ASSIGNMENT 5 DESIGN DOCUMENT

Chris Moon

February 2023

1 Goal

Implement the SS method of file encryption. Write an function that generates public and private key pairs, as well as an encryptor function and decryptor function that uses said pair to encrypt and decrypt files.

In addition, write a short math library to handle the mathematics behind the SS encryption method.

2 Pseudocode

RANDOMIZER MODULE

-used for the later math library

-include gmp.h (don't forget to download gmp and pkg-config first)

-includes functions to initialize and clear a random state variable, which is defined as an extern variable of type gmp randstate

-use gmp randinit mt(state); and gmp randseed ui(state, seed); to set the state

-use gmp randclear(state) to clear the state

MATH LIBRARY

-GNU multiprecision (GMP) library needed to support precise math on large numbers

-GMP works like this: included gmp.h

-also have to include the randomizer module header

-Use and mpz type variable like this:

-mpz var;

-mpz init(var);

-then use gmp functions, like mpz set() or mpz add() to set a value and do arithmetic operations on the variable

-the math library needs a function for gcd, mod inverse, modular exponentiation, a prime tester, and a prime number generator

KEYGEN

-generates a pair of keys, public and private

-first, use the prime number gen from the math library to get two primes, p and q

-allocate the user specified bits randomly between p and q
-have a function that writes the public key to a file
-the public key = p*p*q
-also have a function to read a file containing a public key
-have similar functions for private keys
-private keys are defined by when the mod inverse of pq = lcm(p-1, q-1);