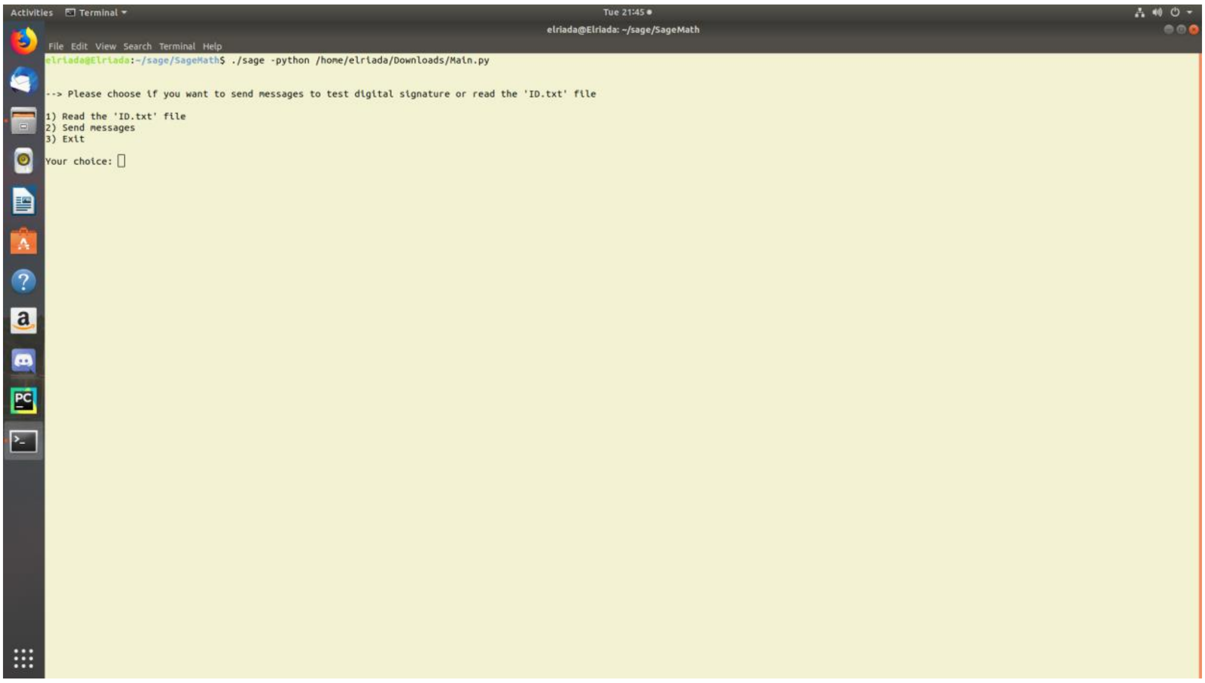
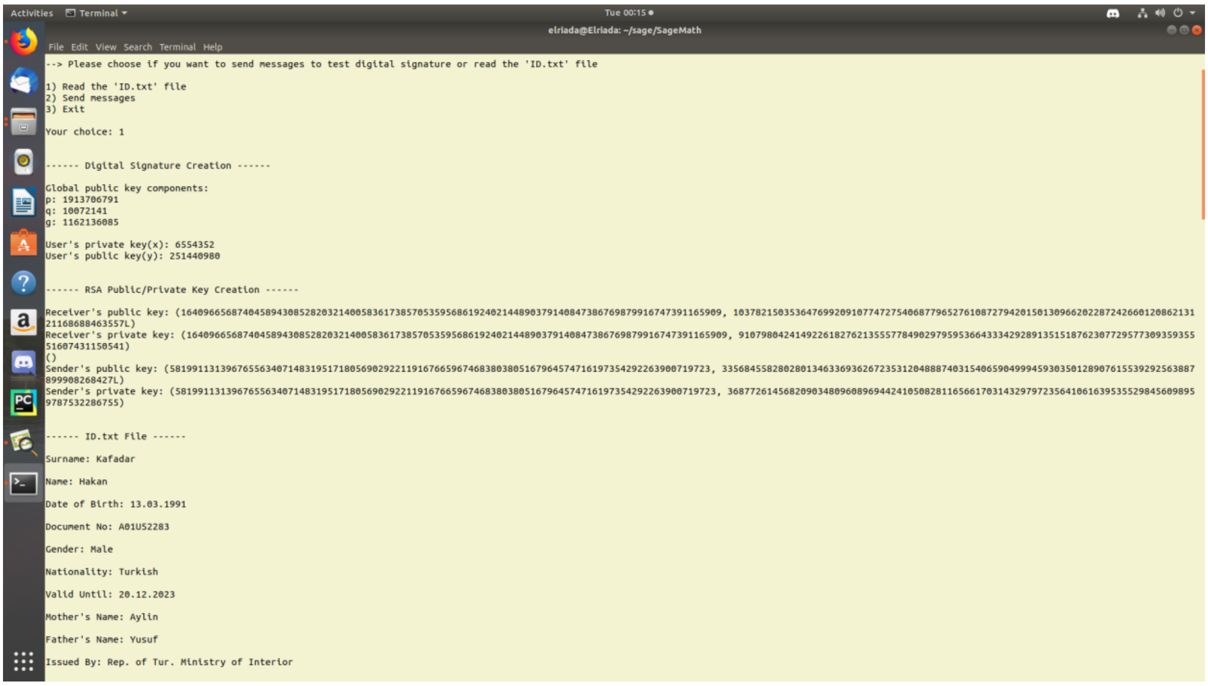
DSA (Digital Signature Algorithm):

As the third project of CE340 course we are asked to implement a Digital Signature Algorithm. DSA has got two main parts first part is creating public and private keys.

You can run sage as shown below.


Activities
Terminal ▾
Tue 21:45 ●
elriada@Elriada: ~/sage/SageMath
File Edit View Search Terminal Help

```
elriada@Elriada:~/sage/SageMath$ ./sage -python /home/elriada/Downloads/Main.py

--> Please choose if you want to send messages to test digital signature or read the 'ID.txt' file

1) Read the 'ID.txt' file
2) Send messages
3) Exit

Your choice: 
```

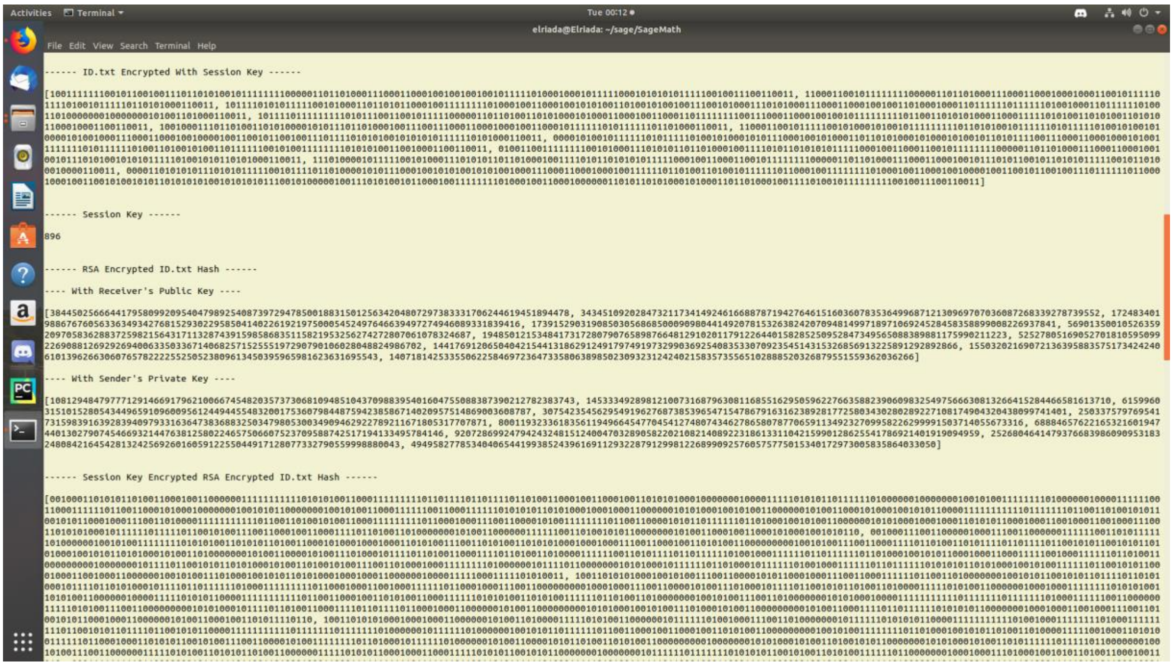

Activities
Terminal ▾
Tue 00:15 ●
elriada@Elriada: ~/sage/SageMath
File Edit View Search Terminal Help

```
--> Please choose if you want to send messages to test digital signature or read the 'ID.txt' file

1) Read the 'ID.txt' file
2) Send messages
3) Exit

Your choice: 1


------ Digital Signature Creation ------

Global public key components:
p: 1913706791
q: 10072141
g: 1162136085

User's private key(x): 6554352
User's public key(y): 251440980


------ RSA Public/Private Key Creation ------

Receiver's public key: (164096656874045894308528203214005836173857053595686192402144890379140847386769879916747391165909, 103782150353647699209107747275406877965276108727942015013096620228724266012086213121168688463557L)
Receiver's private key: (164096656874045894308528203214005836173857053595686192402144890379140847386769879916747391165909, 91079804241492261827621355577849029795953664333429289135151876230772957730935935551607431150541)
()
Sender's public key: (581991131396765563407148319517180569029221191676659674683803805167964574716197354292263900719723, 335684558280280134633693626723531204888740315406590499945930350128907615539292563887899908268427L)
Sender's private key: (581991131396765563407148319517180569029221191676659674683803805167964574716197354292263900719723, 368772614568209034809608969442410508281165661703143297972356410616395355298456098959787532286755)


------ ID.txt File ------

Surname: Kafadar

Name: Hakan

Date of Birth: 13.03.1991

Document No: A01U52283

Gender: Male

Nationality: Turkish

Valid Until: 20.12.2023

Mother's Name: Aylin

Father's Name: Yusuf

Issued By: Rep. of Tur. Ministry of Interior
```

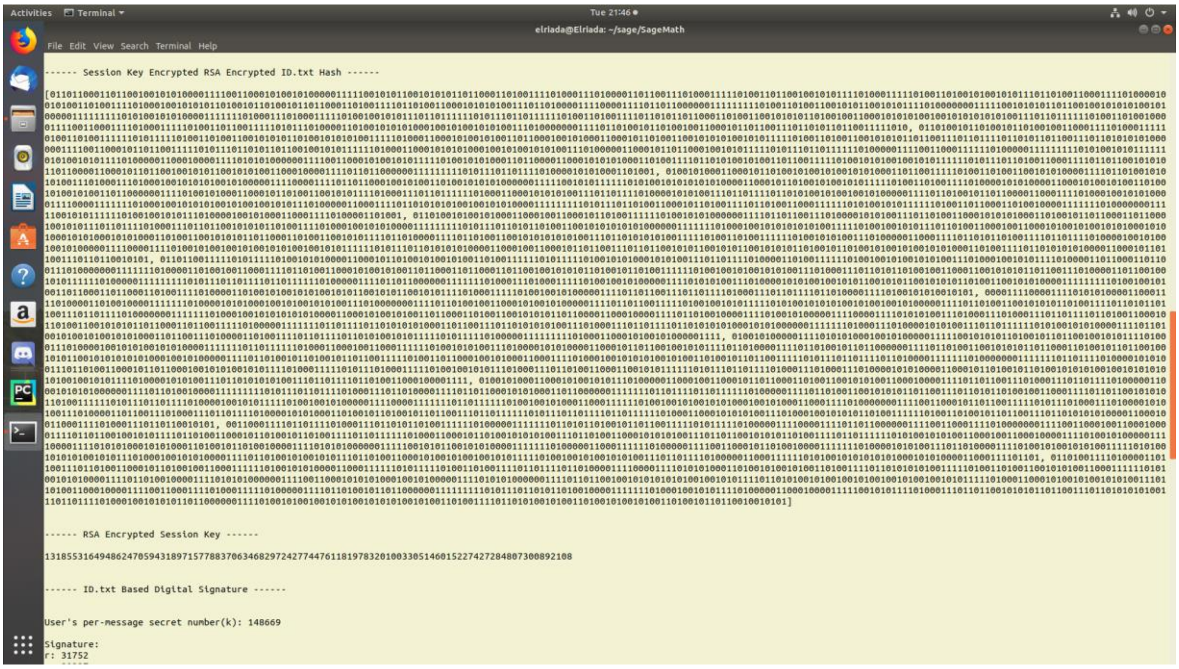
At the picture above we initialize our elements to generate our public and private keys.

Then the target file which is ID.txt in this case is being read and singed and encrypted with our private and public keys.

Some steps and outputs are shown for encryption.

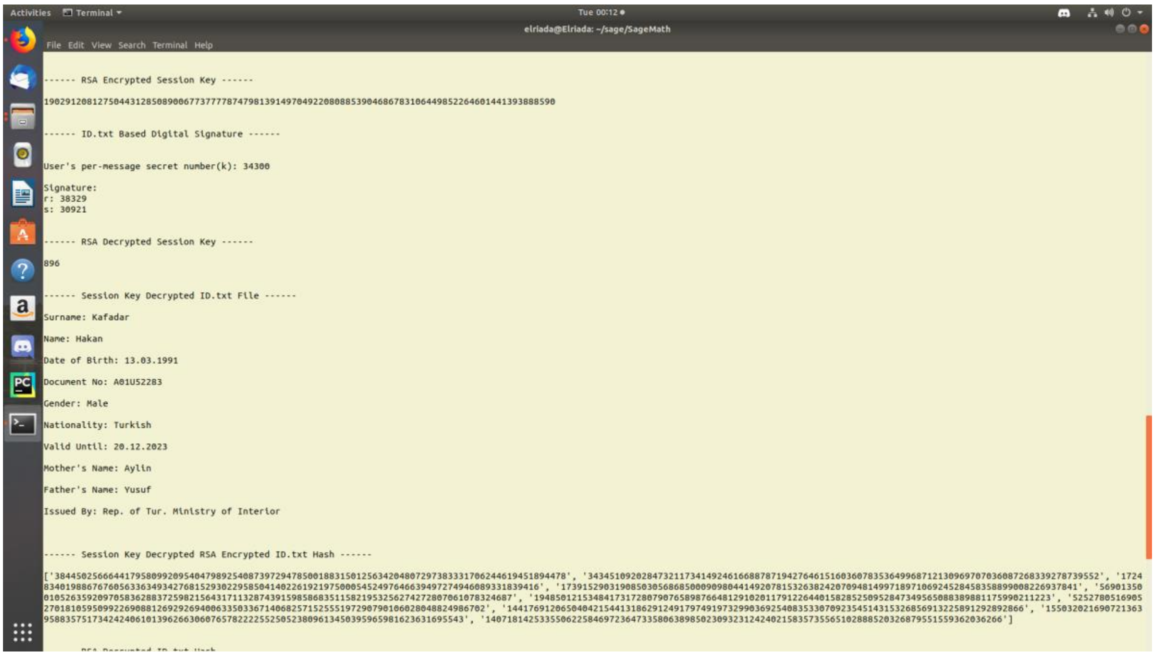


```
------ ID.txt Encrypted With Session Key ------

[illegible]

------ Session Key ------

896

------ RSA Encrypted ID.txt Hash ------

---- With Receiver's Public Key ----

[illegible]

---- With Sender's Private Key ----

[illegible]

------ Session Key Encrypted RSA Encrypted ID.txt Hash ------

[illegible]
```

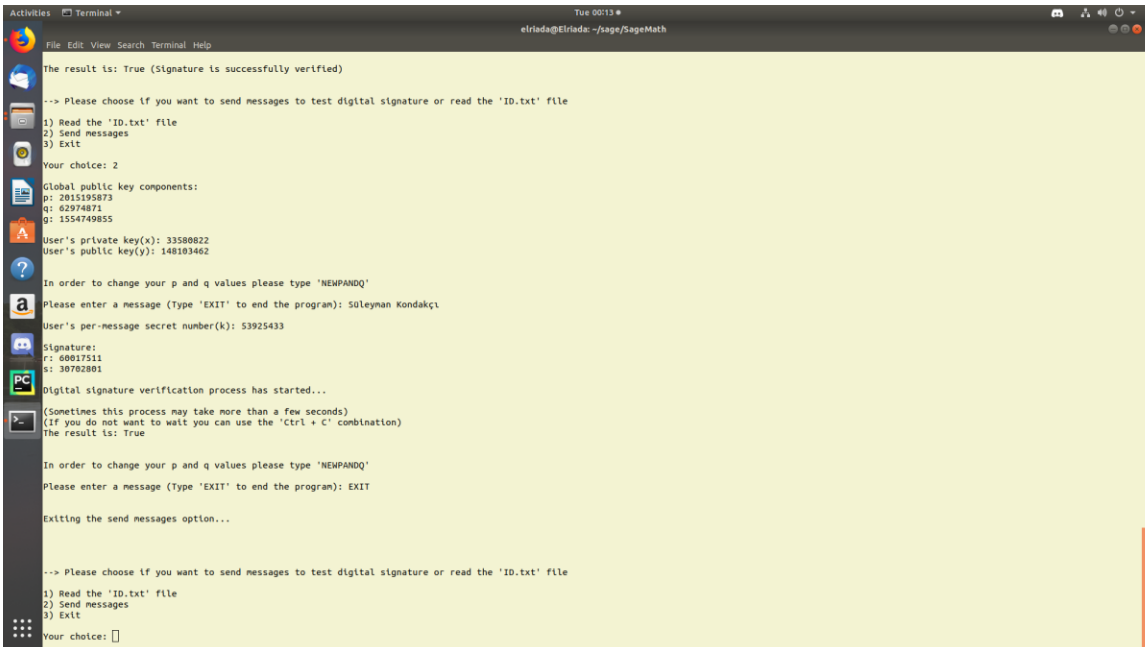

Activities
Terminal
Tue 21:46
elriada@Elriada: ~/sage/SageMath
File Edit View Search Terminal Help

```
------ Session Key Encrypted RSA Encrypted ID.txt Hash ------

[illegible]

------ RSA Encrypted Session Key ------

131855316494862470594318971577883706346829724277447611819783201003305146015227427284807300892108


------ ID.txt Based Digital Signature ------


User's per-message secret number(k): 148669

Signature:
r: 31752
```

And lastly we need to verify the signature if it is same or not.

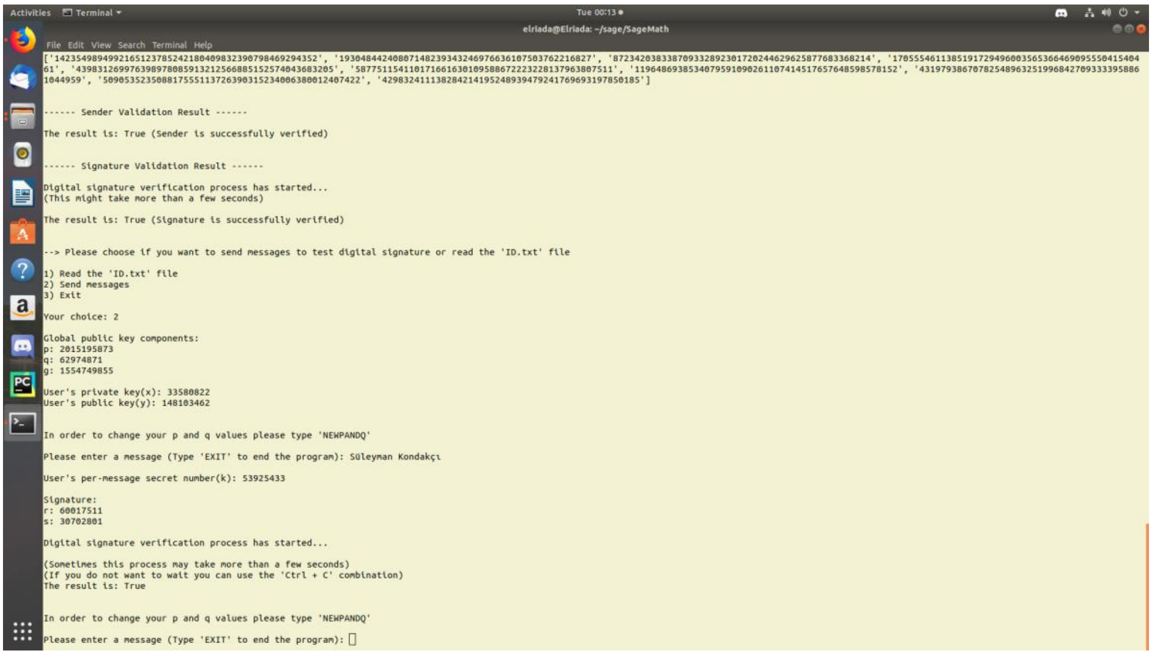

Activities
Terminal
Tue 00:12
elriada@Elriada: ~/sage/SageMath
File Edit View Search Terminal Help

```
------ RSA Encrypted Session Key ------

1902912081275044312850890067737778747981391497049220808853904686783106449852264601441393888590


------ ID.txt Based Digital Signature ------


User's per-message secret number(k): 34300

Signature:
r: 38329
s: 30921


------ RSA Decrypted Session Key ------

896


------ Session Key Decrypted ID.txt File ------

Surname: Kafadar

Name: Hakan

Date of Birth: 13.03.1991

Document No: A01U52283

Gender: Male

Nationality: Turkish

Valid Until: 20.12.2023

Mother's Name: Aylin

Father's Name: Yusuf

Issued By: Rep. of Tur. Ministry of Interior



------ Session Key Decrypted RSA Encrypted ID.txt Hash ------

['38445025666441795809920954047989254087397294785001883150125634204807297383331706244619451894478', '34345109202847321173414924616688787194276461516036078353649968712130969707036087268339278739552', '1724
83401988676760563363493427681529302295850414022619219750005452497646639497274946089331839416', '173915290319085030568685000909804414920781532638242070948149971897106924528458358899008226937841', '56901350
010526359209705836288372598215643171132874391598586835115821953256274272807061078324687', '194850121534841731728079076589876648129102011791226440158285250952847349565088389881175990211223', '5252780516905
2701810595099226908812692926940063350336714068257152555197290790106028048824986702', '144176912065040421544131862912491797491973299036925408353307092354514315326856913225891292892866', '155032021690721363
958835751734242406101396266306076578222255250523809613450395965981623631695543', '140718142533550622584697236473358063898502309323124240215835735565102888520326879551559362036266']
```


Activities
Terminal
Tue 00:13
elriada@Elriada: ~/sage/SageMath
File Edit View Search Terminal Help

```
The result is: True (Signature is successfully verified)

--> Please choose if you want to send messages to test digital signature or read the 'ID.txt' file

1) Read the 'ID.txt' file
2) Send messages
3) Exit

Your choice: 2

Global public key components:
p: 2015195873
q: 62974871
g: 1554749855

User's private key(x): 33580822
User's public key(y): 148103462

In order to change your p and q values please type 'NEWPANDQ'

Please enter a message (Type 'EXIT' to end the program): Süleyman Kondakçı

User's per-message secret number(k): 53925433

Signature:
r: 60017511
s: 30702801

Digital signature verification process has started...

(Sometimes this process may take more than a few seconds)
(If you do not want to wait you can use the 'Ctrl + C' combination)
The result is: True

In order to change your p and q values please type 'NEWPANDQ'

Please enter a message (Type 'EXIT' to end the program): EXIT


Exiting the send messages option...



--> Please choose if you want to send messages to test digital signature or read the 'ID.txt' file

1) Read the 'ID.txt' file
2) Send messages
3) Exit

Your choice: 
```

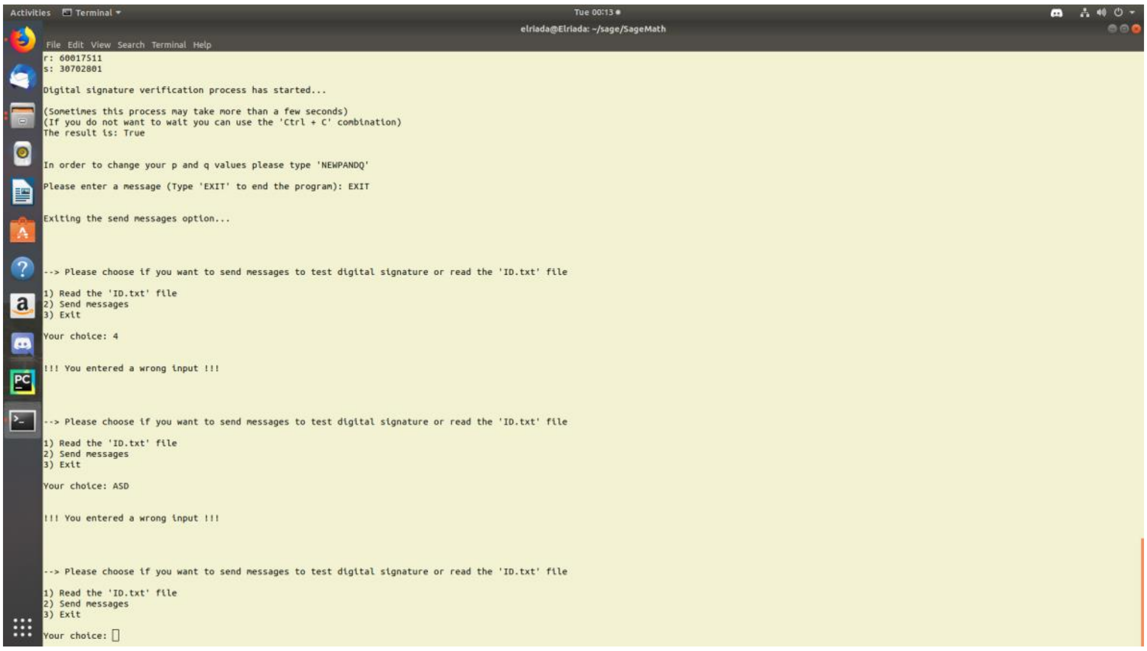
We also added an option for user so that our user can enter his/her own message.


Activities
Terminal
Tue 00:13
elriada@Elriada: ~/sage/SageMath
File Edit View Search Terminal Help

```
['142354989499216512378524218040983239079846929 4352', '193048442408071482393432469766361075037622 16827', '872342038338709332892301720244629625877683368214', '170555461138519172949600356536646909555041540461', '439831269976398978085913212566885152574043683205', '587751154110171661630109588672223228137963807511', '119648693853407959109026110741451765764859857815 2', '431979386707825489632519968427093333958861044959', '509053523508817555113726390315234006380012407422', '429832411138284214195248939479241769693197850185']


------ Sender Validation Result ------

The result is: True (Sender is successfully verified)


------ Signature Validation Result ------

Digital signature verification process has started...
(This might take more than a few seconds)

The result is: True (Signature is successfully verified)

--> Please choose if you want to send messages to test digital signature or read the 'ID.txt' file

1) Read the 'ID.txt' file
2) Send messages
3) Exit

Your choice: 2

Global public key components:
p: 2015195873
q: 62974871
g: 1554749855

User's private key(x): 33580822
User's public key(y): 148103462

In order to change your p and q values please type 'NEWPANDQ'

Please enter a message (Type 'EXIT' to end the program): Süleyman Kondakçı

User's per-message secret number(k): 53925433

Signature:
r: 60017511
s: 30702801

Digital signature verification process has started...

(Sometimes this process may take more than a few seconds)
(If you do not want to wait you can use the 'Ctrl + C' combination)
The result is: True

In order to change your p and q values please type 'NEWPANDQ'

Please enter a message (Type 'EXIT' to end the program): 
```

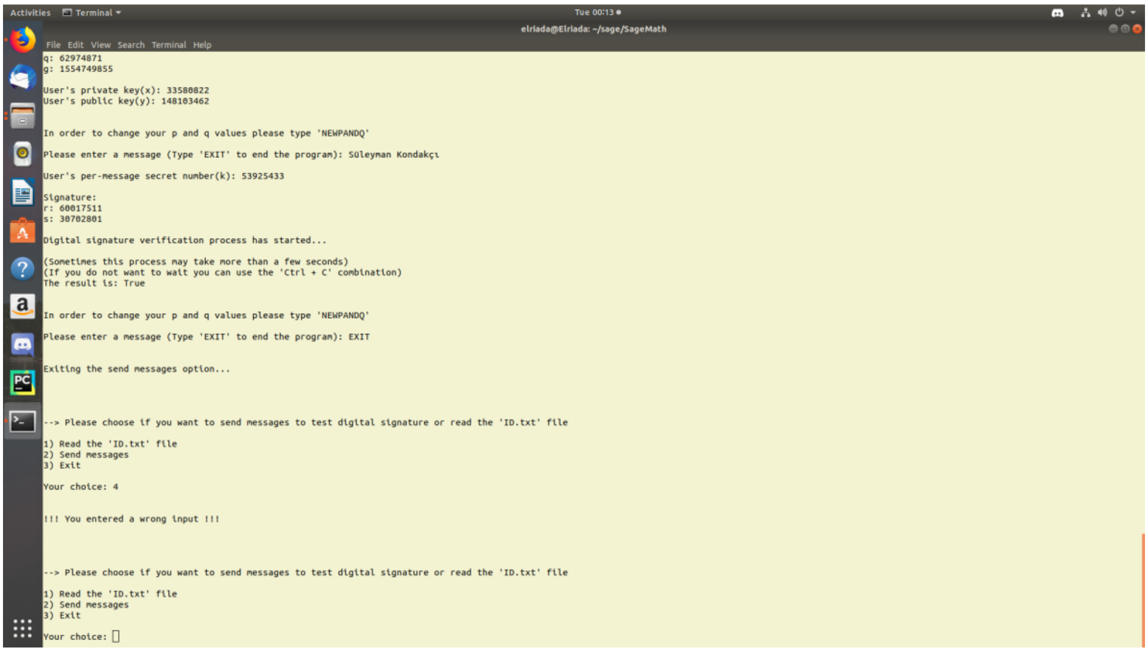
Validation is successfully done!

And we also implemented input validations to make our code more user-friendly!



Activities
Terminal
Tue 00:13
elriada@Elriada: ~/sage/SageMath
File Edit View Search Terminal Help

```
r: 60017511
s: 30702801

Digital signature verification process has started...

(Sometimes this process may take more than a few seconds)
(If you do not want to wait you can use the 'Ctrl + C' combination)
The result is: True


In order to change your p and q values please type 'NEWPANDQ'

Please enter a message (Type 'EXIT' to end the program): EXIT


Exiting the send messages option...




--> Please choose if you want to send messages to test digital signature or read the 'ID.txt' file

1) Read the 'ID.txt' file
2) Send messages
3) Exit

Your choice: 4


!!! You entered a wrong input !!!




--> Please choose if you want to send messages to test digital signature or read the 'ID.txt' file

1) Read the 'ID.txt' file
2) Send messages
3) Exit

Your choice: ASD


!!! You entered a wrong input !!!




--> Please choose if you want to send messages to test digital signature or read the 'ID.txt' file

1) Read the 'ID.txt' file
2) Send messages
3) Exit

Your choice: 
```



Activities
Terminal
Tue 00:13
elriada@Elriada: ~/sage/SageMath
File Edit View Search Terminal Help

```
q: 62974871
g: 1554749855

User's private key(x): 33580822
User's public key(y): 148103462


In order to change your p and q values please type 'NEWPANDQ'

Please enter a message (Type 'EXIT' to end the program): Süleyman Kondakçı

User's per-message secret number(k): 53925433

Signature:
r: 60017511
s: 30702801

Digital signature verification process has started...

(Sometimes this process may take more than a few seconds)
(If you do not want to wait you can use the 'Ctrl + C' combination)
The result is: True


In order to change your p and q values please type 'NEWPANDQ'

Please enter a message (Type 'EXIT' to end the program): EXIT


Exiting the send messages option...




--> Please choose if you want to send messages to test digital signature or read the 'ID.txt' file

1) Read the 'ID.txt' file
2) Send messages
3) Exit

Your choice: 4


!!! You entered a wrong input !!!




--> Please choose if you want to send messages to test digital signature or read the 'ID.txt' file

1) Read the 'ID.txt' file
2) Send messages
3) Exit

Your choice: 
```

And this is it for our DSA implementation.For more explanation of how our DSA implementation works User guide is attached to this file.

USER GUIDE:

This project aims to implement the digital signature algorithm with the rsa algorithm.

In our project we get the ID information from the 'ID.txt' file.

We create a digital signature based on the 'ID.txt' file

We get the hash value of the file with SHA-1 algorithm.

Afterwards we encrypt the hash value with both sender's private key

and receiver's public key.

Later we encrypt the receiver public key encrypted hash value with

simplified DES with the use of a session key.

Also the original 'ID.txt' file is encrypted with the session key as well.

Session key is encrypted with the receiver's public key

After these encryption steps we now send everything to the receiver.

Each decryption process is done in a reverse order of the encryption process.

We validate both the digital signature and the sender.

The source code is explained in more details with comments at each step.

In order to run the Main.py file:

- First you open the terminal
- Change your directory (with the 'cd' command) to where the 'sage' file is.
- After changing your directory enter the below command:

  './sage -python /path/to/Main.py'
- '/path/to/Main.py' indicates the exact location of the 'Main.py' file on your computer.

  For example: '/home/user_name/PycharmProject/Main.py'

For the second and arbitrary option you can enter random messages and test the DSA without any sort of encryption.