

## COMP-4476 - Assignment 2

Name: Srijan Ravisankar  
Student #: 1302850

Editor/Compiler used for the task:

- ★ Editor: Visual Studio Code (VS Code) was used as the primary code editor for development.
- ★ Compiler: The code was compiled and executed using the GNU Compiler Collection (GCC) within the Windows Subsystem for Linux (WSL) environment.

How to Run the Code:

- ★ This C++ program is a single-file source code that can be compiled and executed using g++.
- ★ Prerequisites:
  - Ensure you have g++ installed. You can check by running:  
sh g++ --version
  - If g++ is not installed, you can install it using:
    - On Ubuntu/Debian:  
sh sudo apt update && sudo apt install g++
    - On macOS (via Homebrew):  
sh brew install gcc
    - On Windows (via MinGW):
      - Install MinGW from <https://www.mingw-w64.org/>
      - Ensure g++ is added to your system's PATH
- ★ Compilation and Execution:
  - Use Ubuntu for compilation and execution.
  - Update Your Package Lists:  
sudo apt update
  - Install GMP Development Library:  
sudo apt install libgmp-dev
  - Verify Installation:  
gmp version
  - Compile and then run Sample C++ Program Using GMP:  
g++ test\_gmp.cpp -o outputfile -lgmp  
./test\_gmp
- ★ Opening public key and private key files:
  - Open the output files with VS Code or any Browser.

## Code Screenshots:

```
1  #include <iostream>
2  #include <gmp.h>
3  #include <cstdlib>
4  #include <ctime>
5  #include <fstream>
6
7  void generateKeys(mpz_t e, mpz_t d, mpz_t n) {
8      // setting state and seed
9      gmp_randstate_t state;
10     gmp_randinit_default(state);
11     gmp_randseed_ui(state, time(0));
12
13     // initializing required variables
14     mpz_t p, q, phi, temp1, temp2, range, gcd;
15     mpz_inits(p, q, phi, temp1, temp2, range, gcd, NULL);
16
17     // generating two distinct prime numbers p and q
18     bool isDistinctPrime = false;
19     while (!isDistinctPrime) {
20         mpz_urandomb(p, state, 512);
21         mpz_nextprime(p, p);
22
23         mpz_urandomb(q, state, 512);
24         mpz_nextprime(q, q);
25
26         isDistinctPrime = mpz_cmp(p, q) != 0;
27     }
28
29     // calculating n = p x q
30     mpz_mul(n, p, q);
31
32     // calculating phi(n) = (p - 1)(q - 1)
33     mpz_sub_ui(temp1, p, 1);
34     mpz_sub_ui(temp2, q, 1);
35     mpz_mul(phi, temp1, temp2);
36 }
```

```
EXPLORER    ***    1302850_Srijan_Sourcecode.cpp X
> OPEN EDITORS    1302850_Srijan_Sourcecode.cpp > generateKeys(mpz_t mpz_t, mpz_t)
ASSIGNMENT 2 SUBMIT...
> .vscode
1302850_Srijan_2.pdf
1302850_Srijan_Privat...
1302850_Srijan_Publi...
1302850_Srijan_Sourc...
1302850_Srijan_Sourc...

36
37 // selecting integer e such that 1 < e < phi(n) and gcd(phi(n), e) = 1
38 mpz_sub_ui(range, phi, 2);
39 do {
40     mpz_urandomm(e, state, range);
41     mpz_add_ui(e, e, 2);
42     mpz_gcd(gcd, phi, e);
43 } while (mpz_cmp_ui(gcd, 1) != 0);
44
45 // calculating d such that d x e (mod phi(n)) = 1 or d = e^(-1) (mod phi(n))
46 mpz_invert(d, e, phi);
47
48 // storing public key KU = (e, n)
49 std::ofstream publicKeyFile("1302850_Srijan_Publickey");
50 char* eStr = mpz_get_str(NULL, 10, e);
51 char* nStr = mpz_get_str(NULL, 10, n);
52 publicKeyFile << "(" << eStr << ", " << nStr << ")";
53
54 // storing private key KR = (d, n)
55 std::ofstream privateKeyFile("1302850_Srijan_Privatekey");
56 char* dStr = mpz_get_str(NULL, 10, d);
57 privateKeyFile << "(" << dStr << ", " << nStr << ")";
58
59 // outputting keys
60 std::cout << "Generated public and private keys and saved to 1302850_Srijan_Publickey and 1302850_Srijan_Privatekey" << "\n\n";
61
62 std::cout << "Public key (e, n):" << "\n";
63 std::cout << "(";
64 mpz_out_str(stdout, 10, e);
65 std::cout << ", ";
66 mpz_out_str(stdout, 10, n);
67 std::cout << ")";
68
69 std::cout << "\n\n";
70
71 std::cout << "Private key (d, n):" << "\n";
72 std::cout << "(";
```

```
EXPLORER    ...    G: 1302850_Srijan_Sourcecode.cpp X
> OPEN EDITORS
ASSIGNMENT 2 SUBMITTI...
> .vscode
1302850_Srijan_Privat...
1302850_Srijan_Publi...
1302850_Srijan_Sourc...
G: 1302850_Srijan_Sourc...

7  void generateKeys(mpz_t e, mpz_t d, mpz_t n) {
72
73     std::cout << "Private key (d, n):" << "\n";
74     std::cout << "(";
75     mpz_out_str(stdout, 10, d);
76     std::cout << ", ";
77     mpz_out_str(stdout, 10, n);
78     std::cout << ")";
79
80     std::cout << "\n\n";
81 }
82
83 void encrypt(mpz_t C, mpz_t M, mpz_t e, mpz_t n) {
84     // calculates ciphertext C such that C = M^e (mod n)
85     mpz_powm(C, M, e, n);
86
87     // outputting ciphertext after encryption
88     std::cout << "Ciphertext after encryption: " << "\n";
89     mpz_out_str(stdout, 10, C);
90     std::cout << "\n\n";
91 }
92
93 void decrypt(mpz_t M, mpz_t C, mpz_t d, mpz_t n) {
94     // calculates plaintext M such that M = C^d (mod n)
95     mpz_powm(M, C, d, n);
96
97     // converting mpz to plaintext
98     size_t count;
99     size_t size = mpz_sizeinbase(M, 2) / 8 + 1;
100    char* buffer = new char[size];
101    mpz_export(buffer, &count, 1, 1, 0, 0, M);
102    std::string result(buffer, count);
103
104    // outputting plaintext after decryption
105    std::cout << "Plaintext after decryption: " << "\n";
106    std::cout << result;
107    std::cout << "\n\n";
108 }
```

```
EXPLORER    ...    1302850_Srijan_Sourcecode.cpp X
> OPEN EDITORS
1302850_Srijan_Sourcecode.cpp > ...
ASSIGNMENT 2 SUBMITT...
> .vscode
1302850_Srijan_Privat...
1302850_Srijan_Publi...
1302850_Srijan_Sourc...
1302850_Srijan_Sourc...
1302850_Srijan_Sourc...

110  int main() {
111      // initializing required variables
112      mpz_t e, d, n, C, M;
113      mpz_inits(e, d, n, C, M, NULL);
114
115      // generating keys
116      generateKeys(e, d, n);
117
118      // getting plaintext from the user
119      std::string input;
120      std::cout << "Enter the plaintext (without spaces): ";
121      std::cin >> input;
122      std::cout << "\n\n";
123
124      // converting plaintext to mpz
125      mpz_import(M, input.length(), 1, 1, 0, 0, input.c_str());
126
127      // encrypting plaintext
128      encrypt(C, M, e, n);
129
130      // decrypting ciphertext
131      decrypt(M, C, d, n);
132
133      return 0;
134  }
```

> OUTLINE  
> TIMELINE

## Output Screenshots:

## Terminal output:

```
srijanvr@Tiger: /mnt/c/Users/ srijanvr@Tiger:~$ cd /mnt/c/Users/srija/OneDrive/Srijan/"Assignment 2 Submission"
srijanvr@Tiger:/mnt/c/Users/srija/OneDrive/Srijan/Assignment 2 Submission$ g++ 1302850_Srijan_Sourcecode.cpp -o 1302850_Srijan_Sourcecode -lgmp
srijanvr@Tiger:/mnt/c/Users/srija/OneDrive/Srijan/Assignment 2 Submission$ ./1302850_Srijan_Sourcecode
Generated public and private keys and saved to 1302850_Srijan_Publickey and 1302850_Srijan_Privatekey

Public key (e, n):
(52327986016428990643903941183219572103451226444725661163505079084129447484554352834099356960536279944525797965644519464111470658062581783134193
403450295307362365741153454777565581893155659028131291189997263468934212281200891013406537622060706289304918364147240750956151190477117051892414
1942221100116674797, 109606036081431485679221303800884167514816604388617736739755453845123769391057669483656158945168740456096123809416881640461
308671254165745910924401921464102902640979816458118698673092033931087716412380362613315825770438641625105884946499924842734555141118126414014814
2663053975640395963473536903923618380903)

Private key (d, n):
(70425380978215723972144613206750473539944662657517281684146254207174893666209609829886567667451045009106843294018115167330266570143683596658918
323222738308320825947198894278568389041684432418477057089261200665935494503269324610896682686877967549104980951105389732152043229285281056169756
280150339767772333, 109606036081431485679221303800884167514816604388617736739755453845123769391057669483656158945168740456096123809416881640461
086712541657459109244019214641029026409798164581186986730920339310877164123803626133158257704386416251058849464999248427345551411181264140148142
663053975640395963473536903923618380903)

Enter the plaintext (without spaces): Srijan2203

Ciphertext after encryption:
290953329324600031509386791555875200113169940734391591571461002195745336005479340400943545791934917155150001783555229152086505881042809908597530
215542610715993692679987381702180033216150187669985816596740610317825850460144928947022526597170961802226075278526701720624615292534587475824989
639618825621348612

Plaintext after decryption:
Srijan2203

srijanvr@Tiger:/mnt/c/Users/srija/OneDrive/Srijan/Assignment 2 Submission$
```

## Public key file output:

```
EXPLORER  ...  1302850_Srijan_Sourcecode.cpp  1302850_Srijan_Publickey
> OPEN EDITORS
ASSIGNMENT 2 SUBMISSION 1 (523279860164289906439039411832195721034512264447256611635050790841294474845543528340993569605362799445257979656445
> .vscode 1946411147065806258178313419340345029530736236574115345477756558189315565902813129118999726346893421228120089101340
1302850_Srijan_2.pdf 65376220607062893049183641472407509561511904771170518924141942221100116674797,
1302850_Srijan_Privat... 1096060360814314856792213038008841675148166043886177367397554538451237693910576694836561589451687404560961238094168
1302850_Srijan_Publi... 8164046130867125416574591092440192146410290264097981645811869867309203393108771641238036261331582577043864162510588
1302850_Srijan_Sourc... 49464999248427345551411181264140148142663053975640395963473536903923618380903)
1302850_Srijan_Sourc...
```

## Private key file output:

```
EXPLORER  ...  1302850_Srijan_Sourcecode.cpp  1302850_Srijan_Privatekey
> OPEN EDITORS
ASSIGNMENT 2 SUBMISSION 1 (704253809782157239721446132067504735399446626575172816841462542071748936662096098298865676674510450091068432940181
> .vscode 1516733026657014368359665891832322273830832082594719889427856838904168443241847705708926120066593549450326932461089
1302850_Srijan_2.pdf 6682686877967549104980951105389732152043229285281056169756280150339767772333,
1302850_Srijan_Privat... 1096060360814314856792213038008841675148166043886177367397554538451237693910576694836561589451687404560961238094168
1302850_Srijan_Publi... 8164046130867125416574591092440192146410290264097981645811869867309203393108771641238036261331582577043864162510588
1302850_Srijan_Sourc... 49464999248427345551411181264140148142663053975640395963473536903923618380903)
1302850_Srijan_Sourc...
```