller really confused me before I understood that block k had nothing to do with the lines of text.

3 Conclusion

SS encryption really makes sense as a good encryption method because each encrypted message is made for one person's eyes using their public key and they alone can read it with their private key. There's no need for some other private way to share keys. It sort of reminds me of a PO box where there's no need to share your personal address but people can still send you things. I imagine encryption is very important in the government and international affairs but the simplicity of it allows anyone to keep their information safe while still sharing it with people who need to see it. I think I have a bit of a mindset where I can't comprehend why someone might what to steal MY information because I don't see much value in it. But something like money through online banks, venmo, zelle, and other applications I imagine has some sort of encryption that keeps me safe for the most part.