Digital-Signature-Std-Assignment-6_CS6530

Digital Signature Standard (DSS) Assignment-6 Cryptography.

Name- Ayub Shaikh

Roll Number:- CS21M515 Email-Id - Ayub.Shaikh.Vahid@gmail.com

The program is in C- language. name of program file is- **DigitalSignaturesStdAlgo.c**

To generate binary EXE file use this command -

```
gcc DigitalSignaturesStdAlgo.c -o main-lgmp
```

and then run the exe.

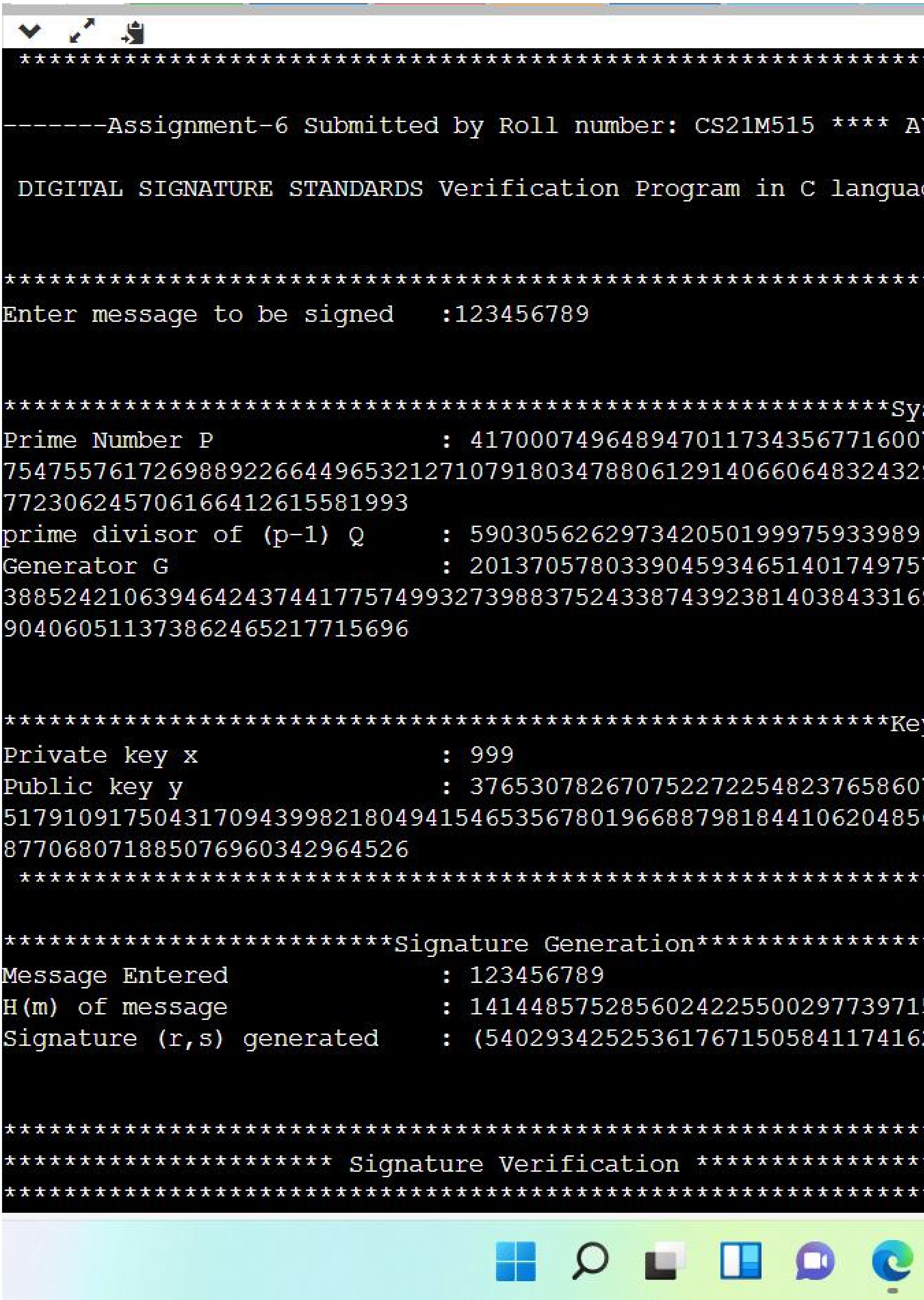
Or directly compile the program DigitalSignaturesStdAlgo.c and sha_256.h programs it will run the We can use the online c compiler to Run this as well just add these 2 files DigitalSignaturesStdAlgo.c and sha_256.h and it will run the program easy way.

(online compiler to run the program https://www.onlinegdb.com/online_c_compiler)

Sample Output 1 :

1. Enter the message: any number can enter below is example msg is-123456789

2. then program do the key generation and signature generation as per screen shot.



```
 ************************************************************

-------Assignment-6 Submitted by Roll number: CS21M515 **** A

 DIGITAL SIGNATURE STANDARDS Verification Program in C langua


************************************************************
Enter message to be signed    :123456789


***********************************************************Sy
Prime Number P                : 417000749648947011734356771600
7547557617269889226644965321271079180347880612914066064832432
77230624570616641261558199 3
prime divisor of (p-1) Q      : 590305626297342050199975933989
Generator G                   : 201370578033904593465140174975
3885242106394642437441775749932739883752433874392381403843316
90406051137386246521771569 6


***********************************************************Ke
Private key x                 : 999
Public key y                  : 376530782670752272254823765860
5179109175043170943998218049415465356780196688798184410620485
87706807188507696034296452 6
 ************************************************************

**************************Signature Generation***************
Message Entered               : 123456789
H(m) of message               : 141448575285602422550029773971
Signature (r,s) generated     : (54029342525361767150584117416


*************************************************************
********************** Signature Verification ***************
*************************************************************
```

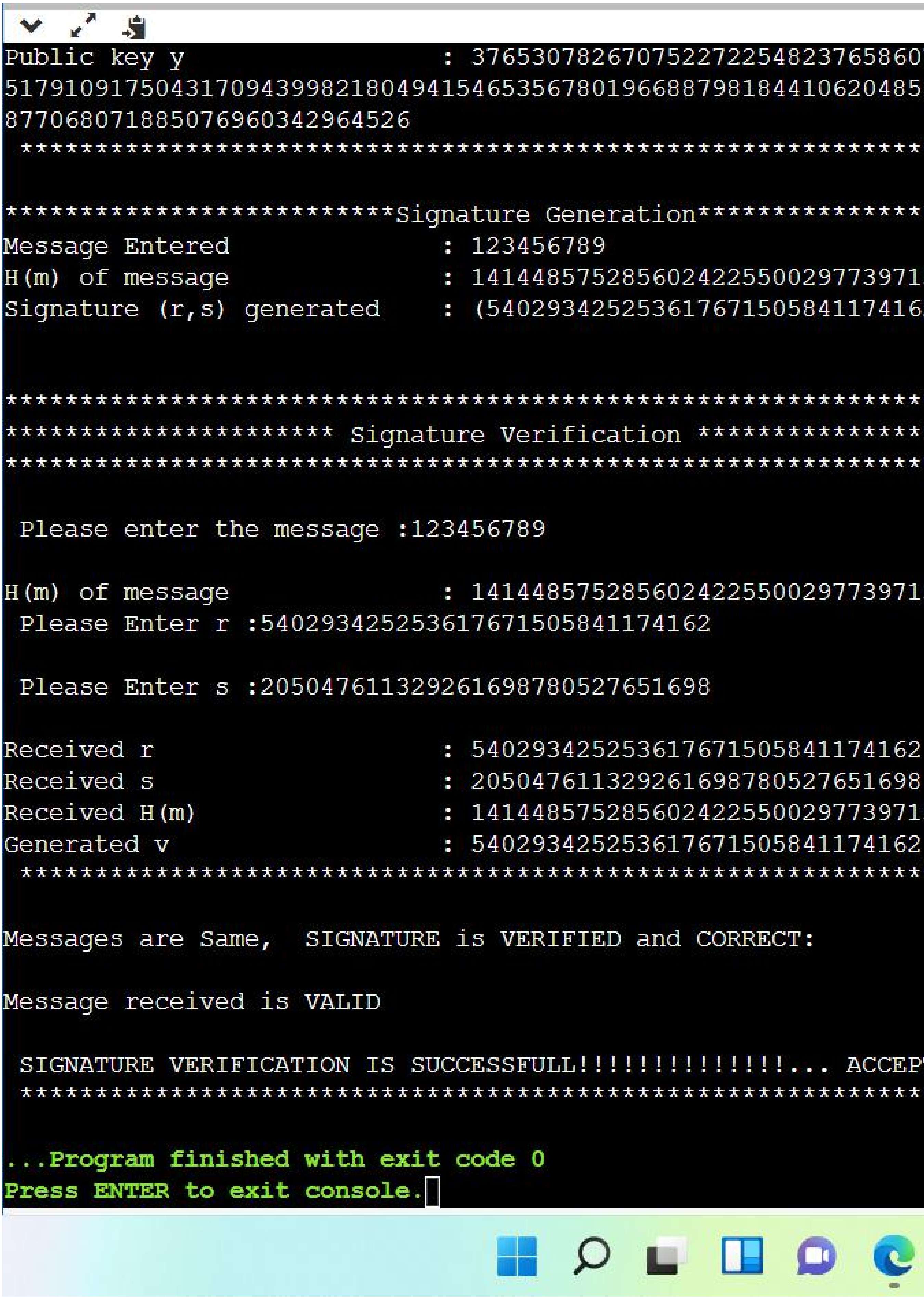
Now to verfiy the Signature belwo is screen shot

1.

we enter the same message which entered initially to check - msg is- **123456789**

then we enter the r and s to verify Signature as below screen shot we enter correct data of r and s and message and signature is same so it gives the Successful message as per belwo screen shot **SIGNATURE VERIFICATION IS SUCCESSFULL!!!!!!!!!!!!!!... ACCEPTED..!! :-) :-)

**

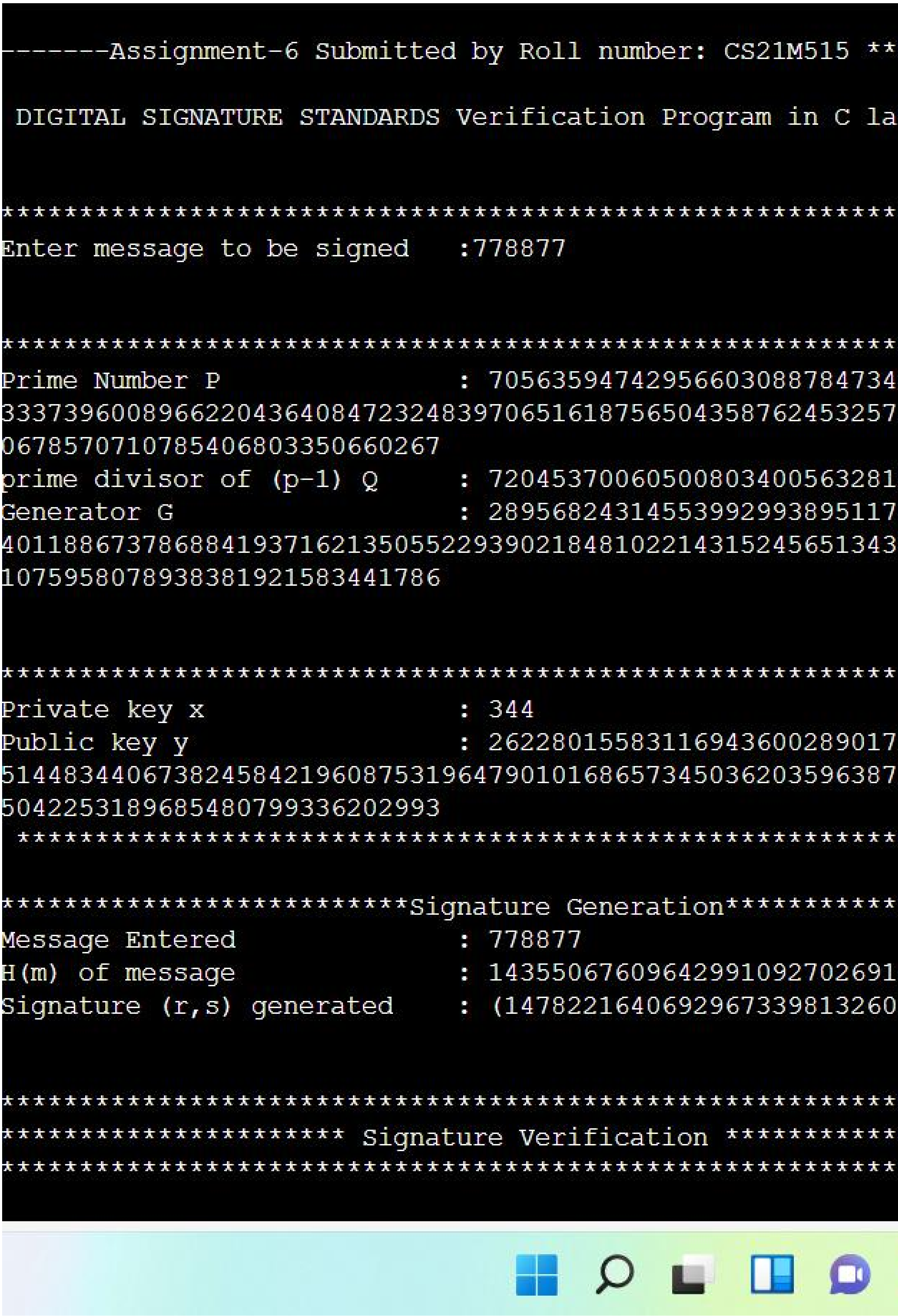


```
Public key y                 : 376530782670752272254823765860
5179109175043170943998218049415465356780196688798184410620485
877068071885076960342964526
 ************************************************************


**************************Signature Generation***************
Message Entered              : 123456789
H(m) of message              : 141448575285602422550029773971
Signature (r,s) generated    : (54029342525361767150584117416


************************************************************
********************** Signature Verification ***************
************************************************************


 Please enter the message :123456789

H(m) of message              : 141448575285602422550029773971
 Please Enter r :540293425253617671505841174162

 Please Enter s :205047611329261698780527651698

Received r                   : 540293425253617671505841174162
Received s                   : 205047611329261698780527651698
Received H(m)                : 141448575285602422550029773971
Generated v                  : 540293425253617671505841174162
 ************************************************************

Messages are Same,  SIGNATURE is VERIFIED and CORRECT:

Message received is VALID

 SIGNATURE VERIFICATION IS SUCCESSFULL!!!!!!!!!!!!!... ACCEP
 ************************************************************


...Program finished with exit code 0
Press ENTER to exit console.
```

2.

Sample Output 2 :

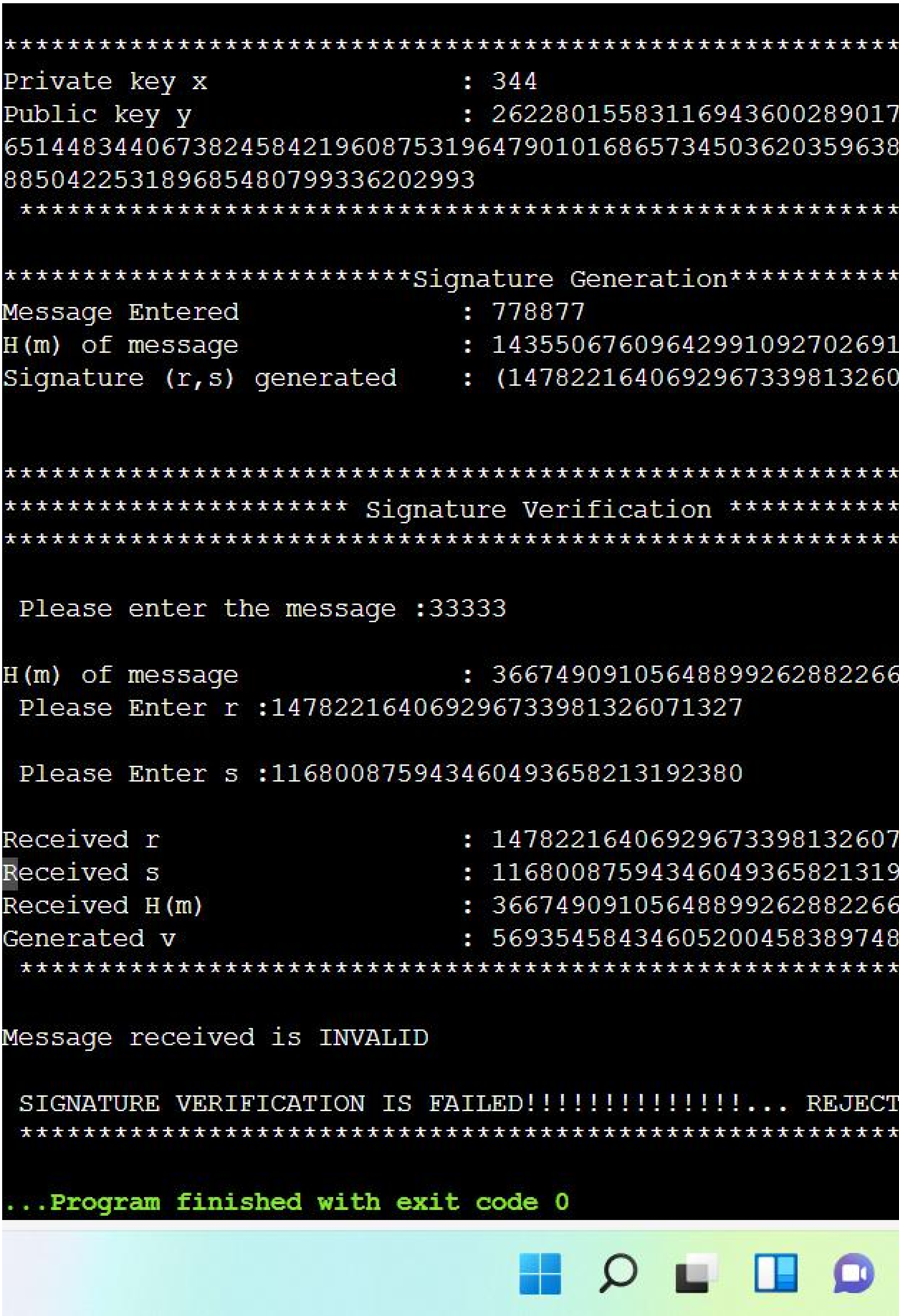
1. Test number message is entered is **778877**



```
-------Assignment-6 Submitted by Roll number: CS21M515 **

 DIGITAL SIGNATURE STANDARDS Verification Program in C la


*********************************************************
Enter message to be signed    :778877



*********************************************************
Prime Number P                : 7056359474295660308878473
3337396008966220436408472324839706516187565043587624532570
0678570710785406803350660267
prime divisor of (p-1) Q      : 7204537006050080340056328
Generator G                   : 2895682431455399299389511
4011886737868841937162135055229390218481022143152456513430
10759580789383819215834417886



*********************************************************
Private key x                 : 344
Public key y                  : 2622801558311694360028901
5144834406738245842196087531964790101686573450362035963870
5042253189685480799336202993
 ********************************************************

**************************Signature Generation***********
Message Entered               : 778877
H(m) of message               : 1435506760964299109270269
Signature (r,s) generated     : (147822164069296733981326



*********************************************************
********************** Signature Verification ***********
*********************************************************
```

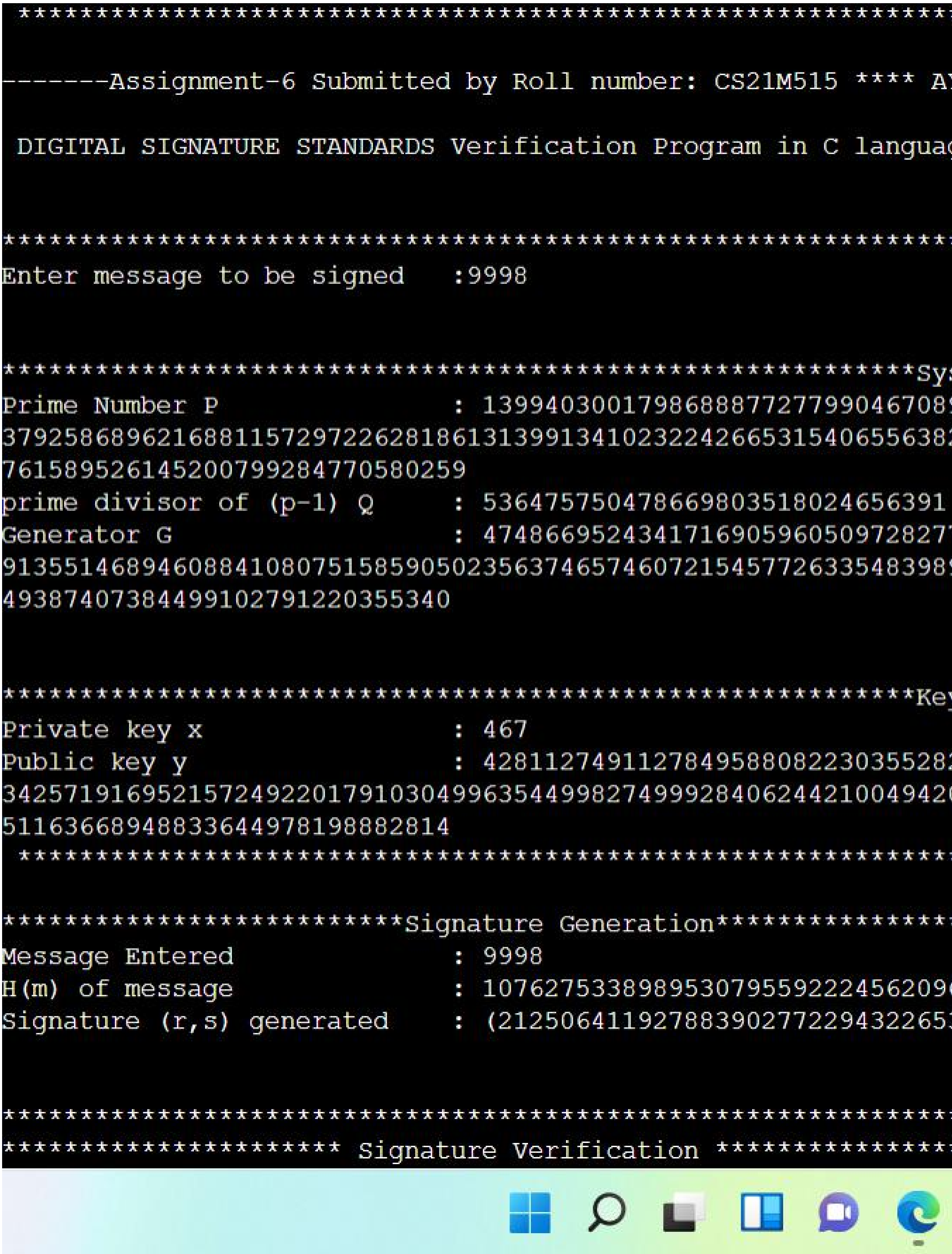
2. Now we pass the wrong message **33333** to check with correct r and s values as per below screen shot it reject the message with Message received is INVALID.. SIGNATURE VERIFICATION IS FAILED!!!!!!!!!!!!!!...

REJECTED..!!



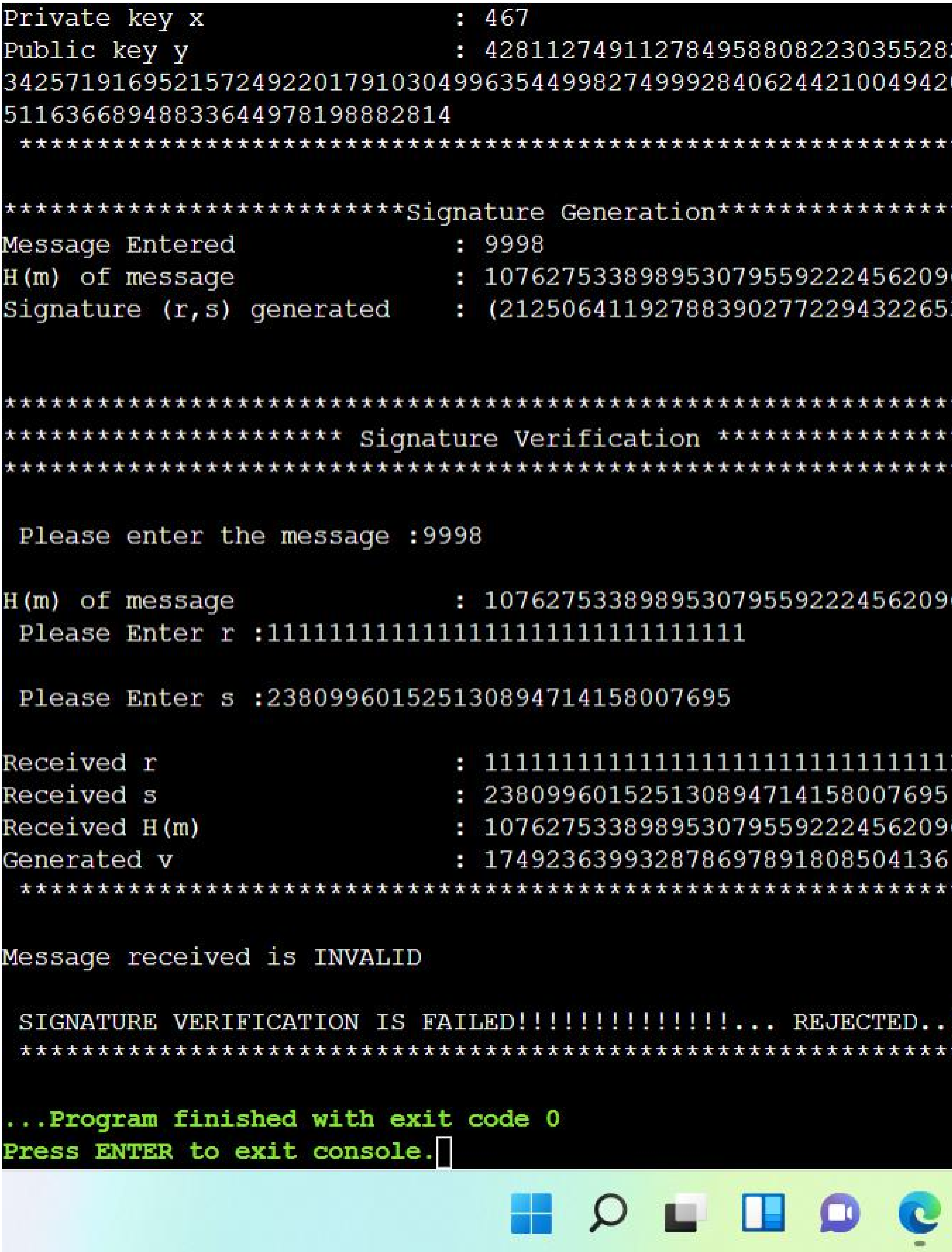
```
*********************************************************
Private key x                : 344
Public key y                 : 26228015583116943600289017
651448344067382458421960875319647901016865734503620359638
88504225318968548079933620299 3
 ********************************************************

**************************Signature Generation**********
Message Entered              : 778877
H(m) of message              : 143550676096429910927026 91
Signature (r,s) generated    : (1478221640692967339813260


*********************************************************
********************** Signature Verification **********
*********************************************************

 Please enter the message :33333

H(m) of message              : 366749091056488992628822 66
 Please Enter r :14782216406929673398132607 1327

 Please Enter s :11680087594346049365821319 2380

Received r                   : 147822164069296733981326 07
Received s                   : 116800875943460493658213 19
Received H(m)                : 366749091056488992628822 66
Generated v                  : 569354584346052004583897 48
 ********************************************************

Message received is INVALID

 SIGNATURE VERIFICATION IS FAILED!!!!!!!!!!!!!!... REJECT
 ********************************************************

...Program finished with exit code 0
```

Sample Output 3 : any number entered 9998 then program do the key gernartion and signature generation as per screen
shot.



```
 **********************************************************

-------Assignment-6 Submitted by Roll number: CS21M515 **** A

 DIGITAL SIGNATURE STANDARDS Verification Program in C langua


**********************************************************
Enter message to be signed    :9998


***********************************************************Sy
Prime Number P                : 139940300179868887727799046708
3792586896216881157297226281861313991341023224266531540655638
76158952614520079928477058025 9
prime divisor of (p-1) Q      : 536475750478669803518024656391
Generator G                   : 474866952434171690596050972827
91355146894608841080751585905023563746574607215457726335483989
4938740738449910279122035534 0


***********************************************************Ke
Private key x                 : 467
Public key y                  : 428112749112784958808223035528
34257191695215724922017910304996354499827499928406244210049420
511636689488336449781988828l4
 **********************************************************


**************************Signature Generation***************
Message Entered               : 9998
H(m) of message               : 107627533898953079559222456209
Signature (r,s) generated     : (212506411927883902772294322651


**********************************************************
********************** Signature Verification ***************
```

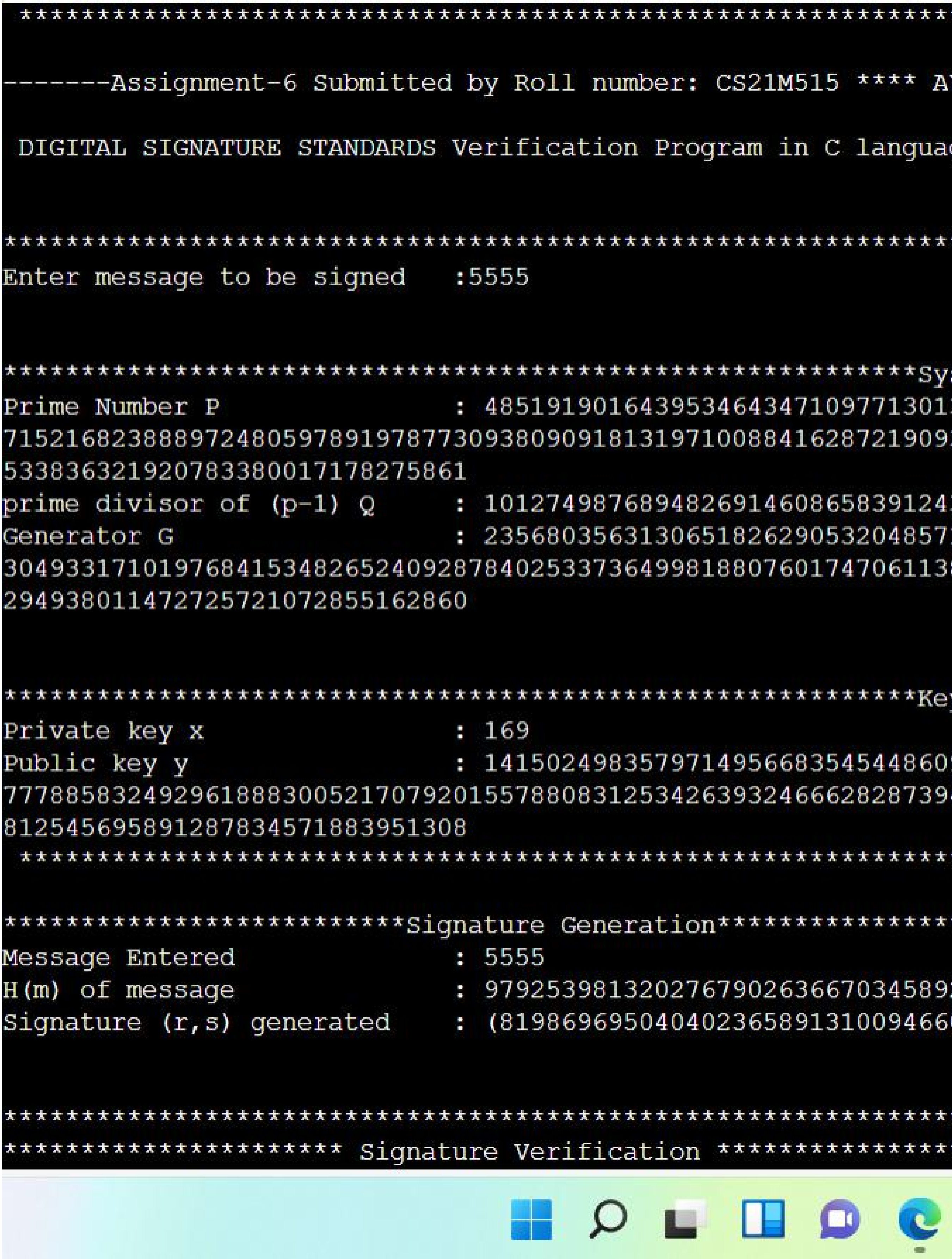
Now we will pass the wrong value of Signature r as 1111111 just any value So as we are passing signature value Wrong it fails the verification and gives this message: ****SIGNATURE VERIFICATION IS FAILED!!!!!!!!!!!!!!... REJECTED..!! ** below is screen shot of** this



```
Private key x                 : 467
Public key y                  : 428112749112784958808223035528
3425719169521572492201791030499635449982749992840624421004942
5116366894883364497819888 2814
 ************************************************************


**************************Signature Generation***************
Message Entered               : 9998
H(m) of message               : 107627533898953079559222456209
Signature (r,s) generated     : (21250641192788390277229432265



*************************************************************
********************** Signature Verification ***************
*************************************************************


 Please enter the message :9998

H(m) of message               : 107627533898953079559222456209
 Please Enter r :1111111111111111111111111111111

 Please Enter s :238099601525130894714158007695

Received r                    : 111111111111111111111111111111
Received s                    : 238099601525130894714158007695
Received H(m)                 : 107627533898953079559222456209
Generated v                   : 174923639932878697891808504136
 ************************************************************


Message received is INVALID

 SIGNATURE VERIFICATION IS FAILED!!!!!!!!!!!!!... REJECTED..
 ************************************************************


...Program finished with exit code 0
Press ENTER to exit console.
```

Sample output 3

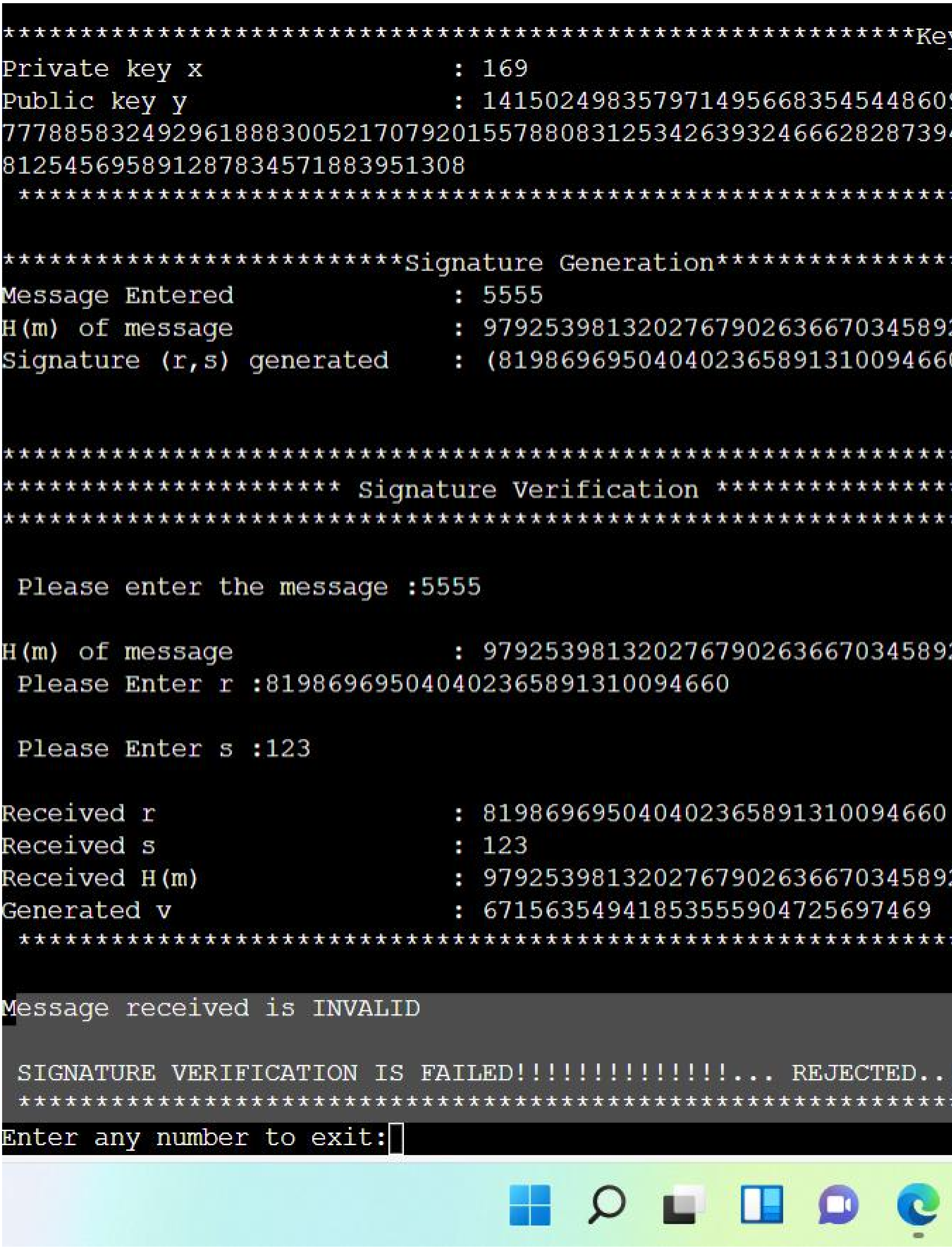
Test number message is entered
is **5555**



```
 ************************************************************

-------Assignment-6 Submitted by Roll number: CS21M515 **** A

 DIGITAL SIGNATURE STANDARDS Verification Program in C languag


*************************************************************
Enter message to be signed    :5555


***********************************************************Sy
Prime Number P                : 485191901643953464347109771301
71521682388897248059789197877309380909181319710088416287219092
53383632192078338001717827586 1
prime divisor of (p-1) Q      : 101274987689482691460865839124
Generator G                   : 235680356313065182629053204857
30493317101976841534826524092878402533736499818807601747061133
2949380114727257210728551628 60


***********************************************************Ke
Private key x                 : 169
Public key y                  : 141502498357971495668354544860
77788583249296188830052170792015578808312534263932466628287394
8125456958912878345718839513 08
 ************************************************************


**************************Signature Generation***************
Message Entered               : 5555
H(m) of message               : 979253981320276790263667034589
Signature (r,s) generated     : (81986969504040236589131009466


*************************************************************
********************** Signature Verification ***************
```

Now we will enter the wrong value of signature s as just 123 somthing as shown in belwo screenshot so it will fail the Signature validation as per belwo screen shot.SIGNATURE VERIFICATION IS FAILED!!!!!!!!!!!!!!... REJECTED..!!**

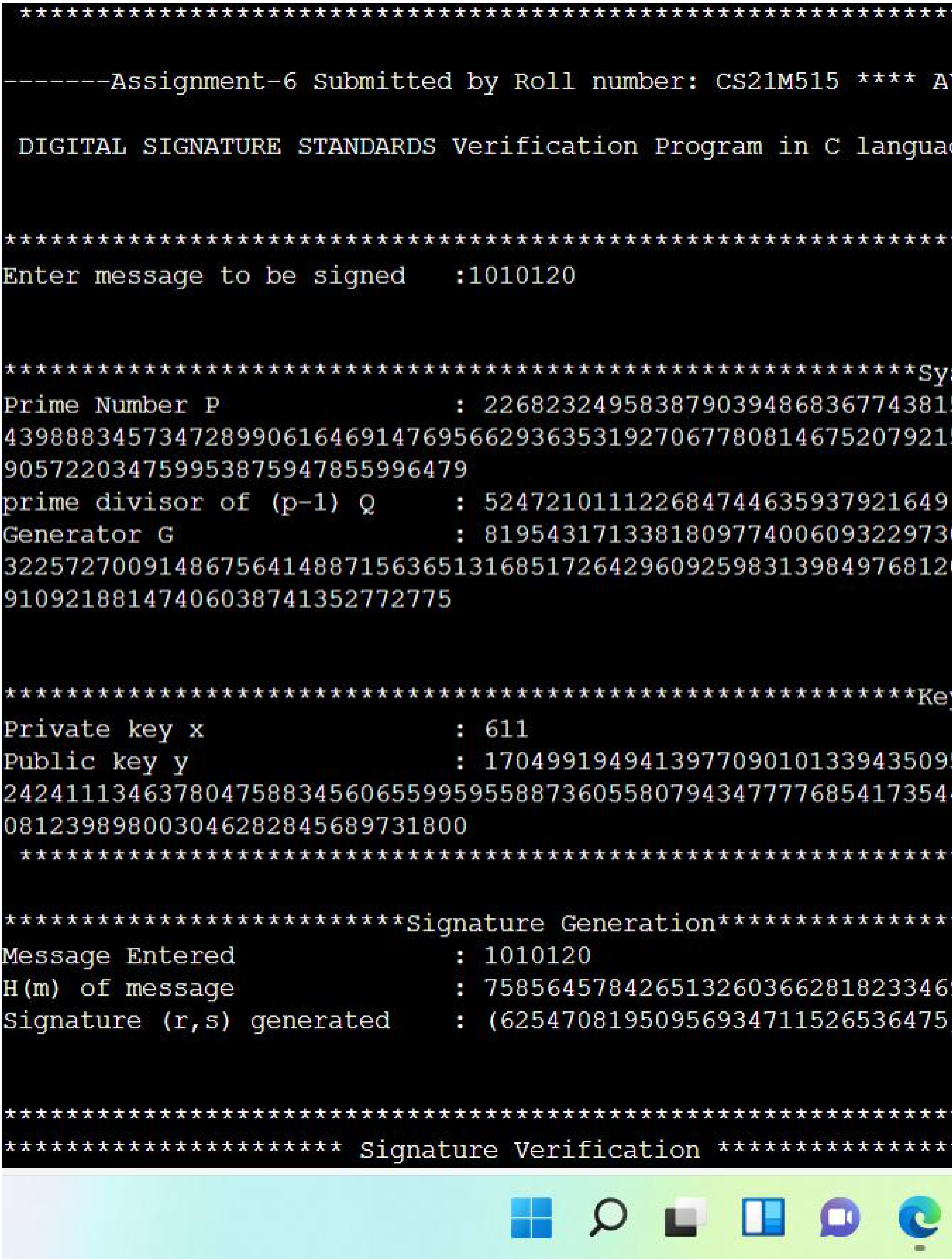
**



```
***********************************************************Key
Private key x                : 169
Public key y                 : 14150249835797149566835454486O
7778858324929618883005217079201557880831253426393246662828739
8125456958912878345718839513O8
 ************************************************************

**************************Signature Generation***************
Message Entered              : 5555
H(m) of message              : 97925398132027679026366703458 9
Signature (r,s) generated    : (8198696950404023658913100946 6


*************************************************************
********************** Signature Verification ***************
*************************************************************


 Please enter the message :5555

H(m) of message              : 97925398132027679026366703458 9
 Please Enter r :819869695040402365891310094660

 Please Enter s :123

Received r                   : 819869695040402365891310094660
Received s                   : 123
Received H(m)                : 97925398132027679026366703458 9
Generated v                  : 671563549418535559047256 97469
 ************************************************************

Message received is INVALID

 SIGNATURE VERIFICATION IS FAILED!!!!!!!!!!!!!... REJECTED..
 ************************************************************
Enter any number to exit:
```

Sample out put 4

We will enter any
number

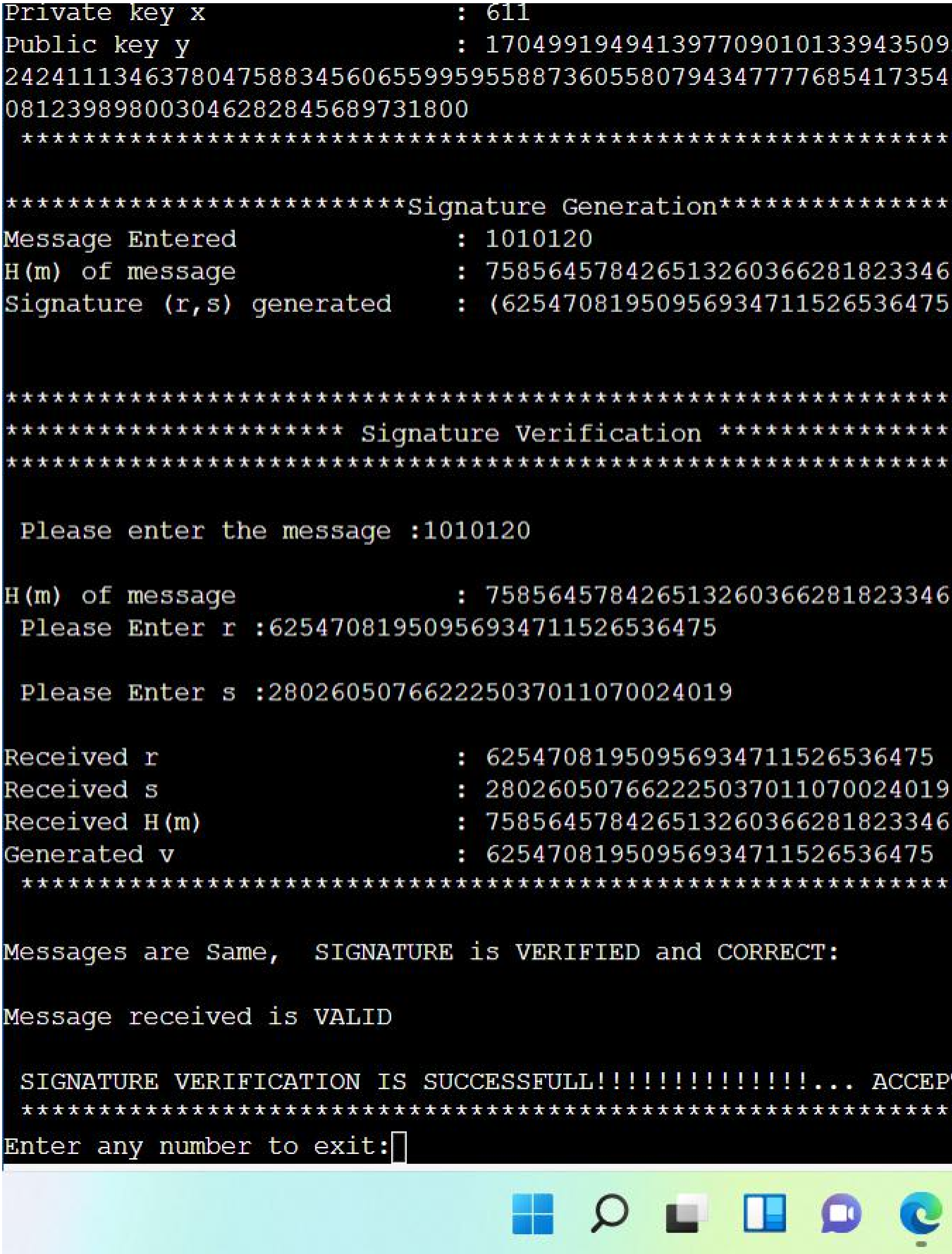


```
 ************************************************************

-------Assignment-6 Submitted by Roll number: CS21M515 **** A

 DIGITAL SIGNATURE STANDARDS Verification Program in C langua


*************************************************************
Enter message to be signed    :1010120


***********************************************************Sy
Prime Number P                : 22682324958387903948683677438l
43988834573472899061646914769566293635319270677808146752079215
9057220347599538759478559964 79
prime divisor of (p-1) Q      : 5247210111226847446359379216 49
Generator G                   : 8195431713381809774006093229 73
32257270091486756414887156365131685172642960925983139849768120
91092188147406038741352772775


***********************************************************Ke
Private key x                 : 611
Public key y                  : 1704991949413977090101339435095
24241113463780475883456065599595588736055807943477768541735 4
081239898003046282845689731800
 ************************************************************


**************************Signature Generation***************
Message Entered               : 1010120
H(m) of message               : 7585645784265132603662818233465
Signature (r,s) generated     : (6254708195095693471152653647 5


*************************************************************
********************** Signature Verification ***************
```

Then we will verify by entering the CORRECT message number

and Correct SIGNATURE values r and s , SO we get successful message as

belwo.



```
Private key x                  : 611
Public key y                   : 170499194941397709010133943509
2424111346378047588345606559959558873605580794347776854173554
0812398980030462828456897318 00
 ************************************************************

**************************Signature Generation***************
Message Entered                : 1010120
H(m) of message                : 758564578426513260366281823346
Signature (r,s) generated      : (625470819509569347115265364475


*************************************************************
********************** Signature Verification ***************
*************************************************************


 Please enter the message :1010120

H(m) of message                : 758564578426513260366281823346
 Please Enter r :625470819509569347115265364475

 Please Enter s :280260507662225037011070024019

Received r                     : 625470819509569347115265364475
Received s                     : 280260507662225037011070024019
Received H(m)                  : 758564578426513260366281823346
Generated v                    : 625470819509569347115265364475
 ************************************************************

Messages are Same,  SIGNATURE is VERIFIED and CORRECT:

Message received is VALID

 SIGNATURE VERIFICATION IS SUCCESSFULL!!!!!!!!!!!!!... ACCEP
 ************************************************************
Enter any number to exit:
```