Assignment 5 Public Key Cryptography

Writeup

Derrick Ko - Winter 2023

1 Summary

You must use the fullpage and fourier packages. This write-up document should include everything you learned from this assignment. You should also discuss the applications of public-private cryptography and how it influences the world today. Be sure to describe at least one way in which you personally take advantage of public-private cryptography on a day-to-day basis.

2 What I Learned

2.1 Valgrind

This tool is really useful for pin pointing exactly where a memory leak happened. I am starting to be able to analyze it better and use it more efficiently.

2.1.1 Scan-Build

This tool was easy to learn since it was really organized and had easy to understand messages. It directed everything and made it easier to find my error in Valgrind.

2.2 GMP

Lots of gmp functions were learned since that was basically the bulk of the asignment being numtheory. A breif summary of GMP is (GNU Multiple Precision Arithmetic Library) is an open-source library designed to provide a range of high-precision arithmetic operations for integers, rational numbers, and floating-point numbers. Many of the functions store the return value within the function and learning that was one of the hardest things to understand for me for some reason. I had to go over and change all my numtheory to fix it since i stored the "output" value as something else. Any functions initialized with GMP has to be cleared after usage.

3 Usage of Cryptography today

In modern day, cryptography is used in small things like emailing. One of the most important applications of cryptography is in securing online transactions. Things like eCommerce, banking, and other money transactions all rely on secure encryption protocols to protect sensitive data from theft and fraud. Cryptography is also used extensively in digital signatures, which are used to authenticate the identity of individuals and organizations. Another area where cryptography is essential is in securing communication. Encrypted messaging apps like Telegram and WhatsApp use strong cryptography to protect messages from eavesdropping and ensure the privacy of their users. This also makes lots of problems legally with these apps. Also, VPNs use encryption to secure internet connections and protect user data from being stolen. In addition to these applications, cryptography plays a critical role in national security and intelligence. Governments use cryptography to protect classified information, and intelligence agencies use cryptography to intercept and decipher encrypted communications of potential threats. Personally, I use a VPN that is built into my browser on the daily. This is really important especially on public networks that everyone has access to.