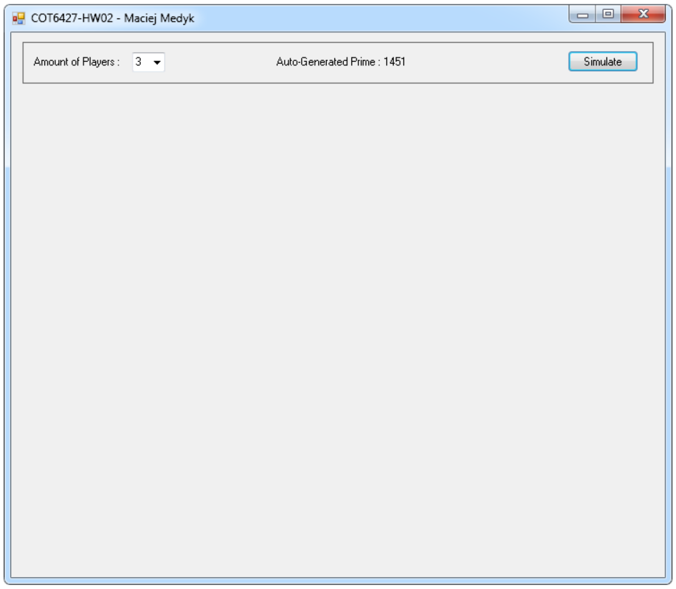
Maciej Medyk – COT6427 – Secret Sharing Algorythms – Homework 02

Question 1 – Write a computer program to simulate secure MPC for the addition and multiplicationgates.

For the assignment, I have chosen option 1 which is creation of computer program. In the program, you choose number of players from 3 to 7 and prime number is auto generated between 50 – 2000. Once you hit button simulate, the program will allow to enter the private key for each player while generating public keys that will be sendout. The formulas for generating public key is randomized. Once all players are entered you are given a choice of selecting either an addition gate or multiplication gate. At that moment gate calculations will display. Lastly, the button MPC will appear and once you click it it will give you a result of the addition or multiplication using modulo the prime number.

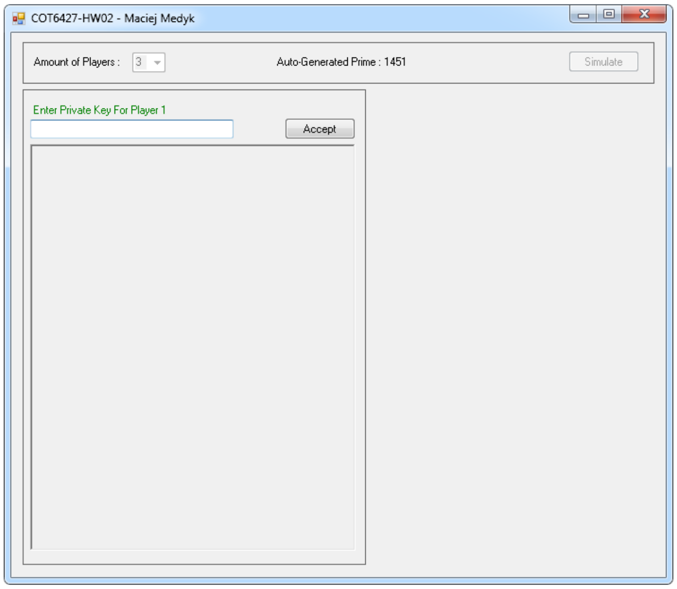
Below are the screenshots of addition gate operations first, followed by multiplication operations.

Addition gate example. Private keys entered are 10 + 20 + 30 = 60


COT6427-HW02 - Maciej Medyk

Amount of Players : 3

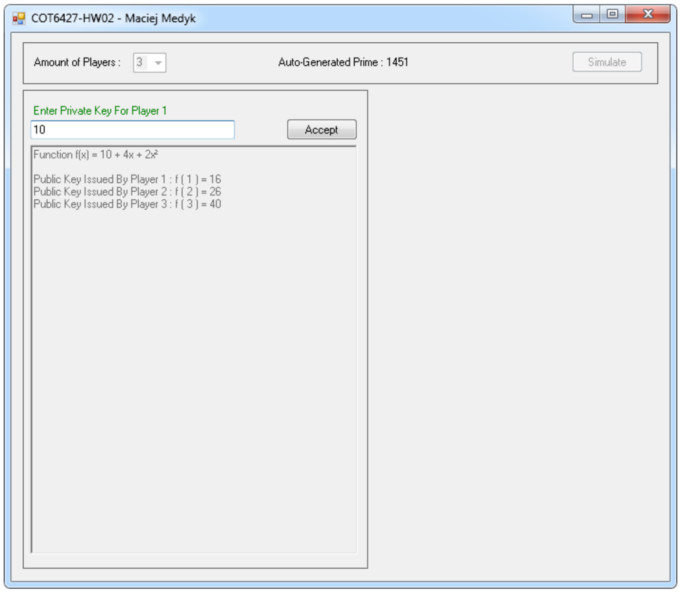
Auto-Generated Prime : 1451


COT6427-HW02 - Maciej Medyk

Amount of Players : 3

Auto-Generated Prime : 1451

Enter Private Key For Player 1


COT6427-HW02 - Maciej Medyk

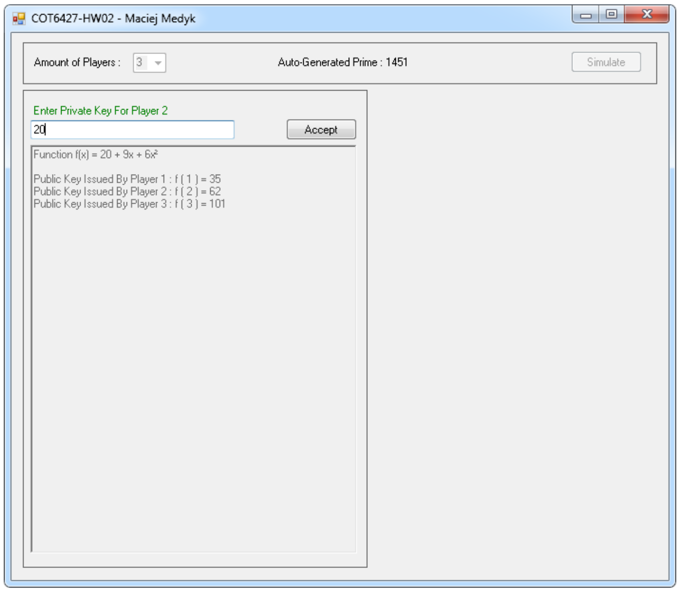
Amount of Players : 3

Auto-Generated Prime : 1451

Enter Private Key For Player 1

10

```
Function f(x) = 10 + 4x + 2x²

Public Key Issued By Player 1 : f ( 1 ) = 16
Public Key Issued By Player 2 : f ( 2 ) = 26
Public Key Issued By Player 3 : f ( 3 ) = 40
```


COT6427-HW02 - Maciej Medyk

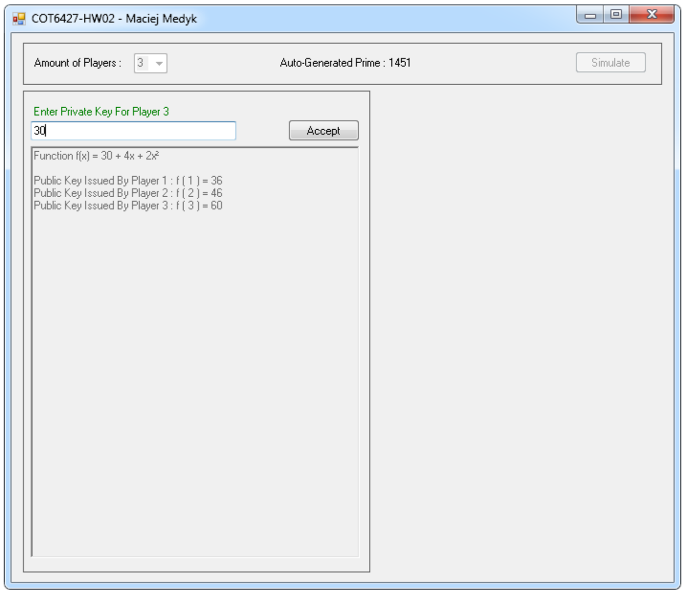
Amount of Players : 3

Auto-Generated Prime : 1451

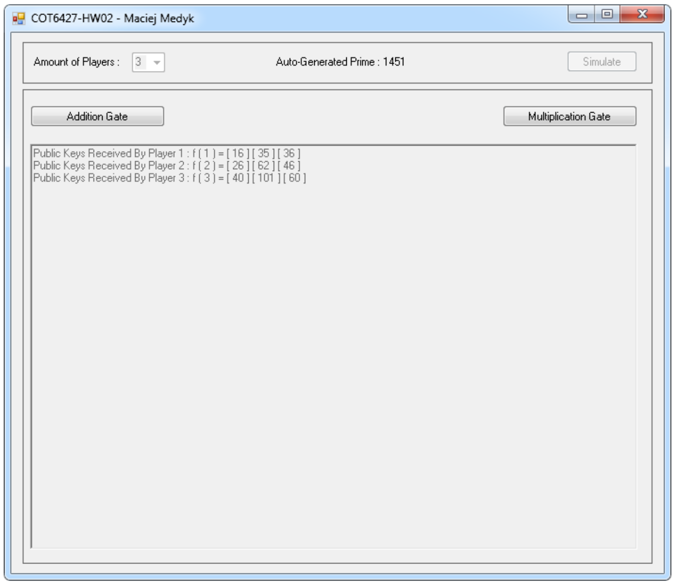
Enter Private Key For Player 2

20

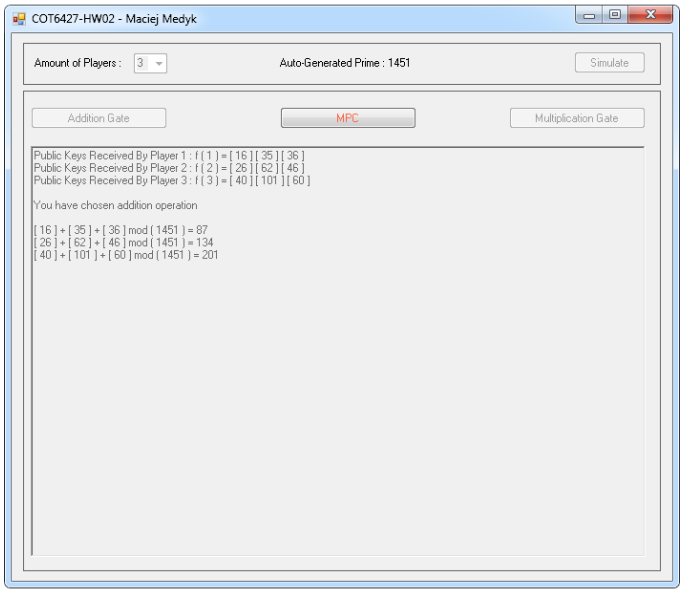
```
Function f(x) = 20 + 9x + 6x²

Public Key Issued By Player 1 : f ( 1 ) = 35
Public Key Issued By Player 2 : f ( 2 ) = 62
Public Key Issued By Player 3 : f ( 3 ) = 101
```



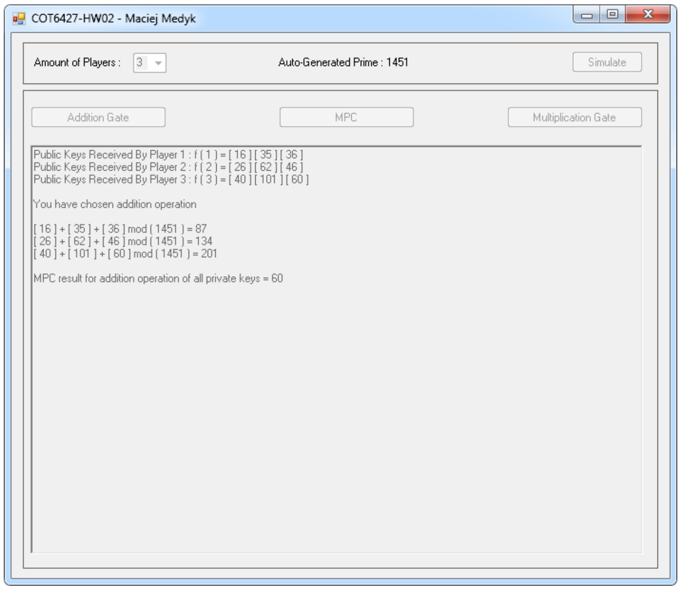
```
Amount of Players : 3
Auto-Generated Prime : 1451

Enter Private Key For Player 3
30

Function f(x) = 30 + 4x + 2x²

Public Key Issued By Player 1 : f ( 1 ) = 36
Public Key Issued By Player 2 : f ( 2 ) = 46
Public Key Issued By Player 3 : f ( 3 ) = 60
```



```
Amount of Players : 3
Auto-Generated Prime : 1451

Public Keys Received By Player 1 : f ( 1 ) = [ 16 ] [ 35 ] [ 36 ]
Public Keys Received By Player 2 : f ( 2 ) = [ 26 ] [ 62 ] [ 46 ]
Public Keys Received By Player 3 : f ( 3 ) = [ 40 ] [ 101 ] [ 60 ]
```

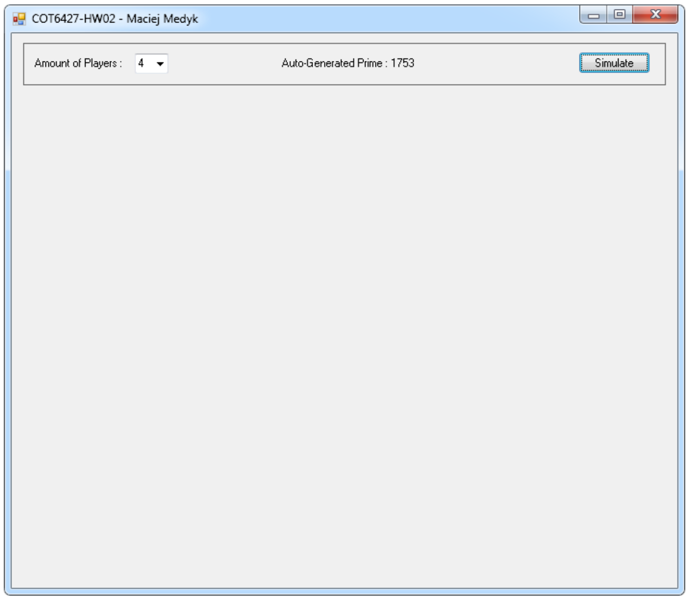


```
Amount of Players : 3
Auto-Generated Prime : 1451

Public Keys Received By Player 1 : f ( 1 ) = [ 16 ] [ 35 ] [ 36 ]
Public Keys Received By Player 2 : f ( 2 ) = [ 26 ] [ 62 ] [ 46 ]
Public Keys Received By Player 3 : f ( 3 ) = [ 40 ] [ 101 ] [ 60 ]

You have chosen addition operation

[ 16 ] + [ 35 ] + [ 36 ] mod ( 1451 ) = 87
[ 26 ] + [ 62 ] + [ 46 ] mod ( 1451 ) = 134
[ 40 ] + [ 101 ] + [ 60 ] mod ( 1451 ) = 201
```

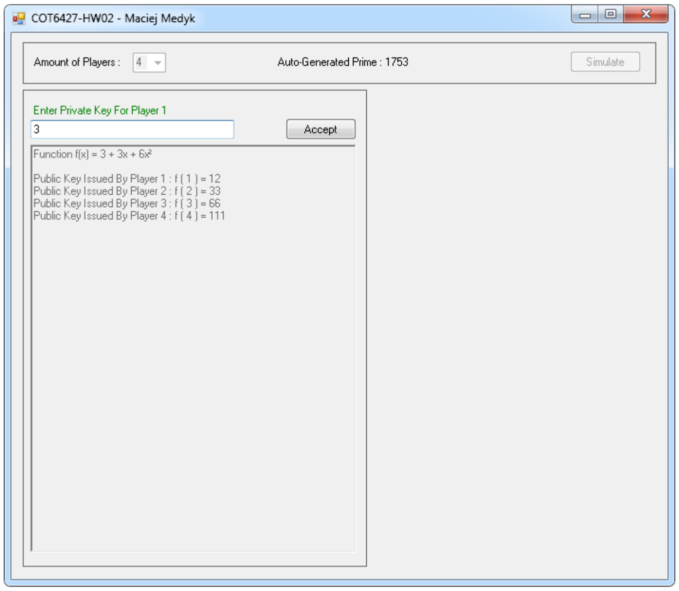


```
Amount of Players : 3
Auto-Generated Prime : 1451

Public Keys Received By Player 1 : f ( 1 ) = [ 16 ] [ 35 ] [ 36 ]
Public Keys Received By Player 2 : f ( 2 ) = [ 26 ] [ 62 ] [ 46 ]
Public Keys Received By Player 3 : f ( 3 ) = [ 40 ] [ 101 ] [ 60 ]

You have chosen addition operation

[ 16 ] + [ 35 ] + [ 36 ] mod ( 1451 ) = 87
[ 26 ] + [ 62 ] + [ 46 ] mod ( 1451 ) = 134
[ 40 ] + [ 101 ] + [ 60 ] mod ( 1451 ) = 201

MPC result for addition operation of all private keys = 60
```

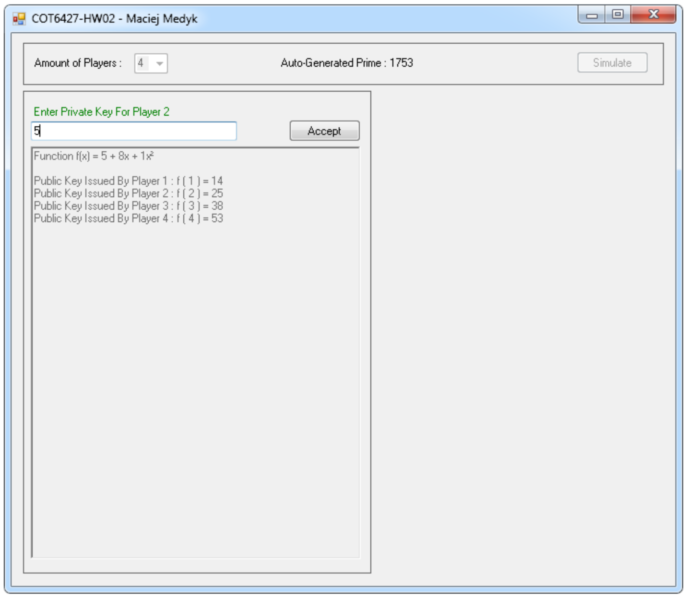
Multiplication gate example. Private keys entered are 3 * 5 *8 * 11 = 1320



```
Amount of Players : 4
Auto-Generated Prime : 1753
```



```
Amount of Players : 4
Auto-Generated Prime : 1753

Enter Private Key For Player 1
3

Function f(x) = 3 + 3x + 6x²

Public Key Issued By Player 1 : f ( 1 ) = 12
Public Key Issued By Player 2 : f ( 2 ) = 33
Public Key Issued By Player 3 : f ( 3 ) = 66
Public Key Issued By Player 4 : f ( 4 ) = 111
```



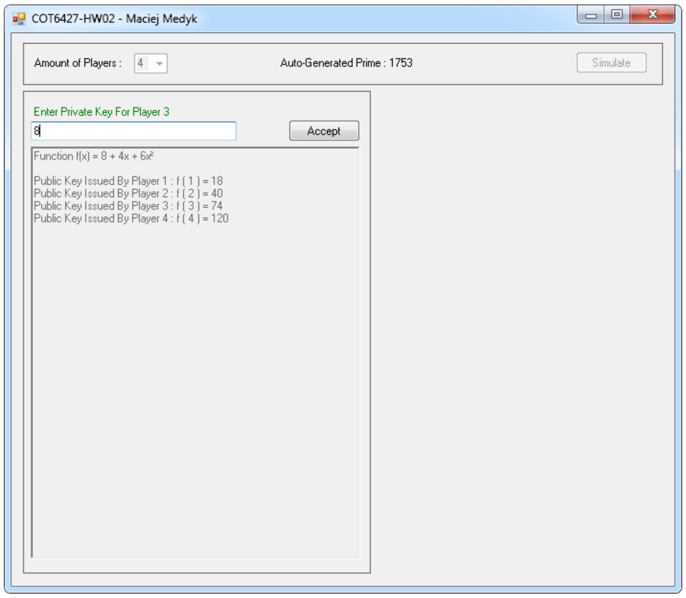
Amount of Players : 4

Auto-Generated Prime : 1753

Enter Private Key For Player 2

5

```
Function f(x) = 5 + 8x + 1x²

Public Key Issued By Player 1 : f ( 1 ) = 14
Public Key Issued By Player 2 : f ( 2 ) = 25
Public Key Issued By Player 3 : f ( 3 ) = 38
Public Key Issued By Player 4 : f ( 4 ) = 53
```



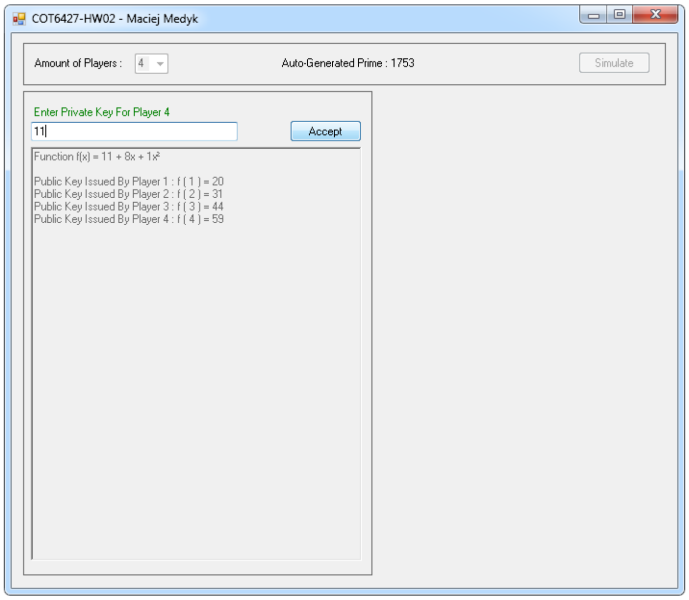
Amount of Players : 4

Auto-Generated Prime : 1753

Enter Private Key For Player 3

8

```
Function f(x) = 8 + 4x + 6x²

Public Key Issued By Player 1 : f ( 1 ) = 18
Public Key Issued By Player 2 : f ( 2 ) = 40
Public Key Issued By Player 3 : f ( 3 ) = 74
Public Key Issued By Player 4 : f ( 4 ) = 120
```



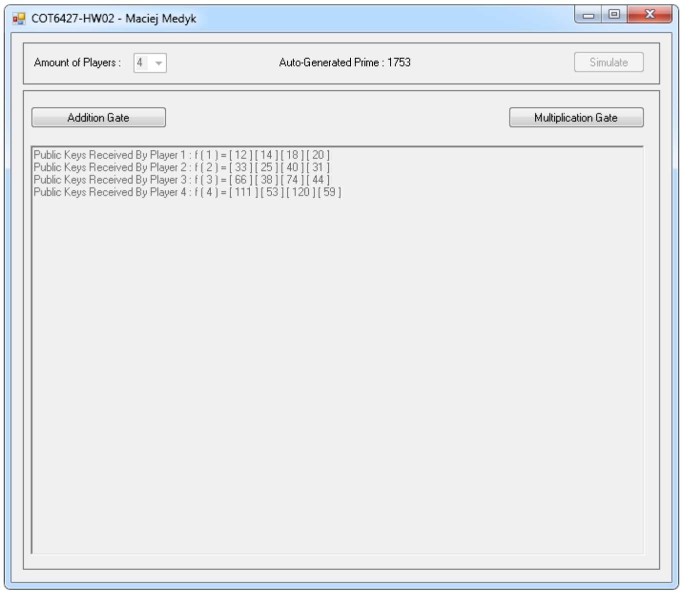
Amount of Players : 4

Auto-Generated Prime : 1753

Enter Private Key For Player 4

11

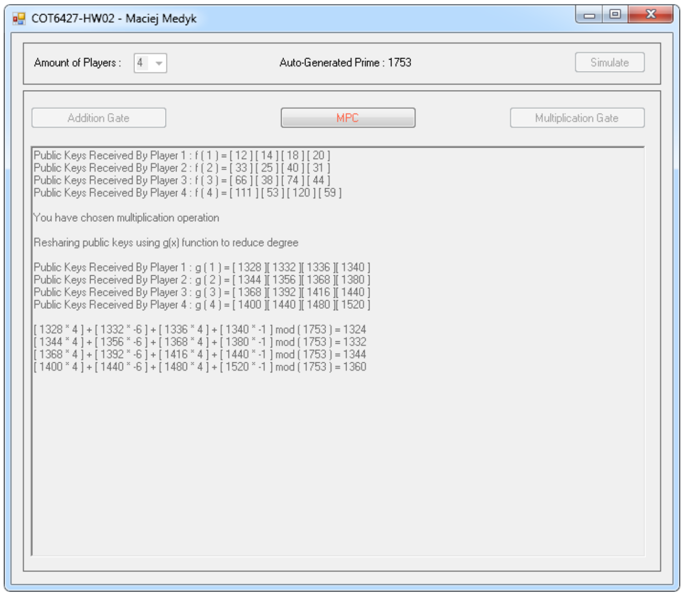
```
Function f(x) = 11 + 8x + 1x²

Public Key Issued By Player 1 : f ( 1 ) = 20
Public Key Issued By Player 2 : f ( 2 ) = 31
Public Key Issued By Player 3 : f ( 3 ) = 44
Public Key Issued By Player 4 : f ( 4 ) = 59
```



Amount of Players : 4

Auto-Generated Prime : 1753

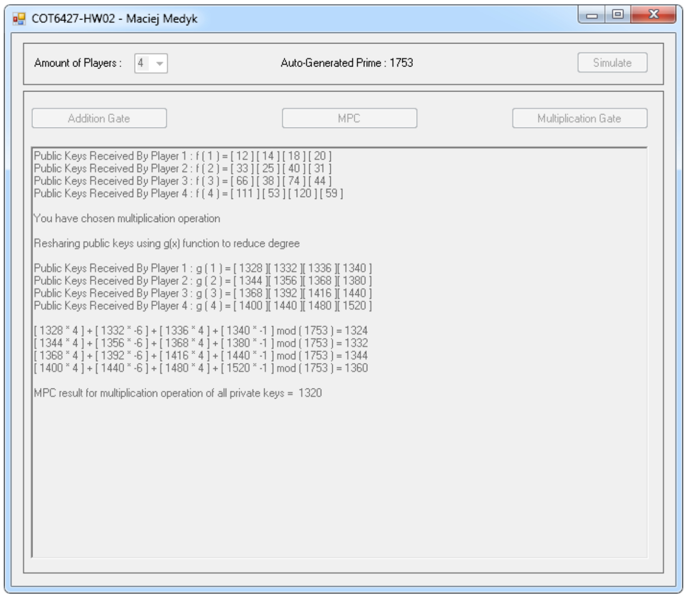
```
Public Keys Received By Player 1 : f ( 1 ) = [ 12 ] [ 14 ] [ 18 ] [ 20 ]
Public Keys Received By Player 2 : f ( 2 ) = [ 33 ] [ 25 ] [ 40 ] [ 31 ]
Public Keys Received By Player 3 : f ( 3 ) = [ 66 ] [ 38 ] [ 74 ] [ 44 ]
Public Keys Received By Player 4 : f ( 4 ) = [ 111 ] [ 53 ] [ 120 ] [ 59 ]
```



Amount of Players : 4

Auto-Generated Prime : 1753

```
Public Keys Received By Player 1 : f ( 1 ) = [ 12 ] [ 14 ] [ 18 ] [ 20 ]
Public Keys Received By Player 2 : f ( 2 ) = [ 33 ] [ 25 ] [ 40 ] [ 31 ]
Public Keys Received By Player 3 : f ( 3 ) = [ 66 ] [ 38 ] [ 74 ] [ 44 ]
Public Keys Received By Player 4 : f ( 4 ) = [ 111 ] [ 53 ] [ 120 ] [ 59 ]

You have chosen multiplication operation

Resharing public keys using g(x) function to reduce degree

Public Keys Received By Player 1 : g ( 1 ) = [ 1328 ][ 1332 ][ 1336 ][ 1340 ]
Public Keys Received By Player 2 : g ( 2 ) = [ 1344 ][ 1356 ][ 1368 ][ 1380 ]
Public Keys Received By Player 3 : g ( 3 ) = [ 1368 ][ 1392 ][ 1416 ][ 1440 ]
Public Keys Received By Player 4 : g ( 4 ) = [ 1400 ][ 1440 ][ 1480 ][ 1520 ]

[ 1328 * 4 ] + [ 1332 * -6 ] + [ 1336 * 4 ] + [ 1340 * -1 ] mod ( 1753 ) = 1324
[ 1344 * 4 ] + [ 1356 * -6 ] + [ 1368 * 4 ] + [ 1380 * -1 ] mod ( 1753 ) = 1332
[ 1368 * 4 ] + [ 1392 * -6 ] + [ 1416 * 4 ] + [ 1440 * -1 ] mod ( 1753 ) = 1344
[ 1400 * 4 ] + [ 1440 * -6 ] + [ 1480 * 4 ] + [ 1520 * -1 ] mod ( 1753 ) = 1360
```



Amount of Players : 4

Auto-Generated Prime : 1753

```
Public Keys Received By Player 1 : f ( 1 ) = [ 12 ] [ 14 ] [ 18 ] [ 20 ]
Public Keys Received By Player 2 : f ( 2 ) = [ 33 ] [ 25 ] [ 40 ] [ 31 ]
Public Keys Received By Player 3 : f ( 3 ) = [ 66 ] [ 38 ] [ 74 ] [ 44 ]
Public Keys Received By Player 4 : f ( 4 ) = [ 111 ] [ 53 ] [ 120 ] [ 59 ]

You have chosen multiplication operation

Resharing public keys using g(x) function to reduce degree

Public Keys Received By Player 1 : g ( 1 ) = [ 1328 ][ 1332 ][ 1336 ][ 1340 ]
Public Keys Received By Player 2 : g ( 2 ) = [ 1344 ][ 1356 ][ 1368 ][ 1380 ]
Public Keys Received By Player 3 : g ( 3 ) = [ 1368 ][ 1392 ][ 1416 ][ 1440 ]
Public Keys Received By Player 4 : g ( 4 ) = [ 1400 ][ 1440 ][ 1480 ][ 1520 ]

[ 1328 * 4 ] + [ 1332 * -6 ] + [ 1336 * 4 ] + [ 1340 * -1 ] mod ( 1753 ) = 1324
[ 1344 * 4 ] + [ 1356 * -6 ] + [ 1368 * 4 ] + [ 1380 * -1 ] mod ( 1753 ) = 1332
[ 1368 * 4 ] + [ 1392 * -6 ] + [ 1416 * 4 ] + [ 1440 * -1 ] mod ( 1753 ) = 1344
[ 1400 * 4 ] + [ 1440 * -6 ] + [ 1480 * 4 ] + [ 1520 * -1 ] mod ( 1753 ) = 1360

MPC result for multiplication operation of all private keys =  1320
```

Code can be found at link : https://www.dropbox.com/s/r5b8bf4gk32kk66/Homework%20-%2002%20-%20Code.zip?dl=0