Noel Ball
CSE13S

Writeup Document SS Encryption

I built my Makefile off of my previous assignment, although I included shell pkg-config –cflags gmp, -Wno-format-invalid-specifier, -Wno-format-extra-args, and -Wno-format in my CFLAGS. I also used -pkg-config –libs gmp in my LDFLAGS to link pkg-config and gmp. I learned how to create multiple executables and how to separate their dependencies, as my original process that involved automation of the object files based on all the c files created overlaps between where mains should be defined.

For the Keygen, Encrypt, and Decrypt executables I struggled with how to correctly read a file name as a command line argument to be set to the input and output file pointers, while still including stdin and stdout as defaults. I mistakenly created files called “stdin” and “stdout” instead of correctly using their file pointers, and assigning the file pointers to a different name if input.

I thought it was fun to learn how to use the mpz_t data types, although it took some getting used to, it really reminded me of assembly. My first design edited practically all of the const mpz_t’s that are input to the functions created in numtheory.c and ss.c, so I edited everything to use temp values correctly.

Due to my original mistakes with the assignment of file pointers, I really struggled with getting gmp_fscanf and fprintf to work correctly. And with enough debugging, it led me to the major mistakes with file handling in my project.

Noel Ball
CSE13S

As far as the function library files numtheory and ss, I had the most trouble with is_prime(). My first design with make_prime created a random odd number in the bit range, and iteratively tested if it was prime and added 2 if not. It took forever, and constantly ran into problems. My next design used a new random generation every prime check, which allowed me to successfully avoid a stuck loop and effectively debug my mistakes in is_prime().

Overall, this project really tested my endurance and self-confidence as a learning programmer. It almost broke me, with long nights debugging and editing, finally finishing after the deadline. Now I know I am capable of learning how to approach problems I don’t understand, with enough time and effort.