

CSE4003 - Cyber Security

Digital Assignment 1 - 10/09/2017

Prepared By - Hargur Partap Singh Bedi (15BCE1257), Kumar Shubham (15BCE1283)

Digital Assignment 1: Implementing Elliptic Curve Cryptography based on ElGamal Technique

The code for this entire project is present in [this](#) repository

Code : elgamal_ellip_curve.cpp

Output :

```
hargur@LAPTOP-H7MPSUPM: /mnt/c/Users/Hargur Bedi/Desktop$ g++ elgamal_ellip_curve.cpp
hargur@LAPTOP-H7MPSUPM: /mnt/c/Users/Hargur Bedi/Desktop$ ./a.out
Elliptic Curve General Form      y^2 mod p = (x^3 + A*x + B) mod p
Enter the value of P:
7
Enter the Value of a:
3
Enter the Value of b:
11
Current Elliptic Curve      ---> y^2 mod 7 = (x^3 + 3*x + 11) mod p

Generated Points are:
1      ( 0 , 2 )
2      ( 0 , 5 )
3      ( 1 , 1 )
4      ( 1 , 6 )
5      ( 2 , 2 )
6      ( 2 , 5 )
7      ( 5 , 2 )
8      ( 5 , 5 )
9      ( 6 , 0 )
Base Point: (0,2)
Enter the random number 'd' i.e. Private key of Sender (d<n)
5
Enter the random number 'k' (k<n)
6
```

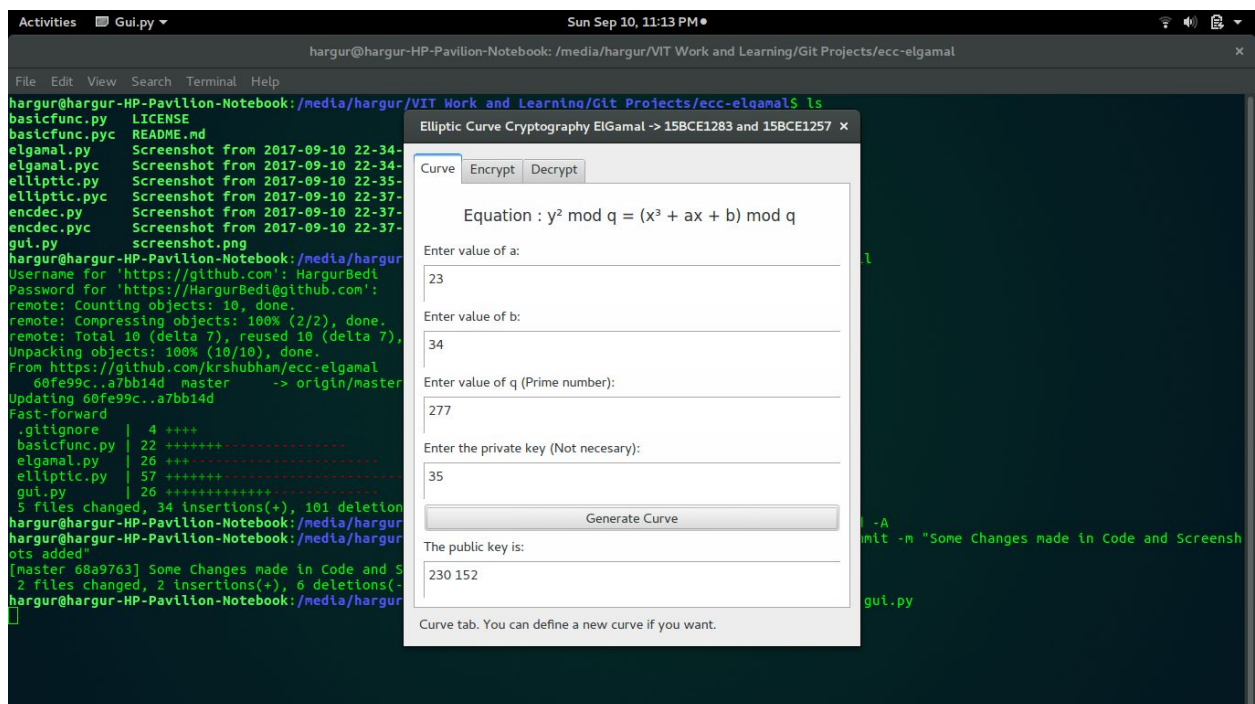
```
hargur@LAPTOP-H7MPSUPM: /mnt/c/Users/Hargur Bedi/Desktop
Enter the Value of a:
3
Enter the Value of b:
11
Current Elliptic Curve      ---> y^2 mod 7 = (x^3 + 3*x + 11) mod p

Generated Points are:
1      ( 0 , 2 )
2      ( 0 , 5 )
3      ( 1 , 1 )
4      ( 1 , 6 )
5      ( 2 , 2 )
6      ( 2 , 5 )
7      ( 5 , 2 )
8      ( 5 , 5 )
9      ( 6 , 0 )
Base Point: (0,2)
Enter the random number 'd' i.e. Private key of Sender (d<n)
5
Enter the random number 'k' (k<n)
3
Enter the message to be sent:
123
The message to be sent is:
123
Value of C1: (0,6)
Value of C2: (123,153)

The message received is:
123hargur@LAPTOP-H7MPSUPM: /mnt/c/Users/Hargur Bedi/Desktop$
```

Now the whole implementation in Python :

Output :



The screenshot shows a terminal window with a git commit message and a GUI application titled "Elliptic Curve Cryptography ElGamal -> 15BCE1283 and 15BCE1257". The GUI has tabs for "Curve", "Encrypt", and "Decrypt". The "Curve" tab is active, showing the equation $y^2 \bmod q = (x^3 + ax + b) \bmod q$. The input fields are filled with: a=23, b=34, q=277, and private key=35. The "Generate Curve" button is highlighted. Below the button, it says "The public key is: 230 152". At the bottom, it says "Curve tab. You can define a new curve if you want."

```
hargur@hargur-HP-Pavillon-Notebook: /media/hargur/VIT Work and Learning/Git Projects/ecc-elgamal$ ls
basicfunc.py  LICENSE
basicfunc.pyc README.md
elgamal.py    Screenshot from 2017-09-10 22-34-
elgamal.pyc   Screenshot from 2017-09-10 22-34-
elliptic.py   Screenshot from 2017-09-10 22-35-
elliptic.pyc  Screenshot from 2017-09-10 22-37-
encdec.py     Screenshot from 2017-09-10 22-37-
encdec.pyc    Screenshot from 2017-09-10 22-37-
gui.py        screenshot.png
hargur@hargur-HP-Pavillon-Notebook: /media/hargur
Username for 'https://github.com': HargurBedi
Password for 'https://HargurBedi@github.com':
remote: Counting objects: 10, done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 10 (delta 7), reused 10 (delta 7),
Unpacking objects: 100% (10/10), done.
From https://github.com/krishubhan/ecc-elgamal
   60fe99c..a7bb14d  master    -> origin/master
Updating 60fe99c..a7bb14d
Fast-forward
 .gitignore      | 4 ++++
 basicfunc.py    | 22 ++++++-----
 elgamal.py      | 26 ++++++-----
 elliptic.py     | 57 ++++++-----
 gui.py          | 26 ++++++-----
 5 files changed, 34 insertions(+), 101 deletions
hargur@hargur-HP-Pavillon-Notebook: /media/hargur
hargur@hargur-HP-Pavillon-Notebook: /media/hargur
ots added"
[master 68a9763] Some Changes made in Code and S
 2 files changed, 2 insertions(+), 6 deletions(-)
hargur@hargur-HP-Pavillon-Notebook: /media/hargur
```

