This ReadMe describes how to compile and run my RSAGenKey.java, RSAEncryption.java, RSADecryption.java, and the additional java files on a Linux (Ubuntu) machine from the terminal with the javac compiler.

There are additional java class files that are used. They are listed below.

Additional Java Files) CryptUtility.java

IOutility.java

KeyGenUtil.java

Utility.java

Warning: My Implementation of RSA will only successfully encrypt/decrypt a text file that is 128 bytes or less in size. Anything greater than 128 bytes will produce a decrypted file that will not be like the original text file. This problem comes from c (ciphertext) being bigger in bits then n (modules).

Step 1. Enter the below command into the terminal to compile the programs. All java files are assumed to be in the same directory.

```
javac RSAGenKey.java RSAEncrypt.java RSADecrypt.java
```

or

```
javac RSAGenKey.java RSAEncrypt.java RSADecrypt.java CryptUtility.java IOutility.java KeyGenUtil.java Utility.java
```

Step 2. Enter the below command into the terminal to execute the RSAGenKey program. Keys generated by the program will be written to the given file destination. Absolute and Relative paths can be used.

```
java RSAGenKey /PathToFile/Data.dat
```

Exampless)

```
java RSAGenKey /root/Documents/data.dat
```

or

```
java RSAGenKey Documents/data.dat
```

Step 3. Enter the below command into the terminal to execute the RSAEncrypt program. The given text file content will be encrypted by the program using the keys from the provided key file. The encrypted file content will be written to the given file destination. Absolute and Relative paths can be used.

```
java RSAEncrypt /PathToTextFile/file /PathToStoreEncyrptFile/file.enc /PathToKeysFile/Data.dat
```

Examples)

```
java RSAEncrypt /root/Documents/file /root/Documents/file.enc /root/Documents/data.dat
```

or

```
java RSAEncrypt Documents/file Documents/file.enc Documents/data.dat
```

Step 4. Enter the below command into the terminal to execute the RSADecrypt program. The given encrypted file content will be decrypted by the program using the keys from the provided key file. The decrypted content will be written to the given file destination. Absolute and Relative paths can be used.

```
java RSADecrypt /PathToEncyrptFile/file.enc /PathToDecryptFile/dec_file  /PathToKeysFile/Data.dat
```

Example)

```
java RSADecrypt /root/Documents/file.enc /root/Documents/dec_file /root/Documents/data.dat
```

or

```
java RSADecrypt Documents/file.enc Documents/file.dec Documents/data.dat
```

Step 5. To test the RSA algorithm, you can use the md5sum tool from the command line on the original text file and the decrypted file. If the same checksum is produced, then the algorithm was successful.

```
md5sum [FileName]
```

Example)

```
md5sum file
```

and

```
md5sum file.dec
```

If you have any questions you can email me at rjsalazar@cpp.edu