ASSIGNMENT 5 WRITEUP

Pehara Vidangamachchi

October 28th 2022

Ethan L. Miller

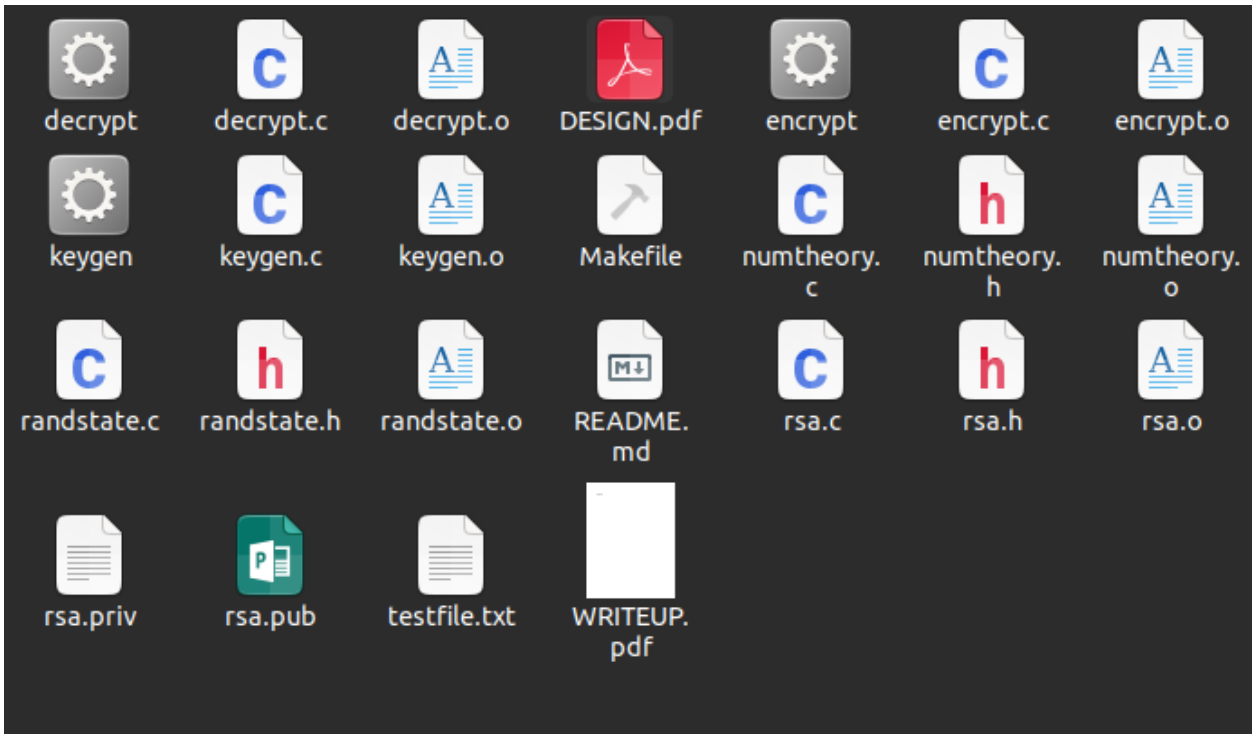
About:

This assignment contains my implementation of cryptography using RSA. I was able to do this by creating a working numtheory file that covered most of the math aspects of my assignment. Then from there, I had to implement the RSA functions which I was able to do following the assignment directions. Then from there I just had to combine each of the files so they would all work in unison so I could generate a key, encrypt a file and finally decrypt it back.

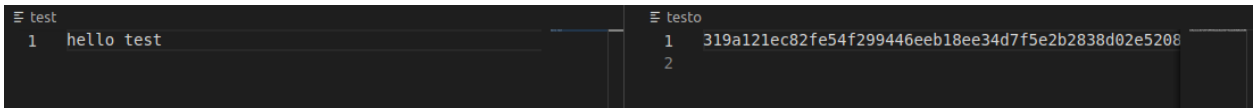
I found that My code displayed no prominent errors and when I ran every case worked fine, alongside the code being able to properly encrypt and decrypt a file.

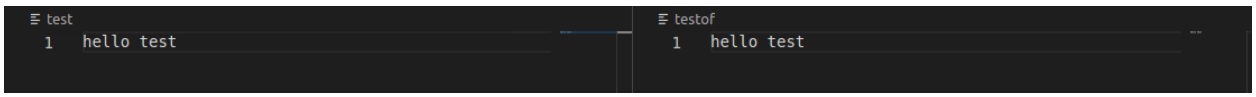
```
pehara@peharaVB:~/cse13s/asgn5$ ./keygen -h
Usage ./keygen [options]
./keygen generates a public / private key pair, placing the keys into the public and private key files as specif
ied below. The keys have a modulus (n) whose length is specified in the program options.

USAGE
./keygen [-h] [-v] [-n filename] [-d filename]  [-s seed]

OPTIONS
   -s specifies the random seed for the random state initialization (default: the seconds since the UNIX epoch,
given by time(NULL))
   -b specifies the minimum bits needed for the public modulus n
   -i specifies the number of Miller-Rabin iterations for testing primes (default:50)
   -n pbfile:specifies the public key file (default:rsa.pub)
   -d pvfile:specifies the privatekey file (default:rsa.priv)
   -v enables verbose output
   -h displays program synopsis and usage
pehara@peharaVB:~/cse13s/asgn5$ ./encrypt -h
SYNOPSIS
Encrypts data using RSA encryption.
Encrypted data is decrypted by the decrypt program.

USAGE
./encrypt [-h] [-v] [-i input file name] [-o output file name]

OPTIONS
   -i specifies the input file to encrypt (default: stdin).
   -o specifies the out put file to encrypt (default:stdout).
   -n specifies the file containing the public key (default:rsa.pub)
   -v enables verbose output
   -h displays program synopsis and usage
pehara@peharaVB:~/cse13s/asgn5$ ./decrypt -h
SYNOPSIS
Decrypts data using RSA encryption.
Encrypted data is encrypted by the encrypt program.

USAGE
./decrypt [-h] [-v] [-i input file name] [-o output file name]

OPTIONS
   -i specifies the input file to decrypt (default:stdin)
   -o specifies the output file to decrypt (default:stdout)
   -n specifies the file containing the private key (default:rsa.priv)
   -v enables verbose output
   -h displays program synopsis and usage
pehara@peharaVB:~/cse13s/asgn5$
```

The screenshot above displays my working help functions for all my executables.



The image above contains a screenshot of my files after using keygen.





These are my results after running a test on a test file which proves it to be working just fine. The first one is my original file and encrypted, followed by my original and decrypted file.