

RSA Project

PROJECT -2

GROUP 16

By:

Alejandro Alatorre

Kasthuri Ariram

Victor Raj

Part 1: RSAGenKey

Generate key based on one argument (k)

```
E:\Fall 2021\CS 4780\project from discord\RSA>javac RSAGenKey.java  
E:\Fall 2021\CS 4780\project from discord\RSA>java RSAGenKey.java 12  
Randomly selected p,q are 3571,2857  
public key [11 , 10202347]  
private key [5561411 , 10202347]
```

Generate key based p, q, and e as the input

To compile we use *javac RSAGenKey.java*

Then, *java RSAGenKey 6551 4733 8311*

```
D:\RSAProject>javac RSAGenKey.java  
  
D:\RSAProject>java RSAGenKey 6551 4733 8311  
public key [8311 , 31005883]  
private key [11296191 , 31005883]
```

Generates two files: **pub_key.txt** and **pri_key.txt**

ScreenShots:

Pub_key.txt file

```
e=8311  
n=31005883
```

pri_key.txt file

```
d=11296191  
n=31005883
```

Part 2: RSAEncrypt

To compile use *javac RSAEncrypt.java*

Then, use *java RSAEncrypt text.file pub_key.txt*

```
D:\RSAProject>javac RSAEncrypt.java

D:\RSAProject>java RSAEncrypt test.txt pub_key.txt
File Successfully created!
```

Creates test.enc file:

ScreenShot test.enc file output:

```
8894930 30343517 7299234 2627674 25049800 3621872 21375730 13028187 23725513 18634591 12942266 18336704 5842752 20228072 23367078 1452413 21170617 27678296 8579889 17787974 27477733 1861708
9210376 15725687 2050190 21999827 20357152 16556187 23354892 16467662 5227372 1319224 7299234 2627674 25049800 15480229 20953935 18513374 27561108 6888903 13503162 13998836 23104308 7707430
5316895 15902828 30275341 7108468 11647839 27926952 7855910 6051527 13417385 11815700 25563297 30275341 11997122 11997122 3255115 19065407 5476584 12947815 9879954 14937573 16284736 7347046
7531217 17345915 7299234 27562545 30275341 11997122 11997122 12947815 9879954 14937573 2050190 8008988 18893594 21295961 7108468 11647839 27926952 23725513 19563223 18672442 24508781
17692954 22601413 19562386 20832903 28391766 16001598 13823151 27420162 27281366 19441456 8579889 17787974 13823151 4350595 28502027 13410236 13998836 22601413 20228072 24057763
```

Part 3: RSADecrypt

To compile use *javac RSADecrypt.java*

Then, use *java RSADecrypt test.enc pri_key.txt*

```
D:\RSAProject>javac RSADecrypt.java

D:\RSAProject>java RSADecrypt test.enc pri_key.txt
File Successfully created!
```

Creates test.dec file:

We made the output text all Capitalized words.

ScreenShot test.dec file output:

WHEN A GAMERTAG COMES UP AS VIOLATING OUR POLICIES FOR ONLINE BEHAVIOR, THE PERSON WHO OWNS THAT GAMERTAG IS PUNISHED BY BEING BANNED FROM THE SERVICE. KEEP IN MIND, THIS IS NOT JUST A BAN ON A PARTICULAR GAME. THIS IS A BAN ON THE XBOX LIVE SERVICE AS A WHOLE, SO YOU WILL NOT BE ABLE TO GO ONLINE AT ALL DURING YOUR BAN