Parna Praveen
11/06/2022

WRITEUP

I tested my numtheory functions using online calculators and compared my output values with this.

In order to test my code, I downloaded the binary files from Piazza and compared the outputs of those files with those of mine. For example, for the help message I put this command into the terminal:

```
parna@parna:~/cse13s/asgn5$ ./keygen-dist -h
Usage: ./keygen-dist [options]
  ./keygen-dist generates a public / private key pair, placing the keys into the public and private
  key files as specified below. The keys have a modulus (n) whose length is specified in
  the program options.
    -s <seed>   : Use <seed> as the random number seed. Default: time()
    -b <bits>   : Public modulus n must have at least <bits> bits. Default: 1024
    -i <iters>  : Run <iters> Miller-Rabin iterations for primality testing. Default: 50
    -n <pbfile> : Public key file is <pbfile>. Default: rsa.pub
    -d <pvfile> : Private key file is <pvfile>. Default: rsa.priv
    -v          : Enable verbose output.
    -h          : Display program synopsis and usage.
parna@parna:~/cse13s/asgn5$ ./encrypt-dist -h
Usage: ./encrypt-dist [options]
  ./encrypt-dist encrypts an input file using the specified public key file,
  writing the result to the specified output file.
    -i <infile> : Read input from <infile>. Default: standard input.
    -o <outfile>: Write output to <outfile>. Default: standard output.
    -n <keyfile>: Public key is in <keyfile>. Default: rsa.pub.
    -v          : Enable verbose output.
    -h          : Display program synopsis and usage.
parna@parna:~/cse13s/asgn5$ ./decrypt-dist -h
Usage: ./decrypt-dist [options]
  ./decrypt-dist decrypts an input file using the specified private key file,
  writing the result to the specified output file.
    -i <infile> : Read input from <infile>. Default: standard input.
    -o <outfile>: Write output to <outfile>. Default: standard output.
    -n <keyfile>: Private key is in <keyfile>. Default: rsa.priv.
    -v          : Enable verbose output.
    -h          : Display program synopsis and usage.
```

I then input the same commands onto my files and made sure they're the same.

I also tested incorrect files with the binary files to get the message for this as well. I did them by doing this:

```
parna@parna:~/cse13s/asgn5$ ./encrypt-dist -i kdjfn
encrypt-dist: Couldn't open kdjfn to read plaintext: No such file or directory
parna@parna:~/cse13s/asgn5$ ./encrypt -i kdjfn
Couldn't open kdjfn to read plaintext: No such file or directory.
parna@parna:~/cse13s/asgn5$
```

This is a sample message test:

```
parnapraveen — parna@parna: ~/cse13s/asgn5 — ssh parna@localhost -p 2220 — 126×46
This is a test message for the writeup.
~
~
~
```

```
[parna@parna:~/cse13s/asgn5$ ./encrypt-dist -i writeuptest.txt -o writeupoutput.txt
[parna@parna:~/cse13s/asgn5$ ./decrypt-dist -i writeupoutput.txt -o writeupdecrypt.txt
[parna@parna:~/cse13s/asgn5$ ./encrypt -i writeuptest.txt -o writeupoutputmine.txt
[parna@parna:~/cse13s/asgn5$ ./decrypt -i writeupoutputmine.txt -o writeupdecryptmine.txt
[parna@parna:~/cse13s/asgn5$ diff writeupoutput.txt writeupoutputmine.txt
[parna@parna:~/cse13s/asgn5$ diff writeupdecrypt.txt writeupdecryptmine.txt
 parna@parna:~/cse13s/asgn5$
```